LE PREMIER MINISTRE

REPUBLIQUE TOGOLAISE
Travail-Liberté-Patrie

ARRETE N° 2025-005/PMRT
portant adoption du référentiel d'exigences des prestataires d'audit de la sécurité des systèmes d'information

---

LE PREMIER MINISTRE,

Vu la constitution du 06 mai 2024 ;

Vu la loi n° 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité modifiée par la loi n° 2022-009 du 24 juin 2022 ;

Vu le décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'Agence nationale de la cybersécurité ;

Vu l'arrêté n° 2022-040/PMRT du 29 juin 2022 portant adoption des règles de cybersécurité en République togolaise ;

Vu le décret n° 2022-09/PR du 25 août 2022 relatif à la qualification des prestataires de services de confiance de cybersécurité et des produits de sécurité et à l'agrément des centres d'évaluation ;

Vu le décret n° 2024-040/PR du 1er août 2024 portant nomination du Premier ministre ;

Vu le décret n° 2024-041/PR du 20 août 2024 portant composition du gouvernement ;

Vu le procès-verbal de la réunion du Comité stratégique de l'Agence nationale de la cybersécurité (ANCy), en sa séance du 02 décembre 2024 ;

ARRETE :

Article 1er : Objet

Le présent arrêté porte adoption du référentiel d'exigences des prestataires d'audit de la sécurité des systèmes d'information en République togolaise.

Article 2 : Application

Les ministres, chacun en ce qui le concerne, veillent à l'application des dispositions du présent arrêté par les administrations et les opérateurs de services essentiels (OSE) relevant de leur ressort.

Article 3 : **Exécution**

Le Directeur général de l'Agence nationale de la cybersécurité (ANCy), est chargé de l'exécution du présent arrêté qui sera publié au Journal officiel de la République togolaise.

Fait à Lomé, le 31 JAN 2025

Le Premier ministre

SIGNE

Victoire S. TOMEGAH-DOGBE

Pour ampliation,
Le Ministre,
Secrétaire général du Gouvernement

Christian Eninam TRIMUA

ANCy
Agence Nationale de la Cybersécurité

RÉPUBLIQUE TOGOLAISE

REFERENTIEL D'EXIGENCES

Prestataires d'Audit de la Sécurité des Systèmes d'Information (PASSI)

Version 1.0 du 31 JAN 2025

www.ancy.gouv.tg

Premier Ministre	
Comité Stratégique	Agence Nationale de la Cybersécurité (ANCy)

HISTORIQUE DES VERSIONS			
DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
31/01/2025	1.0	Première version applicable	ANCy

Les commentaires sur le présent document sont à adresser à :

Agence Nationale de la Cybersécurité

63, Boulevard du 13 janvier, Nyékonakpoè

07 BP 7878 Lomé – TOGO

Téléphone : +228 70 60 60 83 / 97 52 58 58

secretariat.ancy@ancy.gouv.tg

Table des matières

FICHE SYNTHETIQUE

1. Introduction

Face à l'évolution rapide des menaces cybernétiques, il est indispensable de disposer de mécanismes robustes pour évaluer et renforcer la sécurité des systèmes d'information (SSI). Ce référentiel vise à définir les règles, exigences et méthodologies que les prestataires d'audit doivent respecter afin de garantir la qualité et la crédibilité de leurs services. Il s'agit d'un cadre structurant qui établit les bases pour des audits efficaces, indépendants et conformes aux meilleures pratiques internationales.

2. Objectifs du référentiel

Le **Référentiel des Prestataires d'Audit de la Sécurité des Systèmes d'Information (PASSI)** poursuit plusieurs objectifs stratégiques. Tout d'abord, il vise à assurer la qualité des audits en imposant des normes strictes et des méthodologies éprouvées. Ensuite, il cherche à renforcer la confiance des parties prenantes, notamment les entreprises et les institutions publiques, en garantissant l'indépendance et la transparence des audits réalisés. Enfin, il met un accent particulier sur la protection des données sensibles, en encadrant l'accès, le traitement et la conservation des informations collectées lors des missions d'audit.

3. Processus d'Audit : Étapes Essentielles

Préparation de l'audit : la première étape consiste à définir clairement le périmètre de l'audit, en précisant les objectifs spécifiques et les limites de la mission. Une fois ce périmètre établi, un plan d'audit détaillé est élaboré. Ce plan inclut les ressources nécessaires, les outils à utiliser, ainsi que le calendrier des activités.

Exécution de l'audit : lors de l'exécution, les auditeurs procèdent à une collecte méthodique de données en utilisant des outils fiables et des techniques éprouvées. Ces données sont ensuite analysées pour identifier les vulnérabilités et évaluer leur impact potentiel sur les activités de l'organisation.

Rapport d'audit : une fois les analyses terminées, un rapport d'audit est élaboré. Ce rapport inclut un résumé exécutif destiné aux décideurs, une description des vulnérabilités identifiées et des recommandations pratiques pour remédier aux failles.

Suivi et validation : après la remise du rapport, l'ANCy et le PASSI qualifié accompagnent le client dans la mise en œuvre des recommandations. Si nécessaire, un audit de suivi est réalisé pour s'assurer que les mesures correctives ont été efficaces.

4. Exigences applicables aux prestataires

Compétences professionnelles : les prestataires d'audit doivent posséder des certifications reconnues, telles que ISO 27001 ou CISA, et justifier d'une expérience pratique dans le domaine de la sécurité des systèmes d'information et de l'audit.

Code d'éthique : les auditeurs doivent respecter un code d'éthique rigoureux, incluant des principes tels que l'intégrité, l'impartialité et la confidentialité. Ce code garantit que les missions sont conduites de manière professionnelle et responsable.

Capacité opérationnelle : les prestataires doivent disposer des ressources humaines, matérielles et technologiques nécessaires pour mener à bien leurs missions. Les outils utilisés doivent être conformes aux standards internationaux et adaptés aux spécificités des missions d'audit.

5. Types d'audits couverts

Audit organisationnel : l'audit de l'organisation de la sécurité permet de réaliser un état des lieux exhaustif du niveau de sécurité de l'ensemble du système d'information sur les volets organisationnels, procéduraux et technologiques.

Audit environnemental et physique : l'audit environnemental et physique permet de s'assurer que les aspects physiques de la sécurité du système d'information sont correctement couverts.

Audit des architectures : l'audit d'architecture consiste à contrôler la conformité du choix, du déploiement et de la mise en œuvre d'un système d'information, notamment les dispositifs matériels et logiciels, à des référentiels ou standards internationaux et aux exigences et règles internes d'une entité. L'audit peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

Audit des configurations : l'audit de configuration consiste à vérifier la mise en œuvre de pratiques de sécurité conformes à des référentiels ou des standards internationaux et aux exigences et règles internes d'une entité en matière de configuration des dispositifs matériels et logiciels déployés dans un système d'information.

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 en vue 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.

Audits intrusifs : les tests d'intrusion permettent 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 potentiel attaquant. Ces tests peuvent être réalisés en interne (à partir du système d'information) ou en externe.

Audit des systèmes industriel SCADA : l'audit des systèmes industriels est une spécialisation des audits de vulnérabilités qui évalue et traite les questions de sécurité relatives aux systèmes industriels. La connaissance des technologies spécifiques à la production industrielle est souvent primordiale dans ce type d'audit.

6. Importance du référentiel pour la cybersécurité

Le référentiel des prestataires d'audit de SSI joue un rôle crucial dans le renforcement de la résilience des organisations face aux menaces cybernétiques. Il permet de prévenir les cyberattaques en identifiant et en corrigeant les failles de sécurité. En harmonisant les pratiques et en uniformisant les attentes, ce référentiel contribue à professionnaliser les acteurs du secteur et à élever le niveau global de sécurité des systèmes d'information.

7. Conclusion

En établissant des standards clairs et rigoureux, le référentiel des prestataires d'audit de SSI offre une garantie de qualité et de fiabilité. Il constitue un outil indispensable pour renforcer la confiance des parties prenantes, améliorer la sécurité des systèmes d'information et accompagner les organisations dans leur démarche de conformité et de résilience face aux menaces cybernétiques.

1.PRÉSENTATION GENERALE

1.1. AVANT-PROPOS

La digitalisation croissante des services et des processus engendre une interconnexion plus accrue des réseaux. Ce mouvement expose les systèmes d'information à de nombreux risques, notamment de vol, de modification, de détournement ou de destruction des données. La réalisation de ces risques est généralement permise par des points d'interconnexion avec l'extérieur, en particulier les accès internet associés à la messagerie ou à des téléservices, qui rendent possibles l'introduction et le maintien de fraudeurs au sein des systèmes d'information.

Afin de sécuriser leurs systèmes d'informations, il est recommandé aux entités, dans une démarche de gestion des risques, de mettre en place des mesures adaptées et proportionnées aux menaces auxquelles elles font face, tout en tenant également compte des enjeux liés à leur organisation et à leur fonctionnement.

Les mesures de sécurité auxquelles les entités peuvent avoir recours sont de plusieurs ordres, notamment organisationnel, physique et technique. L'audit occupe une place centrale au rang de ces mesures de sécurité.

L'audit constitue en effet l'un des moyens permettant à toute entité d'éprouver et s'assurer du niveau de sécurité de son système d'information. Il permet en pratique, de mettre en évidence à la fois les forces, les faiblesses et les vulnérabilités des systèmes d'information, à travers notamment ses conclusions. Les conclusions d'audit permettent d'identifier des axes d'amélioration, de proposer des recommandations et de contribuer à l'élévation du niveau de sécurité des systèmes d'information.

L'audit se présente donc comme une étape cruciale dans l'amélioration de la maturité des systèmes d'information.

Une prestation d'audit peut avoir pour objectif d'évaluer un niveau :

- De conformité vis-à-vis d'un ensemble de règles, de bonnes pratiques, de guides, de référentiels, ou de normes ;
- De sécurité afin d'identifier des vulnérabilités ;
- De conformité et de sécurité.

1.2. OBJECTIF DU REFERENTIEL ET DOMAINE D'APPLICATION

Le présent document constitue le Référentiel d'exigences applicables à un prestataire d'audit de la sécurité des systèmes d'information qui délivre des prestations d'audit correspondant à des activités d'audit bien définies dans le présent document.

Ainsi, les prestations d'audit couvertes par le Référentiel sont les suivantes :

- Audit organisationnel ;
- Audit environnemental et physique ;
- Audit des architectures ;
- Audit des configurations ;
- Audit de code source ;
- Audits intrusifs ;
- Audit des systèmes industriels SCADA.

Le présent Référentiel vise à établir un cadre permettant la qualification des prestataires de services d'audit de la sécurité des systèmes d'information, conformément à la règlementation en vigueur et selon les modalités décrites dans le Modèle de qualification des prestataires de service de confiance en cybersécurité.

Il permet d'une part d'accompagner les responsables d'audit dans la réalisation des missions d'audit de sécurité des systèmes d'information, et d'autre part de permettre au commanditaire de la prestation d'audit de disposer de garanties sur les compétences du prestataire et de son personnel, sur la qualité des prestations d'audit qui sont et/ou seront fournies, et sur la confiance que le commanditaire peut accorder au prestataire.

1.3. DOCUMENTS DE REFERENCE

Le présent Référentiel s'inscrit dans un cadre légal et règlementaire plus global en vigueur au Togo, et applicable aux prestataires de services de confiance en cybersécurité.

L'ensemble des textes découlant de ce cadre légal et règlementaire et susceptibles de s'appliquer aux prestataires d'audit de la sécurité des systèmes d'information ainsi qu'aux prestations d'audit, sont listés ci-dessous de manière non-exhaustive. Ils sont identifiés dans le Référentiel en tant que « Documents de référence ».

Le présent référentiel s'applique en complément des Documents de référence dont il n'exclut pas l'application. Il n'exclut pas non plus l'application des règles générales imposées aux Prestataires en leur qualité de professionnels, et notamment leur devoir de conseil vis-à-vis des Clients finaux.

Le Référentiel peut être utilisé à titre de bonnes pratiques en dehors de tout contexte règlementaire.

1.3.1. Publications de l'ISO

- La norme ISO 19011 :2018, qui fournit les principes théoriques de management d'un audit mais aussi les compétences attendues par les auditeurs et les responsables d'audits ;
- La norme ISO 22301 :2019, Sécurité et résilience, Systèmes de management de la continuité d'activité ;
- La norme ISO 27001 :2022, Sécurité de l'information, cybersécurité et protection de la vie privée ;
- La norme ISO 27002 :2022, Sécurité de l'information, cybersécurité et protection de la vie privée-Mesures de sécurité de l'information ;
- La norme ISO 27005 :2022, Sécurité de l'information, cybersécurité et protection de la vie privée-Préconisations pour la gestion des risques liés à la sécurité de l'information.

1.3.2. Textes législatifs et règlementaires

- La loi n° 2017-007 du 22 juin 2017 relative aux transactions électroniques en République togolaise ;
- La loi n° 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité, modifiée par la loi n° 2022-009 du 24 juin 2022 ;
- Le décret n°2018-062/PR du 21 mars 2018 portant réglementation des transactions et services électroniques au Togo ;
- L'arrêté n°016/MPEN/CAB du 17 décembre 2018 fixant les conditions de reconnaissance au Togo des certificats et signatures électroniques délivrés par des prestataires de services de confiance établis hors du territoire national ;
- La loi n°2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel ;
- La loi n°2020-009 du 10 septembre 2020 relative à l'identification biométrique des personnes physiques au Togo ;
- Le décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'ANCY ;

- Le décret n° 2019-095/PR du 08 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes ;
- Le décret n°2019-098/PR du 11 juillet 2019 portant création, attributions et organisation de la société CYBER DEFENSE AFRICA (CDA) ;
- Le décret n° 2022-09/PR du 25 août 2022 relatif à la qualification des prestataires de services de confiance de cybersécurité et des produits de sécurité et à l'agrément des centres d'évaluation ;
- L'arrêté n° 2022-040/PRMT du 29 juin 2022 portant adoption des règles de cybersécurité en République togolaise.

Ces documents sont disponibles auprès de l'ANCy.

1.3.3. Documents de l'ANCy

- Décision ANCy portant liste des pays tiers de confiance ;
- Modèle de qualification des prestataires de services de confiance en cybersécurité ;
- Déclaration de la politique de qualification.

1.3.4. Autres

- ITIL (*Information Technology Infrastructure Library*) ou « Bibliothèque pour l'infrastructure des technologies de l'information » : il s'agit d'un ensemble d'ouvrages recensant les bonnes pratiques (« *best practices* ») du management du système d'information.

1.4. IDENTIFICATION DU DOCUMENT ET DATE D'APPLICATION

Le présent document est dénommé « Référentiel d'exigences des prestataires d'audit de la sécurité des systèmes d'information ».

Il peut être identifié par son nom, sa référence, son numéro de version et sa date de mise à jour.

Ce document est applicable à compter de sa publication.

Il est élaboré, mis à jour et publié par l'ANCy, qui précisera les modalités de transition et la date d'effet pour chaque mise à jour.

1.5. ACTIVITES D'AUDIT VISEES PAR LE REFERENTIEL

❖ **Audit organisationnel**

L'audit de l'organisation de la sécurité permet de réaliser un état des lieux exhaustif du niveau de sécurité de l'ensemble du système d'information sur les volets organisationnels, procéduraux et technologiques.

❖ **Audit physique et environnemental**

L'audit physique et environnemental permet de s'assurer que les aspects physiques de la sécurité du système d'information sont correctement couverts.

❖ **Audit des architectures**

L'audit d'architecture consiste à contrôler la conformité du choix, du déploiement et de la mise en œuvre d'un système d'information (notamment les dispositifs matériels et logiciels) à des référentiels ou des standards internationaux et aux exigences et règles internes du commanditaire de l'audit. L'audit peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

❖ **Audit des configurations**

L'audit de configuration consiste à vérifier la mise en œuvre de pratiques de sécurité conformes à des référentiels ou des standards internationaux et aux exigences et règles internes du commanditaire d'audit en matière de configuration des dispositifs matériels et logiciels déployés dans un système d'information.

❖ **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 en vue 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.

❖ **Audits intrusifs**

Les tests d'intrusion permettent 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 potentiel attaquant. Ces tests peuvent être réalisés en interne (à partir du système d'information) ou en externe.

❖ **Audit des systèmes industriels SCADA**

L'audit des systèmes industriels est une spécialisation des audits de vulnérabilité qui évalue et traite les questions de sécurité relatives aux systèmes industriels. La connaissance des technologies spécifiques à la production industrielle est souvent primordiale dans ce type d'audit.

1.6. DEFINITIONS ET ACRONYMES

Les termes suivants utilisés dans le présent document auront la signification indiquée ci-dessous :

1.6.1. 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. Dans le cadre du Référentiel, l'audit est constitué d'un sous-ensemble d'activités d'audit de la sécurité d'un système d'information.

1.6.2. Auditeur

Il s'agit de la personne physique procédant à la réalisation d'un audit pour le compte d'un Prestataire d'audit qualifié personne morale.

1.6.3. Champ d'audit :

Il s'agit de l'étendue et des limites d'un audit. Le champ d'audit décrit généralement les lieux, les unités organisationnelles, les activités, les processus ainsi que la période de temps couverte par l'audit.

1.6.4. Client final

Il s'agit de l'entité qui sollicite ou commande la réalisation d'un audit. En d'autres termes, il s'agit de l'entité auditée par l'auditeur, et qui est responsable de tout ou partie du système d'information audité.

1.6.5. Consultant

C'est un Prestataire d'audit qualifié personne physique. Il s'agit de la personne physique qualifiée par l'ANCy en qualité de prestataire d'audit de la sécurité des systèmes d'information.

1.6.6. Constats d'audit

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

1.6.7. Convention d'audit

L'accord écrit entre un Client final et un Prestataire d'audit qualifié pour la réalisation d'une mission d'audit de la sécurité des systèmes d'information.

1.6.8. Critères d'audit

Ensemble des Référentiels, politiques, procédures ou exigences applicables à la sécurité du système d'information audité.

1.6.9. Diffusion restreinte

Une limitation délibérée de la distribution d'informations à un groupe restreint d'utilisateurs autorisés.

1.6.10. DSI

C'est le Directeur des systèmes d'information

1.6.11. État de l'art

Ensemble de bonnes pratiques et de connaissances relatives à la sécurité des systèmes d'information, publiquement accessibles et reconnues à un moment donné, ainsi que des informations qui en découlent de façon évidente.

1.6.12. Plan d'audit

La description des activités et des dispositions nécessaires pour réaliser un audit préparé par le Responsable équipe de l'audit de commun accord entre l'équipe de l'audit et le Client final, en vue de faciliter la programmation dans le temps et la coordination des activités d'audit.

1.6.13. Prestataire d'audit qualifié

Un prestataire d'audit qualifié par l'ANCy qui offre des services d'audit de la sécurité des systèmes d'information. Il peut s'agir d'une personne physique ou d'une personne morale.

1.6.14. Rapport d'audit

Document de synthèse élaboré par l'équipe d'audit et remis au Client final 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.

1.6.15. Référentiel

Le présent document.

1.6.16. Responsable équipe de l'audit

C'est la personne Responsable de l'équipe d'audit et de la constitution de l'équipe d'audit.

Dans le contexte d'un prestataire d'audit qualifié personne physique, la personne Responsable équipe de l'audit est directement la personne physique qualifiée par l'ANCy.

1.6.17. RSSI

C'est le Responsable de la Sécurité des Systèmes d'Information.

1.6.18. Preuves d'audit

Enregistrements, énoncés de faits ou autres informations qui se rapportent aux critères d'audit et qui sont vérifiables. Les preuves d'audit peuvent être qualitatives ou quantitatives.

Les preuves d'audit peuvent être classées en 4 catégories :

- La preuve physique : c'est ce que voit et constate l'auditeur. En d'autres termes, c'est l'observation que fait l'auditeur ;

- La preuve testimoniale : il s'agit de témoignages. La preuve testimoniale est une preuve très fragile. Par conséquent, elle doit toujours être entérinée par au moins une autre catégorie de preuves ;
- La preuve documentaire : ce sont des procédures écrites, des comptes rendus et des notes ;
- La preuve analytique : elle résulte de calculs, rapprochements, déductions et comparaisons diverses.

1.6.19. PV

Il s'agit du Procès-verbal.

1.6.20. Sécurité d'un système d'information

C'est l'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.

1.6.21. SI

Il s'agit du système d'information.

2. EXIGENCES RELATIVES AU PRESTATAIRE D'AUDIT

2.1. EXIGENCES GENERALES

a. Le prestataire d'audit peut être (i) soit une entité ou une partie d'une entité, dotée de la personnalité morale, (ii) soit une personne physique exerçant sous la forme d'un établissement, dans l'un ou l'autre cas, dûment enregistrée au RCCM (Registre du Commerce et du Crédit Mobilier) pour les besoins de l'activité d'audit ;
b. Le prestataire d'audit doit pouvoir être tenu juridiquement responsable de toutes ses activités d'audit.
c. Le prestaire d'audit doit respecter la règlementation en vigueur au Togo y compris le Modèle de qualification et le présent Référentiel, ainsi que l'état de l'art ;
d. Le prestataire d'audit doit décrire l'organisation de son activité d'audit au Client final, et garantir que les informations fournies à cet égard sont exactes. ;

e. En sa qualité de professionnel, le prestataire est redevable d'un devoir de conseil à l'égard du Client final ;

f. Le prestataire d'audit a l'obligation de formaliser les activités d'audit qu'il réalise pour le compte du Client final dans le cadre d'une Convention d'audit écrite et signée avec celui-ci. Cette convention est conforme aux exigences du Référentiel et aux lois en vigueur au Togo ;

g. Le prestataire d'audit doit démontrer au Client final qu'il a analysé les risques associés à ses activités d'audit et qu'il a mis en place les mesures nécessaires pour atténuer lesdits risques ;

h. Le prestataire d'audit peut, après approbation du Client final, sous-traiter une partie des prestations d'audit à un autre prestataire d'audit qualifié, sous réserve que ce dernier soit conforme et réponde aux exigences du référentiel d'exigences qui lui est applicable ;

i. Le prestataire d'audit doit réaliser les prestations d'audit de manière loyale et impartiale. Il doit par ailleurs faire preuve de respect et de professionnalisme à l'égard du Client final, de son personnel et de ses infrastructures. A cet égard, le prestataire doit apporter une preuve suffisante que son organisation, ses moyens mis en œuvre pour délivrer la prestation, et les modalités de son fonctionnement, notamment financières, ne sont pas susceptibles de compromettre son impartialité et la qualité de sa prestation à l'égard du Client final ou de provoquer des conflits d'intérêts ;

j. Le prestataire doit assumer la responsabilité des activités qu'il réalise pour le compte du Client final dans le cadre de la prestation et en particulier les éventuels dommages qu'il pourrait lui causer. Le prestataire d'audit doit à cet égard souscrire une assurance professionnelle couvrant les éventuels dommages causés au Client final et notamment à son système d'information dans le cadre de la prestation ;

k. Le prestataire d'audit doit s'assurer du consentement du Client final avant toute communication d'informations obtenues ou produites dans le cadre de la prestation. Plus spécifiquement en ce qui concerne les données à caractère personnel, le prestataire d'audit est tenu de procéder au traitement de ce type de données en observant strictement les exigences prévues par la loi togolaise n°2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel ;

l. Le prestataire d'audit doit disposer des licences valides sur les outils (logiciels ou matériels) utilisés pour la réalisation de la prestation ;

m. Le prestataire d'audit doit demander au Client final de lui communiquer les éventuelles exigences légales et réglementaires spécifiques auxquelles il est soumis et notamment celles liées à son secteur d'activité, s'y conformer, et le cas échéant accompagner le Client final dans la démarche de mise en

œuvre de ces obligations si ce dernier lui en fait la demande et dans la mesure où la mobilisation du prestataire d'audit est nécessaire à ces fins ;

n. Le prestataire d'audit doit informer le Client final lorsque ce dernier est tenu de déclarer un incident de sécurité à une instance gouvernementale (par exemple à l'ANCy dans le cadre de l'article 17 du décret n°2019-095/PR relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes) et doit l'accompagner dans cette démarche si ce dernier en fait la demande.

2.2. CODE D'ETHIQUE

Le prestataire d'audit doit disposer d'un code d'éthique signé et/ou ratifié par chaque membre du personnel, et dont une copie doit être adressée à l'ANCy.

Le Code d'éthique inclut au minimum les exigences ci-après :

- Les prestations d'audit sont réalisées avec loyauté, discrétion, impartialité et indépendance ;
- Les prestations d'audit sont réalisées a minima avec les outils et techniques déclarés à l'ANCy lors du processus de qualification ;
- Les auditeurs s'engagent à ne pas divulguer, y compris aux autres auditeurs du prestataire d'audit non concernés par l'audit, les informations obtenues ou générées dans le cadre des audits, sauf autorisation expresse écrite et préalable du Client final commanditaire de l'audit ;
- Les auditeurs notifient au Client final commanditaire de l'audit tout élément illicite identifié pendant l'audit, sous réserve du respect des restrictions ou obligations légales susceptibles de faire obstacle à une telle notification ;
- Les auditeurs en leur qualité de professionnels, s'engagent à respecter les Documents de Référence, l'état de l'art, et toutes les bonnes pratiques liées à l'audit.

2.3. GESTION DES RESSOURCES ET DES COMPETENCES

2.3.1. Le prestataire est une personne morale

a. Le prestataire d'audit doit en permanence employer au minimum 02 auditeurs pour la portée dont la qualification est sollicitée. Le non-respect de cette condition sur une période au moins ou égale à six (06) mois constitue pour l'ANCy un motif de suspension de la qualification du prestataire d'audit.

b. La relation entre le prestataire d'audit et chaque auditeur doit être encadrée par un contrat signé.

c. Le prestataire d'audit a l'obligation pour chaque mission, de désigner un responsable d'équipe d'audit et éventuellement de sous-traitants, pour assurer les audits pour lesquels il a établi des conventions d'audit avec des Clients finaux commanditaires de prestations d'audit ;

d. Le prestataire d'audit doit s'assurer pour chaque audit, que les auditeurs désignés pour réaliser l'audit ont les qualités et les compétences requises pour la mission concernée ;

e. Au moment du recrutement, le prestataire d'audit doit procéder à une vérification, des formations, compétences et références professionnelles des auditeurs, et de la véracité de leur curriculum vitae. Il doit par ailleurs s'assurer par tous moyens, que les auditeurs en cours de recrutement ne font pas l'objet d'une mesure ou d'une sanction incompatible avec l'exercice de leurs fonctions ;

f. Le prestataire d'audit doit s'assurer du maintien à jour des compétences des auditeurs à travers un processus de formation et une veille technologique. A cet égard, le prestataire d'audit a l'obligation de faire suivre à ses auditeurs impliqués dans des missions d'audit, au minimum une (01) formation chaque année dans le domaine de la sécurité des systèmes d'information. La formation continue du prestataire d'audit et de son personnel peut prendre plusieurs formes notamment des modules d'auto-formation, des séminaires internes, ou des séminaires assurés par le CERT.tg ou par l'ANCy. La nature et la liste des formations validantes au titre de la formation continue du prestataire d'audit et de son personnel font l'objet d'une publication sur le site de l'ANCy. Le prestataire d'audit doit à tout moment être en mesure de documenter son plan de formation continue à l'ANCy sur simple demande de celle-ci ;

g. Le prestataire doit mettre à disposition de son personnel les guides de bonnes pratiques et normes nécessaires aux activités d'audit. Il doit par ailleurs assurer une sensibilisation des auditeurs à la règlementation en vigueur au Togo et applicable à leurs missions ;

h. Le prestataire d'audit est responsable des méthodes, outils (logiciels ou matériels) et techniques utilisées par ses auditeurs et de leur bonne utilisation (précautions d'usage, maîtrise de la configuration...). Il doit par ailleurs s'assurer de la mise à jour continue de ces méthodes, outils et techniques, ainsi que de leur pertinence à pouvoir répondre aux besoins des activités d'audit menées ;

i. Le prestataire d'audit doit justifier au travers de son recrutement, qu'il dispose des compétences techniques, théoriques et pratiques nécessaires pour mener des activités d'audit couvertes par la qualification obtenue ;

j. Plus spécifiquement, le prestataire d'audit doit disposer des compétences suivantes :

Compétences techniques	
Réseaux	▪ Protocoles réseaux et infrastructures ▪ Protocoles applicatifs et services d'infrastructures ▪ Configuration sécurisée des équipements réseaux ▪ Réseaux télécoms ▪ Technologies WIFI, voix sur Ip
Systèmes d'exploitation (environnement et durcissement)	▪ Architectures Microsoft ▪ Systèmes UNIX/Linux ▪ Solution de virtualisation
Couche applicative	▪ Méthodes d'intrusion (Black, Grey et white Box) ▪ Guides et principes de développement sécurisé ▪ Applications de type client/serveur ▪ Langages de programmation dans le cadre d'audits de code ▪ Mécanismes cryptographiques ▪ Infrastructures applicatives (serveurs web, serveurs d'application, systèmes de gestion de bases de données)
Équipements et logiciels de sécurité	▪ *Firewall* ▪ Système de sauvegarde ▪ Système de stockage mutualisé ▪ Serveurs de proxy ▪ IDS/IPS
Compétences organisationnelles et physiques	
Cadre normatif	▪ Normes ISO/IEC 27001 et ISO 27002 ▪ Normes ISO 27005 ▪ Les textes réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes

Organisation de la sécurité des systèmes d'information	▪ Analyse des risques ▪ Politique de sécurité des systèmes d'information ▪ Fonctions 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
Méthodes associées à l'audit	▪ Conduite d'entretien ▪ Visite sur site ▪ Revue documentaire
Référentiel	
Référentiels techniques	▪ Référentiel d'exigences des prestataires d'audit ▪ Règles de cybersécurité en république togolaise, Annexe de l'arrêté N°2022-040 /PMRT portant adoption des règles de cybersécurité en république togolaise

2.3.2. Le prestataire est une personne physique

a. Le prestataire d'audit doit s'assurer du maintien à jour de ses compétences à travers un processus de formation continue et une veille technologique. A cet égard, le prestataire d'audit a l'obligation de suivre au minimum une (01) formation chaque année dans le domaine de la sécurité des systèmes d'information. La formation continue du prestataire d'audit peut prendre plusieurs formes notamment des modules d'auto-formation, des séminaires internes, ou des séminaires assurés par le CERT.tg ou par l'ANCy. La nature et la liste des formations validantes au titre de la formation continue du prestataire d'audit font l'objet d'une publication sur le site de l'ANCy. Le prestataire d'audit doit à tout moment être

en mesure de documenter son plan de formation continue à l'ANCy sur simple demande de celle-ci ;

b. Le prestataire doit disposer de guides de bonnes pratiques et des normes nécessaires aux activités d'audit menées. Il doit par ailleurs s'assurer qu'il est suffisamment sensibilisé à la règlementation en vigueur au Togo et applicable à ses missions ;

c. Le prestataire d'audit doit disposer de contrats d'une durée minimale d'un an renouvelable ou à durée indéterminée, ou d'un partenariat avec au moins deux experts ;

d. Le prestataire d'audit est responsable des méthodes, outils (logiciels ou matériels) et techniques qu'il utilise et de leur bonne utilisation (précautions d'usage, maîtrise de la configuration...). Il doit par ailleurs s'assurer de la mise à jour continue de ces méthodes, outils et techniques, ainsi que de leur pertinence à pouvoir répondre aux besoins des activités d'audit menées ;

e. Le prestataire d'audit doit justifier qu'il dispose des compétences techniques, théoriques et pratiques nécessaires pour mener les activités d'audit couvertes par la qualification obtenue.

f. Le prestataire doit disposer des compétences mentionnées dans le tableau du point 2.5 Section 2 ;

2.4. PROTECTION DE L'INFORMATION DU PRESTATAIRE D'AUDIT

Les informations sensibles liées aux audits, y compris les preuves, les conclusions et les rapports d'audit, doivent être protégés au minimum au niveau Diffusion Restreinte.

Le système d'information que le prestataire d'audit utilise pour le traitement de ces informations doit respecter les normes internationales et les bonnes pratiques relatives aux mesures de protection des systèmes d'information traitant d'information sensibles non classifiées de défense de niveau Diffusion Restreinte.

2.5. EXIGENCES RELATIVES AUX AUDITEURS

Éducation
Minimum Niveau Bac +3 et plus en technologies des systèmes d'information et de communication ou équivalent
Formation
Formation en opérations de cybersécurité
Expérience
Minimum 02 années d'expérience dans le domaine des systèmes d'information et de communication Dont 01 année d'expérience dans le domaine de la sécurité des systèmes d'information Et 01 année d'expérience dans l'activité de l'audit
Principales missions
- Réalisation des activités d'audit - Élaboration de rapports et proposition de recommandations
Les connaissances, compétences et aptitudes
↓ Analyse des risques, politique de sécurité des systèmes d'information ↓ Maîtrise des bonnes pratiques et de la méthodologie d'audit décrite dans la norme ISO 19011 ↓ Capacité à réaliser des audits conformément aux exigences relatives au déroulement d'une prestation d'audit ↓ Maitrise des normes relatives à la sécurité de l'information, Normes ISO/IEC 2700x, NIST, Cobit, Mehari, RGPD, etc... ↓ Connaissances des techniques organisationnelles approfondies nécessaires dans les activités d'audit

- Qualités rédactionnelles et de synthèse, notamment capacité à rédiger un rapport d'audit
- Qualités personnelles décrites au chapitre 7.2.2 de la norme ISO 19011
- Capacité de conseil et recommandation pour différents acteurs
- Capacité à pouvoir s'exprimer à l'oral de façon claire et compréhensible
- Mise à jour régulière des compétences par une veille active sur la méthodologie, les techniques ou les outils utilisés dans le cadre des missions.

3. EXIGENCES RELATIVES AU DEROULEMENT DE L'AUDIT

Les exigences auxquelles doivent se conformer les prestataires d'audit sont regroupées dans les différentes étapes du déroulement d'un audit qui sont :

- Établissement de la convention d'audit
- Préparation et déclenchement de l'audit
- Exécution de l'audit
- Élaboration du rapport d'audit
- Conclusion de l'audit

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

3.1. ÉTABLISSEMENT DE LA CONVENTION D'AUDIT

Préalablement à l'exécution de toute prestation d'audit, le prestataire d'audit doit établir une convention d'audit avec le Client final. Cette convention décrit les conditions et modalités selon lesquelles le prestataire d'audit fournira la prestation d'audit au Client final.

La convention d'audit doit être obligatoirement signée par le prestaire d'audit et le Client final préalablement au démarrage de la prestation d'audit.

Le prestataire d'audit assume la responsabilité de l'audit qu'il réalise pour le compte du Client final de l'audit et en particulier, des dommages éventuellement causés au cours de l'audit. Le prestataire d'audit et le Client

final de l'audit peuvent le cas échéant, préciser les modalités de partage des responsabilités au sein de la convention d'audit.

La convention d'audit établie entre le prestataire d'audit et le commanditaire de l'audit doit a minima contenir ou faire référence aux éléments suivants :

- L'indication que la prestation réalisée est une prestation qualifiée ;
- La mention de l'attestation de qualification du prestataire d'audit par l'ANCy, qui doit figurer en annexe de la convention d'audit ;
- La précision que le prestataire d'audit ne recourt pas à des auditeurs n'ayant pas de relation contractuelle avec lui, ou ayant fait/faisant l'objet d'une mesure ou d'une sanction incompatible avec l'exercice des missions d'audit.
- Le périmètre et les modalités de l'audit (jalons, livrables, objectifs, champs et critères de l'audit, méthodologie, lieux d'exécution de la prestation etc.) ;
- Les rôles et les responsabilités des différents intervenants dans la mission d'audit ;
- Une énonciation des risques liés à la prestation, notamment en matière de disponibilité lors de l'exploitation d'une faille décelée ;
- Les obligations et la responsabilité du prestataire d'audit, notamment l'information du Client final en cas de manquement à la convention d'audit ;
- Les aspects logistiques nécessaires au déroulement de l'audit (moyens matériels, humains, techniques) ;
- Le contenu des différents livrables, leurs destinataires, ainsi que leurs modalités de restitution ;
- L'obligation de confidentialité du prestataire d'audit, qui doit s'abstenir de divulguer ou partager des informations relatives à la prestation d'audit, sauf autorisation expresse écrite du Client final. ;
- Les conditions et modalités de conservation, de restitution ou de destruction en fin de mission ou à la date d'échéance de la durée de conservation, des informations ou documents relatifs au système d'information audité obtenus par le prestataire d'audit en cours de mission, à l'exception de celles pour lesquelles il a reçu une autorisation de conservation du Client final.
- Les règles de titularité des éléments protégés par la propriété intellectuelle, tels que les outils développés spécifiquement par le prestataire d'audit dans le cadre de sa mission ou le rapport d'audit.
- La précision que la convention d'audit est soumise au droit togolais.

Le prestataire d'audit peut sous-traiter une partie de l'audit demandé par le Client final de l'audit à un autre Prestataire d'audit qualifié qui se conforme aux exigences du présent Référentiel, ou avoir recours à un expert pour la réalisation de certaines activités spécifiques. La sous-traitance ou le recours à un expert ne peuvent cependant être réalisés que sous réserve du respect par le prestataire d'audit des conditions ci-après :

- Le prestataire d'audit qualifié sous-traitant se conforme aux exigences du présent Référentiel ;
- Le prestataire d'audit qualifié qui sous-traite la prestation notifie le projet d'accord de sous-traitance à l'ANCy dans un délai raisonnable avant la signature envisagée du contrat avec le sous-traitant ;
- Le recours à la sous-traitance est validé par le Client final ;
- Il existe une convention ou un cadre contractuel documenté entre le prestataire d'audit d'une part et le sous-traitant d'autre part ;
- Le sous-traitant ou l'expert est dûment encadré par le Responsable équipe de l'audit ;
- En aucun cas le sous-traitant ou l'expert ne se substitue à un auditeur.

Lorsque la sous-traitance est envisagée avec un prestataire ne bénéficiant pas d'une qualification délivrée par l'ANCy, les conditions suivantes devront être respectées :

- Le prestataire d'audit qualifié soumet le projet d'accord de sous-traitance à l'accord préalable de l'ANCy. Le projet devra être envoyé à l'ANCy dans un délai minimum de deux (02) mois avant la signature envisagée du contrat avec le sous-traitant ;
- Le recours à la sous-traitance est validé par le Client final ;
- Il existe une convention ou un cadre contractuel documenté entre le prestataire d'audit et le sous-traitant avant le début de l'exécution de sa mission par le sous-traitant.

3.2. PREPARATION ET DECLENCHEMENT DE L'AUDIT

Le prestataire d'audit désigne un Responsable de l'audit, qui doit constituer une équipe d'auditeurs pour les besoins de chaque mission. Les auditeurs retenus par le Responsable équipe de l'audit doivent disposer de compétences adaptées à la nature et la finalité de l'audit à mener.

Le Responsable de l'audit peut, s'il dispose des compétences suffisantes, réaliser l'audit lui-même et seul.

Le responsable équipe de l'audit doit dès le début de la préparation de l'audit, établir un contact avec le Client final en vue de mettre en place les canaux de communication, de collaboration et de décision. A cet égard, le Responsable équipe de l'audit obtient du Client final, une liste de points de contact et de personnes ressources nécessaires à la réalisation de la prestation, notamment la liste des entretiens qui seront conduits. La prise de contact par le Responsable équipe de l'audit vise également à préciser les modalités de la prestation à exécuter.

Le responsable de l'audit élabore un plan d'audit mentionnant le périmètre technique et organisationnel de la prestation, à savoir le planning, les dates et lieux où seront menées les activités d'audit et notamment celles qui auront lieu sur site et celles à distance, les informations générales sur les réunions d'ouverture et de clôture de la prestation, et sur les auditeurs constituant l'équipe d'audit.

Les objectifs, le champ, les critères et le planning de l'audit doivent être définis avec le Client final.

En fonction de l'activité d'audit, l'équipe d'auditeurs doit obtenir au préalable, toute la documentation existante. Dans le cas spécifique des tests d'intrusion, une fiche d'autorisation doit être signée par le Client final de l'audit et d'éventuelles tierces parties. Cette fiche d'autorisation doit préciser la liste des cibles auditées (adresses IP, noms de domaine, etc.), la liste des adresses IP de provenance des tests, les types de tests autorisés, la date et les heures exclusives des tests et la durée de l'autorisation.

Le prestataire d'audit doit, avant le début de la mission, sensibiliser le Client final sur l'intérêt de sauvegarder et préserver les données, applications et systèmes présents sur les machines auditées. L'audit ne doit débuter qu'après une réunion formelle de lancement de la mission au cours de laquelle les représentants habilités du prestataire d'audit et du Client final de l'audit confirment leur accord sur l'ensemble des modalités de la prestation.

3.3. EXECUTION DE L'AUDIT

3.3.1. Conduite de l'audit

La mission d'audit doit être réalisée en respectant les exigences suivantes :

- **Respect du règlement intérieur du Client final**

  Le prestataire d'audit doit respecter les règles et consignes découlant du règlement intérieur du Client final de l'audit, et examiner tous les contrats et les accords, expresses ou implicites.

- **Ressources requises pour l'audit**

  Le prestataire d'audit doit demander toutes les ressources requises pour l'exécution de la mission (documents, habilitations, logistiques, liste des entretiens etc.), en particulier le rapport d'audit précédent s'il existe, comme mentionné en ANNEXE 1 intitulé « Documents requis pour la revue » ;

  À cet effet, le prestataire d'audit fait mention dans le rapport d'audit, de toute ressource ou information demandée au Client final et non transmise par celui-ci. Le prestataire d'audit précise également dans quelle mesure cette abstention influe sur la qualité des résultats de l'audit.

- **Déroulement des entretiens**

  Le prestataire d'audit veille à réaliser des entretiens avec le personnel selon la nature de l'audit réalisé en vue de vérifier les points de contrôle par rapport, aux spécificités organisationnelles, fonctionnelles ou techniques du périmètre audité.

- **Équipe intervenante**

  Le prestataire d'audit veille, pour toute mission conduite sous sa supervision, à présenter au Client final de l'audit lors de la réunion de lancement de la mission, l'équipe intervenante ainsi que les postes auxquels sont affectés chaque membre. Toute modification de la composition de l'équipe d'audit doit être expressément approuvée par écrit par le Client final de l'audit.

- **Périmètre de l'audit**

  Le prestataire d'audit :

  - Veille à définir clairement le périmètre de l'audit avec le Client final, et s'assure que tout changement dans le périmètre convenu soit préalablement approuvé par celui-ci.
  - Veille pendant l'exécution de la mission, à examiner toutes les composantes du périmètre de l'audit, suivant la méthodologie d'audit approuvée par le Client final.
  - Ne procède à l'échantillonnage qu'à la suite de l'approbation par le Client final de la méthode d'échantillonnage.

- **Plan d'audit**

  Le prestaire d'audit :

  - Prépare un plan d'audit détaillant la nature, les objectifs, le calendrier, l'étendue et les ressources nécessaires pour l'audit, en particulier les tests intrusifs, conformément à ce qui a été convenu avec le Client final au cours de la réunion de lancement de la mission.

- Veille à respecter le plan d'audit, en particulier les interventions sur le terrain.
- Veille à appuyer chaque intervention sur le terrain par un Procès-verbal signé par l'ensemble des personnes impliquées.

➢ **Normes, méthodologie et outils d'audit utilisés**

Le prestataire d'audit :

- Adopte une méthodologie d'audit (organisationnel, physique, technique, analyse de risque) adaptée à l'entité auditée, s'engage à la respecter, et veille à l'indiquer dans le rapport d'audit. La méthodologie d'audit proposée par le prestataire d'audit est validée avec le Client final ;
- En vue de proposer une méthodologie d'audit adaptée à la mission à conduire, le prestataire d'audit prend en compte aussi bien les critères d'audit que les risques encourus par le périmètre audité en vue d'évaluer le niveau de conformité et/ou de sécurité attendu dans le cadre de l'audit ;
- Veille à utiliser les outils de tests les plus adaptés pour chaque système cible et à utiliser des versions mises à jour ;
- Veille en fin de mission, à ce que l'état de sécurité du système d'information audité ne soit pas dégradé par rapport à l'état initial.

➢ **Constats de l'audit**

Le prestataire d'audit :

- Présente des constats fiables et pertinents, formulés clairement, de manière synthétique et sans équivoque, et qui doivent être perçus comme tels par toute tierce personne avertie ;
- Documente, et trace ses constats, sur la base de preuve ;
- Évite de limiter ses constats uniquement aux résultats de la revue documentaire ou aux résultats bruts des rapports générés par les outils de tests automatisés de vulnérabilités ;
- S'abstient de répondre au questionnaire d'audit par soi-même si l'interviewé est absent ou ne donne pas de réponse claire lors des entretiens en préparation de l'audit.

3.3.2. Travaux de l'audit

Les travaux d'audit spécifiques à chaque secteur comprennent des examens détaillés qui sont réalisés grâce à la mise en œuvre des contrôles de sécurité spécifiques. Ces différents contrôles de sécurité sont organisés et classifiés en fonction de leurs types.

3.3.2.1. Types de contrôles de sécurité

Les contrôles de sécurité se déclinent en quatre grands types, à savoir :

- **Les contrôles de sécurité organisationnels**

Ces contrôles sont liés aux politiques, procédures, et à la gestion globale de la sécurité de l'information au sein d'une organisation. Ils concernent des aspects tels que la sensibilisation à la sécurité, la formation du personnel, la gestion des risques, la planification de la continuité des activités, la gouvernance de la sécurité, etc.

- **Les contrôles de sécurité applicables aux personnes**

Ces contrôles visent à assurer que les individus au sein de l'organisation sont conscients des pratiques de sécurité et qu'ils les suivent, notamment l'éducation à la sécurité, la gestion des identités et des accès, l'application de politiques de sécurité, la surveillance des activités des utilisateurs, etc.

- **Les contrôles de sécurité physique**

Ces contrôles se concentrent sur la protection des infrastructures physiques de l'organisation à savoir la sécurité des locaux, la gestion des accès physiques, la surveillance par caméra, la protection contre les incendies et les catastrophes naturelles, la gestion des équipements, etc.

- **Les contrôles de sécurité technologiques**

Ces contrôles concernent la sécurisation des systèmes informatiques et des réseaux. Ils incluent la gestion des *firewalls*, des antivirus, des systèmes de détection d'intrusion, la gestion des vulnérabilités, le chiffrement des données, la gestion des correctifs, etc.

Activités de l'audit	Types de contrôles de sécurité
Audit organisationnel	Contrôles de sécurité organisationnels Contrôles de sécurité applicables aux personnes
Audit physique et environnemental	Contrôles de sécurité physique
Audit des architectures	Contrôles de sécurité technologiques
Audit des configurations	Contrôles de sécurité technologiques
Audit de code source	Contrôles de sécurité technologiques
Audits intrusifs	Contrôles de sécurité technologiques
Audit des systèmes industriel SCADA	Contrôles de sécurité technologiques

Les activités d'audit réalisées par l'équipe d'audit doivent être conformes aux modèles de vérification précisés dans L'ANNEXE 2 intitulé « Contrôles de sécurité selon la norme ISO/IEC 27002 :2022 ».

3.3.2.2. Notifications et communications spécifiques durant l'audit

Le Responsable équipe de l'audit doit tenir informé le Client final des vulnérabilités critiques découvertes au cours de l'audit. Il doit rendre compte immédiatement au Client final de tout élément constaté présentant un risque immédiat et significatif, et dans la mesure du possible, lui proposer des mesures permettant d'atténuer ce risque.

Le Responsable équipe de l'audit doit par ailleurs agir en toute transparence avec le Client final, et l'informer à temps de toute action sur son système d'information, en particulier de toute brèche de sécurité observée, même si le système cible n'est pas couvert par le périmètre de l'audit.

3.4. ÉLABORATION DU RAPPORT D'AUDIT

Pour chaque audit mené, le prestataire d'audit doit préparer un rapport d'audit adapté selon l'activité spécifique réalisée.

Le rapport d'audit doit a minima contenir :

a. L'indication que la prestation réalisée est une prestation qualifiée.
b. Les activités réalisées dans le cadre de l'audit.

c. **Une synthèse de la mission menée** précisant :

- Le contexte et le périmètre de l'audit ;
- 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'Etat de l'art et en considération du périmètre d'audit.

Cette synthèse doit être compréhensible par des non experts.

d. **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 ;

e. **Une description du déroulement** linéaire des tests et de la méthodologie employée pour détecter les vulnérabilités et, le cas échéant, les exploiter (dans le cas des tests d'intrusion) ;

f. Une analyse de la sécurité du système d'information du Client final, qui présente les résultats des différentes activités d'audit réalisées ;

g. Les vulnérabilités identifiées 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. Le prestataire peut proposer une échelle pertinente ou le cas échéant se baser sur la norme ISO 27005.Chaque vulnérabilité et non-conformité identifiée doit être associée à une ou plusieurs recommandations. Les recommandations décrivent les solutions permettant de résoudre une vulnérabilité ou une non-conformité et d'améliorer le niveau de sécurité ;

Ces recommandations doivent être proportionnées, adaptées à la cible de l'audit, réalistes, non ambiguës et priorisées.

Les critères suivants doivent notamment être pris en compte ou estimés par le prestataire d'audit : mesures de corrections immédiates, recommandation de mesures d'amélioration en continue ou de minimisation de reconduction de la vulnérabilité, complexités de mise en œuvre.

h. Il est recommandé que le rapport d'audit présente également 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.

i. Le rapport doit contenir les noms et coordonnées des membres de l'équipe qui ont effectivement participé aux travaux d'audit.

3.5. CONCLUSION DE L'AUDIT

À l'issue de l'audit, une réunion de clôture est organisée entre le prestataire d'audit et le Client final subséquemment à la transmission 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 de la suite à donner à la prestation (audit de contrôle). Elle est également l'occasion d'expliquer les recommandations complexes et, éventuellement, de proposer d'autres solutions plus aisées à mettre en œuvre. Elles peuvent permettre de répondre aux questions résiduelles du Client final.

La réunion de clôture de l'audit donne lieu à la rédaction d'un Procès-verbal, qui précise si toutes les traces d'audit, les relevés de l'audit et ceux relatifs au système d'information audité, obtenus par le prestataire d'audit pendant la mission, ont été restitués au Client final ou, sur la demande de ce dernier, détruits conformément à la convention d'audit.

Le responsable équipe de l'audit doit demander au Client final 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.

Le prestataire doit recommander au Client final d'effectuer ultérieurement un audit de contrôle dit post-audit afin de vérifier si les mesures correctives proposées lors de l'audit ont été correctement mises en œuvre.

Un audit de contrôle est un audit complémentaire à l'audit initial et permettant d'évaluer si la sécurité du système d'information s'est améliorée suite à celui-ci. Cet audit permet également d'établir un statut de la correction des non-conformités ou vulnérabilités identifiées lors de l'audit initial. L'audit de contrôle ne se substitue pas à des audits supplémentaires et n'est pas suffisante à elle seule : l'audit de contrôle n'a pour objectif que de les compléter.

L'audit est considéré comme terminé lorsque toutes les actions planifiées ont été exécutées et que le Client final de l'audit a reçu et validé la conformité du rapport d'audit aux objectifs stipulés dans la convention d'audit.

ANNEXE 1 : DOCUMENTS REQUIS POUR LA REVUE

Les documents requis pour la revue dans le cadre d'un audit sont, sans s'y limiter :

- L'ensemble des politiques de sécurité de l'information du Client final de l'audit, approuvées par la direction ;
- Le manuel de procédures relatif à la sécurité de l'information, qui doit inclure au minimum les procédures suivantes :
  - La procédure de mise à jour des documents de politiques de sécurité et des procédures ;
  - La procédure d'attribution des responsabilités au sein de l'organisation de l'entité auditée ;
  - La procédure d'autorisation pour l'ajout d'outils de traitement de l'information
  - La procédure de classification des actifs ;
  - Les procédures de sécurité physique (contrôle des accès physiques, sécurité des équipements hors des locaux, mise au rebut des équipements, etc.) ;
  - La procédure de développement, de test et de déploiement des applications ;
  - La procédure de gestion des ressources par des tiers ;
  - La procédure de protection contre les logiciels malveillants ;
  - La procédure de sauvegarde et de restitution des données ;
  - La procédure de gestion du courrier électronique ;
  - La procédure de gestion des accès logiques (aux réseaux, aux systèmes, aux applications) ;
  - La procédure de gestion des changements ;
  - La procédure de gestion des incidents ;
  - Les procédures de gestion de la continuité des activités ;
- Les fiches de poste du RSSI et des autres employés en relation avec la sécurité du système d'Information ;
- La matrice de flux des données ;
- Les schémas d'architecture du système d'information ;
- L'inventaire du matériel et logiciel informatique

ANNEXE 2 : CONTROLES DE SECURITE SELON LA NORME ISO/IEC 27002 : 2022

Réf ISO 27002	Titre Domaine /Contrôle	Description	Vérifications à effectuer	Moyen de vérification (sans s'y limiter)	Preuves
5	Contrôles de sécurité organisationnels				
5.1	Politiques de sécurité de l'information	Une politique de sécurité de l'information et des politiques spécifiques doivent être définies, approuvées par l'organe de direction de l'entité auditée, publiées, et communiquées au personnel ainsi qu'aux parties intéressées concernées avec demande de confirmation. Ces politiques doivent être révisées à intervalles planifiés et en cas de besoin, lorsqu'interviennent des changements significatifs.	• S'il existe un document de Politique de Sécurité de l'Information (PSI) approuvé par l'organe de direction de l'entité auditée ; • Si tout changement apporté à la PSI est approuvé par la direction ; • Si la PSI est renforcée par des politiques spécifiques complémentaires ; • Si la responsabilité du développement, de la révision et de l'approbation des politiques spécifiques est attribuée au personnel approprié en fonction de son niveau d'autorité et de sa compétence technique ; • Si la PSI et les politiques spécifiques sont publiées et communiquées au personnel et aux parties intéressées concernés ; • S'il est exigé des destinataires des politiques de sécurité de confirmer leur compréhension de ces politiques et accepter de s'y conformer lorsqu'elles sont applicables ; • Si la PSI est passée en revue par un comité de sécurité de haut niveau à intervalles planifiés ou en cas de survenance de changements significatifs, en vue de s'assurer que la PSI et les politiques spécifiques sont toujours pertinentes, adéquates et efficaces.	• Revue des documents de la PSI et des politiques spécifiques ; • Entretien avec le représentant légal de l'entité auditée ; • Interviews d'un échantillon d'utilisateurs ; • Revue des Procès-Verbaux de réunions du comité de sécurité.	• Document de PSI approuvé par la DG ; • Documents de politiques spécifiques approuvés par le niveau de direction approprié ; • Échantillon de décharges (ou courriers électroniques) attestant que les utilisateurs ont reçu une copie de la PSI et des politiques spécifiques applicables, avec confirmation de leur compréhension de des politiques ainsi transmises et acceptation de s'y conformer ; • Historique des mises à jour de la PSI et des politiques spécifiques ; • Procès-Verbaux des réunions du comité de sécurité sur la mise à jour de la PSI.

5.2	Fonctions et responsabilités liées à la sécurité de l'information	Les fonctions et les responsabilités liées à la sécurité de l'information doivent être définies et attribuées selon les besoins de l'entité auditée.	• Si un RSI doté d'un pouvoir décisionnel et assurant le reporting directement à l'organe de direction de l'entité auditée est désigné ; • Si un comité de sécurité est mis en place ; • Si les rôles et les responsabilités liés à la sécurité de l'information sont bien définis et attribués à des individus ayant les compétences requises.	• Revue de l'organigramme, des fiches de postes, des décisions et notes internes en relation avec la sécurité du SI ; • Entretien avec le représentant légal ; • Interview du RSSI (le cas échéant).	• Décision de nomination du RSSI ; • Décision de mise en place du comité de sécurité ; • PVs de réunions du comité de sécurité ; • Fiches de postes.
5.3	Séparation des tâches	Les tâches et les domaines de responsabilité incompatibles doivent être cloisonnés afin d'éviter qu'une personne ne puisse réaliser seule des tâches potentiellement incompatibles.	• Si les tâches qui nécessitent d'être séparées sont identifiées et les responsabilités attribuées en conséquence ; • Si une tâche de vérification régulière de la définition et de l'attribution des responsabilités est prévue et réalisée ; • Si des contrôles compensatoires sont mis en place en cas d'attribution des tâches incompatibles à la même personne.	• Revue des fiches de postes ; • Entretiens avec les responsables des services métier pour l'identification des taches incompatibles ; • Revue des procédures internes qui identifient les tâches incompatibles ; • Vérification des droits d'accès sur les systèmes qui hébergent ou traitent les services métier concernés ; • Vérification des contrôles compensatoires en cas d'attribution de tâches incompatibles à la même personne.	• Fiches de postes ; • Compte rendu de vérification de la définition et de l'attribution des responsabilités.
5.4	Responsabilités de l'organe de direction de l'entité auditée	L'organe de direction doit s'assurer de l'application par tout le personnel, des mesures de sécurité de l'information, conformément à la politique de sécurité de l'information, aux politiques spécifiques et aux procédures établies de l'entité auditée.	• Si l'organe de direction exige explicitement (par une note interne signée par le représentant légal) que le personnel applique les exigences de sécurité conformément à la politique de sécurité de l'information, aux politiques spécifiques et aux procédures établies par l'audité.	• Revue de la note interne signée par le représentant légal ; • Entretien avec le représentant légal ; • Interview du Directeur des Ressources Humaines (DRH) et du Directeur des Affaires Financières (DAF).	• Note interne signée par le représentant légal.

5.5	Contacts avec les autorités	Le contact avec les autorités appropriées doit être établi et maintenu.	• Si les autorités avec lesquelles l'entité auditée peut collaborer en matière de sécurité de l'information sont identifiées ; • Si une liste mise à jour de contacts de ces autorités est maintenue ; • Si une procédure d'échanges entre l'entité auditée et ces autorités est définie et mise en œuvre.	• Revue de la liste des autorités ; • Revue de la procédure d'échanges entre l'entité auditée et les autorités ; • Entretiens avec les responsables des différents services pour l'identification des autorités compétentes.	• Liste mise à jour des contacts des autorités avec lesquelles l'entité auditée peut collaborer ; • Procédure d'échanges entre l'entité auditée et les autorités concernées. • Supports de communication utilisés (Courriers, Emails, PVs de réunions, etc...).
5.6	Contacts avec des groupes d'intérêt spécifiques	Des contacts avec des groupes d'intérêt spécifiques, des forums spécialisés dans la sécurité et des associations professionnelles doivent être établis et maintenus.	• Si des groupes d'intérêt, des forums spécialisés dans la sécurité et des associations professionnelles ont été identifiés ; • Si des contacts sont établis et maintenus avec ces groupes, forums et associations ; • Si des accords de partage d'informations ont été établis pour améliorer la coopération et la coordination en matière de sécurité.	• Revue des accords éventuels établis avec les groupes d'intérêt, les forums et les associations. • Interview du RSSI pour l'identification de ces groupes et les contacts éventuels établis et maintenus avec eux.	• Abonnement à des mailing lists des constructeurs de produits utilisés et d'institutions spécialisées dans le domaine de la sécurité de l'information, • Participation à des workgroups, • Échanges de retour d'expérience ; • Accords établis avec les groupes.
5.7	Renseignements sur les menaces	Les informations relatives aux menaces de sécurité de l'information doivent être collectées et analysées pour produire les renseignements sur les menaces.	• Si des objectifs sur la production de renseignements sur les menaces sont définis et établis ; • Si les sources d'information internes et externes nécessaires pour la production de renseignements sur les menaces sont identifiées ; • Si les informations sur les menaces existantes et émergentes sont collectées, analysées, communiquées aux personnes appropriées et exploitées ; • Si les informations collectées auprès des sources de renseignements sur les menaces sont intégrées dans les processus de gestion des risques de la sécurité de l'information de l'entité auditée.	• Revue du document des objectifs sur la fourniture de renseignements relatifs aux menaces ; • Revue de la liste des sources d'information sur les renseignements relatifs aux menaces ; • Revue des abonnements ou des contrats avec les fournisseurs de renseignements sur les menaces ; • Vérification de l'intégration des informations sur les	• Document des objectifs sur la fourniture des renseignements relatifs aux menaces ; • Liste des sources d'information sur les renseignements relatifs aux menaces ; • Les abonnements et les contrats avec les fournisseurs de renseignements sur les menaces ; • Document de gestion des risques ;

				menaces dans les processus de gestion des risques ; • Revue d'un échantillon des informations sur les menaces ; • Interview du DSI et du RSSI.	• Un échantillon des informations sur les menaces.
5.8	Sécurité de l'information dans la gestion de projets	La sécurité de l'information doit être intégrée dans la gestion de projets.	• Si une analyse des risques liés à la sécurité de l'information est effectuée à un stade précoce du projet afin d'identifier les contrôles de sécurité nécessaires, puis périodiquement en fonction des risques du projet, tout au long du cycle de vie du projet ; • Si l'avancement et l'efficacité du traitement des risques de sécurité de l'information sont contrôlés lors de la gestion de projet ; • Si les responsabilités et autorités en matière de sécurité de l'information appropriées au projet sont définies et attribuées à des fonctions précises ; • Si les exigences de sécurité de l'information pour les produits ou services qui doivent être livrés par le projet sont déterminées ; • Si les exigences de sécurité de l'information sont déterminées pour tous les types de projets, et pas seulement les projets de développement de TIC.	• Revue du document d'analyse des risques ; • Revue des documents des projets et vérification de la prise en compte des besoins de sécurité ; • Revue des PVs des réunions des équipes de projets ; • Interview du RSSI ; • Interviews des responsables métier et des chefs de projets ; • Revue des cahiers des charges des projets ; • Revue des critères d'acceptation des produits.	• Document d'analyse des risques ; • Documents de projets contenant l'expression des besoins de sécurité ; • Procédure de gestion des projets en matière de sécurité de l'information ; • Procédure de gestion des projets (volet en relation avec la sécurité de l'information) ; • PVs des réunions des équipes de projets, cahiers des charges des projets, critères d'acceptation des produits.
5.9	Inventaire des informations et autres actifs associés	Un inventaire des informations et autres actifs associés, y compris leurs propriétaires doit être élaboré et tenu à jour.	• S'il existe des règles relatives à l'inventaire des actifs au niveau de la PSI, qui exigent le maintien d'un inventaire des actifs ; • Si des procédures d'inventaire des actifs sont développées et maintenues ; • Si un inventaire ou registre est maintenu pour les informations et autres actifs associés de l'entité auditée et si leur importance en termes de sécurité de l'information est déterminée ; • Si la propriété d'actif est attribuée à une personne ou à un groupe pour les informations et autres actifs associés identifiés.	• Revue de la PSI pour l'identification des règles relatives à l'inventaire ; • Revue des procédures d'inventaire des actifs ; • Revue de l'inventaire et vérification de son exhaustivité, vérification de l'existence du nom du propriétaire pour les informations et autres actifs associés identifiés. • Interview du DAF ;	• PSI ; • Procédures d'inventaire ; • Inventaire des informations et autres actifs associés.

				• Interview du DSI.	
5.10	Utilisation correcte des informations et autres actifs associés	Les règles d'utilisation correcte et les procédures de traitement des informations et autres actifs associés doivent être identifiées, documentées et mises en œuvre.	• Si une politique spécifique à l'utilisation correcte des informations et autres actifs associés est élaborée, mise en œuvre et communiquée à toute personne qui utilise ou traite les informations et autres actifs associés ; • Si le personnel et les utilisateurs externes ont été sensibilisés aux exigences de sécurité comprises dans cette politique et de leur responsabilité de l'utilisation de tout moyen de traitement de l'information ; • Si des procédures d'utilisation correcte des informations et des actifs associés, en fonction de leur classification et des risques déterminés, sont élaborées et mises en œuvre.	• Revue de la politique spécifique à l'utilisation correcte des informations et autres actifs associés ; • Revue des procédures d'utilisation correcte des informations et des actifs associés ; • Revue d'un échantillon de contrats avec les sous-traitants ayant l'accès aux moyens de traitement de l'information ; • Interviews du RSSI et du DSI ; • Interviews du DRH et du DAF ; • Interviews des responsables métier.	• Politique spécifique à l'utilisation correcte des informations et autres actifs associés ; • Procédures d'utilisation correcte des informations et des actifs associés ; • Échantillon de contrats avec les sous-traitants ayant accès aux moyens de traitement de l'information.
5.11	Restitution des actifs	Le personnel et les autres parties intéressées doivent restituer tous les actifs de l'entité auditée qui sont en leur possession au moment du changement ou à la fin de leur emploi, contrat ou accord.	• Si la restitution des actifs en possession du personnel et des autres parties intéressées au terme de la période de l'emploi, du contrat ou de l'accord est documentée ; • Si pendant la période de préavis et ultérieurement, l'entité auditée contrôle la copie non autorisée des informations pertinentes (par exemple en matière de propriété intellectuelle) par le personnel ayant notifié le préavis ou notifié du préavis.	• Revue des documents relatifs aux fins de période de l'emploi et des contrats des sous-traitants (ex : PVs de passation, PVs de réceptions définitives, etc.) ; • Revue des contrôles mis en place pour empêcher les copies non autorisées des informations pertinentes pendant et après la période de préavis de fin de contrat des employés, des sous-traitants, ou toute autre partie intéressée ; • Interviews du DRH et du DAF.	• PVS de passation au terme de la période d'emploi, PVS de réception définitive ; • Liste de contrôles interdisant les copies non autorisées des informations pertinentes pendant et après la période de préavis de fin de contrat des employés, des sous-traitants, ou toute autre personne intéressée.

5.12	Classification des Informations	Les informations doivent être classifiées conformément aux besoins de sécurité de l'information de l'entité auditée en termes d'exigences de confidentialité, d'intégrité, de disponibilité et des exigences importantes des parties intéressées.	• Si une politique spécifique à la classification des informations est établie et communiquée aux parties intéressées concernées ; • Si le schéma de classification tient compte des exigences de confidentialité, d'intégrité et de disponibilité sur la base des besoins métier et des exigences légales ; • Si les actifs autres que les informations sont classifiées conformément à la classification des informations qu'ils stockent, traitent ou manipulent, ou qu'ils protègent ; • Si des mesures de sécurité spécifiques à chaque classe d'informations sont appliquées en concordance avec le système de classification.	• Revue de politique spécifique à la classification des informations ; • Interview des responsables métier ; • Vérification des mesures de sécurité sur un échantillon d'informations classifiées critiques.	• Politique spécifique à la classification des informations ; • État sur les mesures de sécurité appliquées.
5.13	Marquage des informations	Un ensemble approprié de procédures pour le marquage des informations doit être élaboré et mis en œuvre conformément au schéma de classification adopté par l'entité auditée.	• Si des procédures de marquage de l'information conformément au schéma de classification établi sont élaborées et mises en œuvre.	• Revue des procédures de marquage des informations ; • Interview des responsables métier ; • Vérification de marquage sur un échantillon de documents.	• Procédures de marquage des informations ; • Échantillon de documents.
5.14	Transfert des informations	Des règles, procédures ou accords sur le transfert des informations doivent être mis en place pour tous types de moyens de transferts au sein de l'entité auditée et entre l'entité auditée et des tierces parties.	• Si une politique spécifique au transfert des informations est établie, mise en œuvre et communiquée à toutes les parties intéressées. • Si cette politique couvre tous les types de transferts d'informations : transfert électronique, transfert sur support de stockage physique et transfert verbal ; • Si des accords de transfert sont définis et maintenus lorsque les informations sont transférées entre l'entité auditée et des tierces parties ; • Si les règles, procédures et accords visant à protéger les informations en transit incluent : - les mesures nécessaires pour protéger l'information transférée contre l'interception, l'accès non autorisé, la copie, la modification, les erreurs d'acheminement, la destruction et le déni de service ; - des mesures pour assurer la traçabilité et la non-répudiation telle que le maintien d'une chaîne de traçabilité pour l'information en transit ; - l'utilisation des techniques de cryptographie pour	• Revue de la politique spécifique au transfert des informations ; • Revue des accords et des procédures liés au transfert sécurisé des informations ; • Revue de la procédure propre à la messagerie électronique définissant les précautions d'emploi et les mesures de sécurité à mettre en œuvre ; • Revue des programmes de sessions de sensibilisation réalisées et de leurs bénéficiaires ; • Interviews des responsables métier, du DSI et des administrateurs	• Politique spécifique au transfert des informations, • Accords et procédures liés au transfert des informations, • Procédure propre à la messagerie électronique, • Programmes de sessions de sensibilisation réalisées et bénéficiaires, • Document d'identification des obligations et des responsabilités en cas d'incident lié au transfert des informations, • Rapports de traitement des incidents liés au transfert des informations, • Échantillon de courriers électroniques transférant

			protéger la confidentialité, l'intégrité et l'authenticité des informations sensibles ; - les obligations et les responsabilités en cas d'incident de sécurité de l'information, comme la perte de supports de stockage physiques ou de données ; - l'utilisation d'un système de marquage convenu pour les informations sensibles, la fiabilité et la disponibilité du service de transfert ; - toute mesure particulière qui découle du niveau de classification des informations impliquées ; - la prise en compte des questions juridiques en lien avec le transfert des informations, comme les exigences en matière de signatures électroniques ; • Si les règles, procédures et accords, en cas d'un transfert électronique, prennent également en compte les éléments suivants : - détection et protection contre les logiciels malveillants qui peuvent être transmis via l'utilisation des communications électroniques ; - protection des informations électroniques sensibles communiquées sous forme de pièces jointes comme l'utilisation des techniques de cryptographie ; - des restrictions associées aux moyens de communication électronique, comme le renvoi automatique de courriers électroniques vers des adresses électroniques extérieures, sont mises en place ; - obtention d'une approbation avant d'utiliser des services publics externes tels que les messageries instantanées, les réseaux sociaux, le partage de fichiers ou le stockage en nuage ; - niveaux renforcés d'authentification lors du transfert des informations via des réseaux accessibles au public ; • Si une procédure propre à la messagerie électronique définissant les précautions d'emploi et les mesures de sécurité à mettre en œuvre est élaborée et mise en œuvre ; • Si le personnel et les autres parties intéressées sont sensibilisés, en cas d'un transfert de ne pas tenir de	système et réseau • Interview d'un échantillon d'utilisateurs ; • Revue du document d'identification des obligations et des responsabilités en cas d'incident lié au transfert des informations ; • Revue des rapports de traitement des incidents liés au transfert des informations ; • Vérification des mesures de sécurité mises en place pour la protection des messages ; • Vérification sur un échantillon de courrier électronique de l'utilisation du cryptage des pièces jointes contenant de l'information sensible ; • Vérification des mesures de sécurité sur un échantillon de postes de travail (connexion à la messagerie par mot de passe non enregistré, etc.).	des pièces jointes, • Captures d'écran.

			conversations confidentielles dans des lieux publics ou via des canaux de communication non sécurisés. A cet égard, ces personnes doivent s'assurer que des mesures de sécurité appropriées sont mises en œuvre dans les lieux où interviennent ces échanges (portes de salles fermées, insonorisation, ...), et veillent à démarrer toute conversation sensible par un avertissement concernant le niveau de classification des informations communiquées oralement.		
5.15	Contrôle d'accès	Des règles visant à contrôler l'accès physique et logique aux informations et autres actifs associés en fonction des exigences métier et de sécurité de l'information, doivent être définis et mises en œuvre.	• Si les exigences métier et de sécurité de l'information relatives au contrôle d'accès sont déterminées par les propriétaires des informations et autres actifs associés ; • Si les entités qui nécessitent un type d'accès défini aux informations et autres actifs associés sont bien déterminées (selon « **le besoin d'en connaître** » et « **le besoin d'utiliser** » ; • Si une politique de contrôle d'accès dans le cadre de la politique de sécurité de l'information de l'entité auditée est élaborée et mise en œuvre en prenant en compte les points précédents ; • Si cette politique de contrôle d'accès est appuyée par des procédures de contrôle d'accès aux différents systèmes ; • Si la classification des informations a eu lieu ; • Si les droits d'accès sont cohérents avec la classification des informations ; • Si les fonctions de contrôle d'accès (ex : la demande d'accès, l'autorisation d'accès et l'administration des accès) sont séparées ; • Si les accès nécessaires pour chaque entité selon le principe du « **moindre privilège** » sont identifiés ; • Si les rôles et les responsabilités de chaque entité dans l'attribution de ces accès sont définis ; • Si les approbations sont définies et révisées régulièrement ; • Si les tâches sont séparées.	• Revue de la politique de contrôle d'accès ; • Revue des procédures de contrôle d'accès aux différents systèmes ; • Interviews des responsables métiers pour : - l'identification des exigences métier et de sécurité de l'information relatives au contrôle d'accès des entités qui nécessitent un type d'accès défini et les rôles des propriétaires des informations ; - l'identification des risques d'accès non autorisé à ces entités. • Revue de la procédure de contrôle d'accès au réseau et vérification de sa conformité avec la politique de contrôle d'accès ; • Revue du diagramme des flux réseau pour l'identification des entités pouvant avoir accès, et les accès nécessaires pour chacune d'elle selon le principe du « **moindre privilège** » ;	• Inventaire des informations, leurs propriétaires, les entités qui ont besoin des accès à ces informations et leurs rôles ; • Document d'identification des risques d'accès non autorisé à ces informations ; • Politique de contrôle d'accès ; Procédures de contrôles d'accès, • Diagramme des flux réseau ; • Document d'identification des rôles et des responsabilités de chaque entité dans l'attribution des accès au réseau ; • Document de définition des rôles et des responsabilités de chaque entité dans l'attribution de ces accès ; • ACL sur les équipements réseau et de sécurité ; • Procédure de contrôle d'accès au réseau.

				• Revue de la définition des rôles et des responsabilités de chaque entité dans l'attribution de ces accès ; • Revue des ACL sur les équipements réseau et de sécurité (Switchs, routeurs, firewalls, ...) ; • Interview de l'administrateur réseau.	
5.16	Gestion des identités	Le cycle de vie complet des identités doit être géré.	• Si un processus de gestion des identités est défini, documenté et mis en œuvre ; • Si les identités attribuées aux personnes sont uniques pour tenir la personne responsable des actes effectués sous cette identité spécifique ; • Si l'utilisation d'identifiants partagés n'est autorisée que lorsqu'elle est nécessaire pour des raisons métier ou opérationnelles et si elle est approuvée et documentée ; • Si les identités attribuées à des entités non humaines sont approuvées et surveillées d'une manière continue ; • Si les identités non utilisées sont désactivées ou supprimées (par exemple si les entités associées sont supprimées ou ne sont plus utilisées, ou si la personne liée à une identité a quitté l'entité auditée ou a changé de fonction) ; • Si les évènements liés à la gestion des identités et les informations d'authentification sont conservés ; • Si les identités des tierces parties fournissent le niveau de confiance requis et que tout risque associé est identifié et suffisamment traité ; • Si une procédure de gestion des accès est définie et mise en œuvre ; • Si les identifiants utilisateurs redondants sont périodiquement identifiés et supprimés ou désactivés.	• Revue du processus de gestion des identités ; • Vérification des comptes utilisateurs sur les serveurs pour l'identification de ceux qui sont partagés, redondants ou obsolètes ; • Revue des évènements d'authentification ; • Revue de la procédure de gestion des accès ; • Interview de l'administrateur systèmes, BD et réseaux.	• Document du processus de gestion des identités ; • Liste des comptes utilisateurs sur les serveurs ; • Document de revue des accès ; • Log des serveurs ; • Procédure de gestion des accès.

5.17	Informations d'authentification	L'attribution et la gestion des informations secrètes d'authentification doivent être contrôlées par un processus de gestion incluant des recommandations au personnel sur l'utilisation appropriée des informations d'authentification.	• Si un processus de gestion formel est mis en œuvre pour l'attribution des informations secrètes d'authentification ; • Si les utilisateurs sont tenus de signer un engagement pour garder confidentielles les informations secrètes d'authentification (cet engagement signé peut être inclus dans les conditions d'emploi) ; Si les informations secrètes d'authentification temporaire sont fournies aux utilisateurs de manière sécurisée (l'utilisation de parties externes ou de messages électroniques non protégés (en texte clair) doit être évitée) ; • Si les utilisateurs signent un accusé de réception des informations secrètes d'authentification ; • Si les informations secrètes d'authentification par défaut des fournisseurs des systèmes ou des logiciels sont modifiées après leur l'installation ; • Si tous les utilisateurs sont sensibilisés et invités à : - garder confidentielles les informations secrètes d'authentification, en veillant à ce qu'elles ne soient pas divulguées à d'autres parties, y compris à leurs supérieurs hiérarchiques ; - éviter de conserver un enregistrement d'informations secrètes d'authentification (par exemple sur du papier, un fichier logiciel ou un appareil portatif), sauf si cela peut être stocké de manière sécurisée et si la méthode de stockage a été approuvée (par exemple, coffre-fort) ; - changer les informations secrètes d'authentification chaque fois qu'il y a un soupçon de sa compromission ; - ne pas partager ses propres informations secrètes d'authentification ; - ne pas utiliser les mêmes informations secrètes d'authentification à des fins professionnelles et personnelles ; - modifier leurs mots de passe après la	• Revue du processus d'attribution des informations secrètes d'authentification ; • Revue d'un échantillon d'engagements de confidentialité des utilisateurs détenant des informations secrètes d'authentification ; • Interview des administrateurs systèmes, réseaux, BD et applications ; • Revue d'un échantillon d'accusés de réception de ces informations ; • Test d'accès sur les systèmes et logiciels en utilisant des informations secrètes d'authentification par défaut des fournisseurs ; • Revue des programmes de sessions de sensibilisation ; • Interview du DRH pour l'identification des sujets des sessions de sensibilisation relative à l'utilisation d'informations secrètes d'authentification ; • Interview d'un échantillon d'employés ayant participé à ces sessions.	• Document du processus d'attribution des informations secrètes d'authentification ; • Échantillon d'engagements de confidentialité ; • Échantillon d'accusés de réception des informations secrètes d'authentification, Captures d'écran de tentatives de connexions utilisant des informations secrètes d'authentification par défaut des fournisseurs ; • Programme de sessions de sensibilisation réalisées et leurs bénéficiaires ; • Listes des participants aux sessions de sensibilisation.

			première utilisation, avec la précision que les mots de passe personnels ou les numéros d'identification personnels (codes PIN) sont générés automatiquement pendant les processus d'inscription en tant qu'informations d'authentification secrètes temporaires; • Si le système impose l'utilisation d'identifiants d'utilisateur et de mots de passe individuels pour garantir l'imputabilité ; • Si le système permet aux utilisateurs de sélectionner et de modifier leurs propres mots de passe avec la possibilité de confirmation pour éviter les erreurs de saisie ; • Si le système impose un choix de mots de passe de qualité (longueur, lettres, chiffres, caractères spéciaux ...) ; • Si le système force les utilisateurs à changer leurs mots de passe lors de la première connexion ; • Si le système exige un changement périodique des mots de passe et en tant que de besoin ; • Si le système tient un enregistrement des mots de passe utilisés précédemment et empêche leur réutilisation ; • Si le système masque les mots de passe sur l'écran lors de la saisie ; • Si le système stocke les fichiers de mot de passe séparément des données des applications ; • Si le système stocke et transmet les mots de passe sous une forme protégée.		
		Les droits d'accès aux informations et autres actifs associés doivent être pourvus, révisés, modifiés et supprimés conformément à la politique spécifique au contrôle d'accès et aux règles de contrôle d'accès de l'entité auditée.	• Si un processus de provision ou de révocation des droits d'accès physiques et logiques accordés à l'identité authentifiée d'une entité est mis en œuvre ; • Si l'autorisation du propriétaire des informations et autres actifs associés, pour l'utilisation de ces informations et autres actifs associés, est obtenue et si une approbation distincte des droits d'accès de la part de la direction est nécessaire ; • Si le niveau d'accès accordé est conforme à la politique	• Revue des matrices des droits d'accès et des fiches de postes et vérification : - de la conformité des niveaux d'accès avec la politique de contrôle d'accès ; - de la compatibilité de ces	• Politique de contrôle d'accès ; • Matrice des droits d'accès ; • Fiches de postes d'un échantillon d'utilisateurs.

5.18	Droits d'accès		de contrôle d'accès et est compatible avec d'autres exigences telles que la séparation des tâches ; • Si un enregistrement des droits d'accès accordés à un utilisateur, pour accéder aux informations et autres actifs associés, est maintenu ; • Si les droits d'accès des utilisateurs qui ont changé de rôle ou d'emploi sont mis à jour et si les droits d'accès des utilisateurs ayant quitté l'entité auditée sont supprimés ou bloqués immédiatement ; • Si les droits d'accès sont périodiquement revus avec les propriétaires des informations et autres actifs associés ; • Si les droits d'accès des utilisateurs sont revus à intervalles réguliers et après tout changement, tels qu'une promotion, une rétrogradation ou une cessation d'emploi ; • Si les droits d'accès des utilisateurs sont revus et réaffectés lors de la modification des rôles au sein de l'entité auditée ; • Si les autorisations pour les droits d'accès à privilèges sont revues à des intervalles plus fréquents ; • Si les modifications apportées aux comptes à privilèges sont journalisées ; • Si les droits d'accès de tous les employés et des sous-traitants aux informations et aux moyens de traitement de l'information sont supprimés à la fin de leur emploi, contrat ou convention, ou ajustés en cas de changement.	niveaux d'accès avec la séparation des tâches ; • Interviews des responsables métiers et des administrateurs systèmes et BD ; • Vérification des droits d'accès sur les serveurs et les équipements réseau et de sécurité d'un échantillon d'utilisateurs ayant changé de rôle ou d'emploi, ou quitté l'entité auditée.	
5.19	Sécurité de l'information dans les relations avec les fournisseurs	**D**es processus et procédures pour gérer les risques de sécurité de l'information qui sont associés à l'utilisation des produits ou services des fournisseurs doivent être définis et mis en œuvre.	• Si une politique identifiante et imposante des mesures de sécurité spécifiques aux accès des fournisseurs aux actifs de l'entité auditée est élaborée et mise en œuvre ; • Si des processus et des procédures pour traiter les risques de sécurité associés à l'utilisation des produits et services des fournisseurs sont identifiés et mis en œuvre ; • Si ces processus et ces procédures prennent en considération les relations avec les fournisseurs de services en nuage ;	• Revue de la politique identifiant et imposant des mesures de sécurité spécifiques aux accès des fournisseurs aux actifs de l'entité auditée ; • Revue de la liste des types de fournisseurs (par exemple services informatiques, services logistiques, services	• Politique identifiant et imposant des mesures de sécurité spécifiques aux accès des fournisseurs aux actifs de l'audité ; • Liste des types de fournisseurs (par exemple services informatiques, services logistiques, services financiers, composants de

			• Si les types de fournisseurs (par exemple services informatiques, services logistiques, services financiers, composants de l'infrastructure informatique), auxquels l'entité auditée accordera un accès à son information sont identifiés et si les relations avec ces fournisseurs sont documentées ; • Si les critères d'évaluation et de sélection des fournisseurs sont définis et documentés ; • Si on impose contractuellement à tout fournisseur pouvant avoir accès ou favoriser l'accès à des informations ou à des ressources sensibles, que ses collaborateurs signent un engagement personnel de respect des clauses de sécurité spécifiées ; • Si une analyse des risques liés aux accès du personnel du fournisseur au système d'information ou aux locaux contenant de l'information est réalisée, et si les mesures de sécurité nécessaires sont définies en conséquence ; • Si les types d'accès à l'information que les différents types de fournisseurs se verront accorder sont définis, et si ces accès sont surveillés et contrôlés ; • Si les incidents et les impondérables associés aux accès fournisseurs, incluant les responsabilités de l'entité auditée et celles des fournisseurs sont identifiés et traités ; • Si la sécurité de l'information est préservée pendant la durée du transfert d'informations et des autres actifs associés ; • Si les exigences pour assurer une rupture sécurisée de la relation avec le fournisseur sont définies et documentées ; • Si les procédures pour la continuité du traitement des informations dans le cas où le fournisseur ne serait plus en mesure de fournir ses produits ou ses services sont définies et documentées.	financiers, composants de l'infrastructure informatique) ; • Revue des engagements personnels de respect des clauses de sécurité signés par les collaborateurs du fournisseur ; • Revue du rapport d'analyse des risques liés aux accès du personnel du fournisseur ; • Revue de la définition des types d'accès à l'information accordés aux différents types de fournisseurs ; • Revue du rapport de traitement des incidents et des impondérables associés aux accès fournisseurs.	l'infrastructure informatique) ; • Engagements personnels de respect des clauses de sécurité signés par les collaborateurs du fournisseur ; • Rapport d'analyse des risques liés aux accès du personnel du fournisseur ; • Liste des types d'accès à l'information accordés aux différents types de fournisseurs ; • Rapport de traitement des incidents et des impondérables associés aux accès fournisseurs.

5.20	La sécurité de l'information dans les accords conclus avec les fournisseurs	Les exigences de sécurité de l'information appropriées doivent être mises en place et convenues avec chaque fournisseur, selon le type de relation avec le fournisseur.	• Si l'ensemble des clauses de sécurité que devrait comprendre tout accord signé avec un tiers impliquant un accès au système d'information ou aux locaux contenant de l'information est défini et documenté ; • Si les accords avec les fournisseurs contiennent le respect de toutes les exigences de sécurité de l'information (y compris la description et la classification des informations, les méthodes d'accès aux informations et les règles d'utilisation acceptables des informations et autres actifs associés) ; • Si les accords avec les fournisseurs contiennent les exigences légales, statutaires, réglementaires et contractuelles, y compris la protection des données, le traitement des données à caractère personnel (DCP), les droits de propriété intellectuelle et les droits d'auteur, ainsi que la description de la manière d'assurer du respect de ces exigences ; • Si les accords avec les fournisseurs contiennent les exigences de gestion des incidents (en particulier la notification et la collaboration lors de l'action corrective) ; • Si les accords avec les fournisseurs contiennent les mesures de sécurité pour le transfert des informations ; • Si tout accès d'un tiers au système d'information ou aux locaux contenant de l'information n'est autorisé qu'après la signature d'un accord formel reprenant ces clauses.	• Revue du document de définition de l'ensemble des clauses de sécurité que devrait comprendre tout accord signé avec un tiers ; • Revue d'un échantillon d'accords formels ou de contrats avec les tiers contenant ces clauses ; • Interviews du DAF, du responsable juridique et du RSSI.	• Document de définition de l'ensemble des clauses de sécurité que devrait comprendre tout accord signé avec un tiers ; • Échantillon d'accords formels ou de contrats avec les tiers contenant ces clauses.
5.21	Gestion de la sécurité de l'information dans la chaîne d'approvisionnement	Des processus et procédures pour gérer les risques de sécurité de l'information associés à la chaîne d'approvisionnement des produits et services TIC doivent être définis et mis en œuvre.	• Si une analyse des risques de la sécurité de l'information associés à la chaîne d'approvisionnement est réalisée ; • Si les exigences sur le traitement de ces risques sont incluses dans les accords ou contrats conclus avec les fournisseurs ; • Si les contrats avec les fournisseurs exigent que les fournisseurs de produits TIC propagent des pratiques de sécurité appropriées à travers toute la chaîne d'approvisionnement dans la mesure où ces produits contiennent des composants achetés ou obtenus auprès d'autres fournisseurs ou d'autres entités (par	• Revue du rapport d'analyse des risques de la sécurité de l'information associés à la chaîne d'approvisionnement ; • Revue d'un échantillon d'accords ou de contrats avec les fournisseurs ; • Revue de processus de surveillance pour valider la conformité des produits et	• Rapport d'analyse des risques de la sécurité de l'information associés à la chaîne d'approvisionnement ; • Échantillon d'accords ou de contrats avec les fournisseurs ; • Le processus de surveillance pour valider la conformité des produits et services TIC fournis.

	TIC		exemple, sous-traitants en développement de logiciels et fournisseurs de composants matériels) ; • S'il existe un processus de surveillance pour valider la conformité des produits et services TIC fournis avec les exigences de sécurité spécifiées (exemple : des tests de pénétration et la preuve ou la validation des attestations de tierce partie portant sur les opérations de sécurité de l'information des fournisseurs).	services TIC fournis ; • Interviews du DAF et du RSSI.	
5.22	Surveillance, révision et gestion des changements des services fournisseurs	L'entité auditée doit procéder régulièrement à la surveillance, à la révision, à l'évaluation et à la gestion des changements des services fournisseurs	• Si les niveaux de performance des services sont surveillés et si leur conformité avec les accords est vérifiée ; • Si les rapports de service produits par le fournisseur sont revus et si des réunions régulières sur l'avancement sont organisées comme l'exigent les accords ; • Si les aspects liés à la sécurité de l'information dans les relations du fournisseur avec ses propres fournisseurs sont revus ; • Si les changements apportés aux accords passés avec les fournisseurs sont gérés ; • Si les changements effectués par l'entité auditée pour mettre en œuvre des améliorations aux services offerts, le développement d'applications et de systèmes nouveaux, des changements ou des mises à jour des politiques et des procédures de l'entité auditée sont gérés ; • Si sont gérés les changements dans les services assurés par les fournisseurs pour mettre en œuvre : - des changements et des améliorations apportées aux réseaux ; - l'utilisation de nouvelles technologies ; - l'adoption de nouveaux produits ou des versions/des éditions plus récentes ; - des outils et des environnements de développement nouveaux ; - des changements apportés à l'emplacement physique des équipements de dépannage ; - des changements de fournisseurs ; - la sous-traitance à un autre fournisseur.	• Revue du rapport de surveillance des niveaux de performance des services des fournisseurs ; • Revue des PVs de réunion avec les fournisseurs ; • Revue des aspects liés à la sécurité de l'information dans les relations du fournisseur avec ses propres fournisseurs ; • Interviews du DSI et du RSSI ; • Interview d'un échantillon de fournisseurs ; • Revue du rapport des changements apportés aux accords passés avec les fournisseurs ; • Revue des rapports des changements effectués par l'entité auditée ; • Revue des rapports des changements dans les services assurés par les fournisseurs.	• Rapport de surveillance des niveaux de performance des services des fournisseurs ; • PVs de réunion avec les fournisseurs, ; • Rapport des changements apportés aux accords passés avec les fournisseurs ; • Rapports des changements effectués par l'entité auditée ; • Rapports des changements dans les services assurés par les fournisseurs.

5.23	Sécurité de l'information dans l'utilisation de services en nuage	Les processus d'acquisition, d'utilisation, de gestion et de cessation des services en nuage doivent être établis conformément aux exigences de sécurité de l'information de l'entité auditée.	• Si une politique spécifique à l'utilisation de services en nuage est établie et communiquée à toutes les parties intéressées ; • Si un processus de gestion des risques de sécurité de l'information associés à l'utilisation de services en nuage est défini et communiqué aux utilisateurs du SI; • Si les responsabilités qui incombent au fournisseur de services en nuage et à l'entité auditée en sa qualité de client des services en nuage, sont définies et mises en œuvre de manière appropriée ; • Si toutes les exigences de sécurité de l'information associées à l'utilisation des services en nuage sont définies ; • Si les fonctions et responsabilités relatives à l'utilisation et à la gestion des services en nuage sont définies ; • Si une garantie sur les mesures de sécurité de l'information mises en œuvre par le fournisseur de services en nuage est obtenue ; • Si une procédure de gestion des incidents de sécurité de l'information qui se produisent en lien avec l'utilisation des services en nuage est définie ; • Si la façon de changer ou d'arrêter l'utilisation des services en nuage, y compris les stratégies de sortie des services en nuage est définie ; • Si un contrat avec le fournisseur de services en nuage garantissant la protection des données de l'entité auditée et assurant la disponibilité des services est signé.	• Revue de la politique spécifique à l'utilisation de services en nuage ; • Revue de processus de gestion des risques de sécurité de l'information associés à l'utilisation de services en nuage ; • Revue des fonctions et responsabilités relatives à l'utilisation et à la gestion des services en nuage ; • Revue de la procédure de gestion des incidents de sécurité de l'information ; • Revue des contrats et des garanties signés avec les fournisseurs de services en nuage.	• Politique spécifique à l'utilisation de services en nuage ; • Document de gestion des risques de sécurité de l'information associés à l'utilisation de services en nuage ; • Liste des fonctions et responsabilités relatives à l'utilisation et à la gestion des services en nuage ; • Procédure de gestion des incidents de sécurité de l'information ; • Contrats et garanties signés avec les fournisseurs de services en nuage.
5.24	Planification et préparation de la gestion des incidents de sécurité de l'information	**L'entité auditée** doit planifier et préparer la gestion des incidents de sécurité de l'information en procédant à la définition, à l'établissement et à la communication des processus, fonctions et responsabilités liés à la gestion des incidents de	• Si des responsabilités pour garantir une gestion efficace des incidents sont définies et documentées ; • Si les procédures suivantes sont élaborées et mises en œuvre : - Procédure de surveillance, de détection, d'analyse et de signalement des événements et des incidents liés à la sécurité de l'information ; - Procédure de journalisation des activités de gestion	• Revue du document de définition des responsabilités relatives à la gestion des incidents ; • Revue des fiches de postes du personnel affecté à la gestion des incidents ;	• Document de définition des responsabilités relatives à la gestion des incidents ; • Fiches de postes du personnel affecté à la gestion des incidents ;

		sécurité de l'information.	des incidents ; - Procédure de traitement des incidents ; • Procédure de réponse, incluant les procédures de remontée d'information, de récupération contrôlée de l'incident et de communication aux parties intéressées internes et externes.	• Revue des différentes procédures de gestion des incidents ; • Revue d'un échantillon de fiches d'incidents ; • Interviews du DSI et du RSSI.	• Procédures de gestion des incidents ; • Échantillon de fiches d'incidents.
5.25	Évaluation des événements de sécurité de l'information et prise de décision	Les événements de sécurité de l'information doivent être évalués et il doit être décidé s'il faut les catégoriser comme des incidents de sécurité de l'information.	• S'il existe un schéma de catégorisation et de priorisation des incidents de sécurité de l'information pour l'identification des conséquences et de la priorité d'un incident ; • Si le schéma inclut les critères pour catégoriser les événements en tant qu'incidents de sécurité de l'information ; • Si le point de contact évalue chaque événement de sécurité de l'information en utilisant le schéma ; • Si le personnel responsable de la coordination et de la réponse aux incidents de sécurité de l'information procède à l'évaluation et prend une décision sur les événements de sécurité de l'information ; • Si les résultats de l'évaluation des événements et les décisions prises sont enregistrés de manière détaillée en vue de vérifications ou de références ultérieures.	• Revue du schéma de catégorisation et de priorisation des incidents de sécurité de l'information ; • Revue du rapport d'analyse des événements liés à la sécurité de l'information ; • Revue des enregistrements de l'évaluation des événements et des décisions prises ; • Interviews du DSI et du RSSI, • Revue des registres des résultats de traitement des événements liés à la sécurité.	• Schéma de catégorisation et de priorisation des incidents de sécurité de l'information ; • Rapport d'analyse des événements liés à la sécurité de l'information ; • Enregistrements de l'évaluation des événements et des décisions prises ; • Registres des résultats de traitement des événements liés à la sécurité.
5.26	Réponse aux incidents de sécurité de l'information	Les incidents liés à la sécurité de l'information doivent être traités conformément aux procédures documentées.	• Si une équipe de réponse aux incidents est mise en place ; • Si cette équipe est accessible en permanence ; • Si un système supportant la gestion des incidents est mis en place ; • Si ce système centralise et prend en compte aussi bien les incidents détectés par l'exploitation que ceux signalés par les utilisateurs ; • Si ce système permet un suivi et une relance automatiques des actions nécessaires ; • Si ce système incorpore une typologie des incidents	• Revue de la note de constitution de l'équipe de réponse aux incidents ; • Revue du registre des incidents ; • Revue du plan de traitement des incidents ; • Revue de la BD des incidents ; • Revue du tableau de bord des incidents ;	• Note de constitution de l'équipe de réponse aux incidents ; • Registre des incidents ; • Plan de traitement des incidents ; • BD des incidents ; • Tableau de bord des incidents.

			avec élaboration de statistiques et de tableau de bord des incidents à destination du RSSI ; • Si les preuves sont recueillies aussitôt que possible après l'incident, • Si les failles constatées dans la sécurité de l'information causant ou contribuant à l'incident sont traitées ; • Si, une fois que l'incident a été résolu avec succès, il est clôturé formellement et enregistré.	• Interviews des membres de l'équipe de réponse aux incidents et du RSSI.	
5.27	Tirer des enseignements des incidents de sécurité de l'information	Les connaissances recueillies suite à l'analyse et la résolution d'incidents doivent être utilisées pour réduire la probabilité ou l'impact d'incidents ultérieurs.	• Si les incidents sont revus régulièrement pour quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information, leur volume, les coûts associés et leurs impacts ; • Si les informations obtenues par l'analyse des incidents de sécurité passés sont exploitées afin d'identifier les incidents récurrents ou ayant un fort impact avec les mesures nécessaires pour limiter la fréquence des futurs incidents ainsi que les dommages et les coûts associés.	• Revue des rapports de synthèse des incidents ; • Revue des leçons tirées de l'analyse des incidents ; • Revue de la liste des mesures nécessaires pour limiter la fréquence des futurs incidents ainsi que les dommages et les coûts associés.	• Rapports de synthèse des incidents ; • Document des leçons tirées de l'analyse des incidents ; • Liste des mesures déployées.
5.28	Collecte des preuves	L'entité auditée doit définir et appliquer des procédures d'identification, de collecte, d'acquisition et de protection de l'information pouvant servir de preuve.	• Si une procédure d'identification, de collecte et de protection de l'information pouvant servir de preuve est élaborée et mise en œuvre ; • Si la collecte de preuves est réalisée chaque fois qu'une action juridique doit être envisagée ; • Si lors d'incidents de sécurité suivis d'action en justice contre des personnes physiques ou morales, les éléments de preuve sont collectés, conservés, et présentés conformément aux juridictions concernées pour une investigation légale (Forensique) • Si des procédures sont prévues et suivies pour la collecte d'éléments de preuve en cas d'incidents de sécurité impliquant des procédures disciplinaires internes à l'entité auditée.	• Revue de la procédure d'identification, de collecte et de protection de l'information pouvant servir de preuve ; • Revue d'un échantillon de preuves ; • Interviews du DSI, du RSSI et du DRH.	• Procédure d'identification, de collecte et de protection de l'information pouvant servir de preuve ; • Échantillon de preuves.
5.29	Sécurité de l'information pendant une perturbation	L'entité auditée doit planifier comment maintenir la sécurité de l'information au niveau approprié pendant une perturbation.	• Si une analyse de l'impact sur l'activité des aspects liés à la sécurité de l'information est réalisée ; • Si les exigences de sécurité de l'information applicables aux situations défavorables sont déterminées, à la lumière des résultats de l'analyse	• Revue du rapport d'analyse de l'impact sur l'activité des aspects liés à la sécurité de l'information ; • Revue du document des	• Rapport d'analyse de l'impact sur l'activité des aspects liés à la sécurité de l'information ; • Document des exigences

			de l'impact, et documentées ; • Si les mesures de sécurité de l'information, et les systèmes et outils supports dans les plans de continuité d'activité et de continuité TIC ont été mises en œuvre et maintenues ; • Si les objectifs de continuité de la sécurité de l'information sont approuvés par l'organe de direction ; • Si la continuité de la sécurité de l'information est intégrée au processus de gestion de la continuité de l'activité ou au processus de gestion de la récupération après sinistre ; • Si les exigences de continuité de la sécurité de l'information sont formulées de manière explicite dans les processus de gestion de la continuité de l'activité et de gestion de la récupération après sinistre ; • S'il existe une structure de gestion adéquate pour se préparer, atténuer et réagir à un événement perturbant en mobilisant du personnel possédant l'autorité, l'expérience et les compétences nécessaires ; • Si les membres du personnel chargés de la réponse à apporter aux incidents, et qui possèdent les responsabilités, l'autorité et les compétences nécessaires pour gérer les incidents et maintenir la sécurité de l'information, sont nommées ; • Si des processus, des procédures et des mesures permettant de fournir le niveau requis de continuité de la sécurité de l'information au cours d'une crise sont élaborés et mis en œuvre ; • Si des Plans de Continuité d'Activité (PCA) pour chaque activité critique sont élaborée ; • Si le personnel est formé à la mise en œuvre de ces plans ; • Si ces plans sont mis à jour régulièrement ; • Si ces plans sont testés régulièrement ; • Si les résultats des tests sont analysés avec l'organe de direction et les parties prenantes concernées.	exigences de sécurité de l'information applicables aux situations défavorables ; • Revue du processus qui maintient le fonctionnement des mesures de sécurité de l'information existantes pendant une perturbation ; • Interviews du DSI et du RSSI. • Revue de la note de désignation de la structure de gestion et nomination de ses membres ; • Revue des processus, des procédures et des mesures permettant de fournir le niveau requis de continuité de la sécurité de l'information au cours d'une crise ; • Revue des PCA ; • Revue des rapports de test des PCA ; • Revue du rapport d'analyse des résultats des tests des PCA ; • Interviews du DSI et des membres de la structure de gestion de l'entité auditée ; • Interview d'un échantillon du personnel ; • Revue du rapport de test des fonctionnalités des processus, des procédures et des mesures de continuité de la sécurité de l'information ; • Revue du rapport d'audit de la validité et l'efficacité des mesures de continuité de la	de sécurité de l'information applicables aux situations défavorables ; • Processus qui maintient le fonctionnement des mesures de sécurité de l'information existantes pendant une perturbation. • Note de désignation de la structure de gestion et nomination de ces membres ; • Processus, procédures et mesures permettant de fournir le niveau requis de continuité de la sécurité de l'information au cours d'une crise ; • PCAs et dates de leur mise à jour ; • Rapports de test des PCAs ; • Rapport d'analyse des résultats des tests des PCAs ; • Rapport de test des fonctionnalités des processus, des procédures et des mesures de continuité de la sécurité de l'information ; • Rapport d'audit de la validité et l'efficacité des mesures de continuité de la sécurité de l'information après changement dans les systèmes d'information,

			• Si les fonctionnalités des processus, des procédures et des mesures de continuité de la sécurité de l'information sont testées à intervalles réguliers pour s'assurer qu'elles sont cohérentes avec les objectifs de continuité de la sécurité de l'information ; • Si la validité et l'efficacité des mesures de continuité de la sécurité de l'information sont revues à intervalle régulier lorsque les systèmes d'information, les processus, les procédures et les mesures de sécurité de l'information ou les solutions et les processus de gestion de la continuité de l'activité/gestion de la récupération après sinistre connaissent des changements.	sécurité de l'information après changement dans les systèmes d'information, les processus, les procédures et les mesures de sécurité de l'information ; • Interview du RSSI.	les processus, les procédures et les mesures de sécurité de l'information.
5.30	Préparation des TIC pour la continuité d'activité	La préparation des TIC doit être planifiée, mise en œuvre, maintenue et testée en se basant sur les objectifs de continuité d'activité et des exigences de continuité des TIC.	• Si une structure organisationnelle adéquate est en place pour se préparer, atténuer et répondre à une perturbation prise en charge par du personnel détenant la responsabilité, l'autorité et les compétences nécessaires ; • Si les plans de continuité des TIC, y compris des procédures de réponse et de reprise détaillant la façon dont l'entité auditée prévoit de gérer une perturbation des services TIC, sont : - régulièrement évalués par le biais d'exercices et de tests ; - approuvés par la direction ; • Si les plans de continuité des TIC incluent les informations de continuité des TIC suivantes : • les spécifications de performances et de capacité pour respecter les exigences et les objectifs de continuité d'activité tels que spécifiés dans l'analyse d'impact sur l'activité (AIA) ; • le délai de reprise (DR) de chaque service TIC priorisé et les procédures de restauration de ces composants ; • les objectifs de point de reprise (OPR) des ressources TIC priorisées définies en tant qu'informations et les procédures de restauration des informations.	• Revue des fiches de postes ; Revue du plan continuité des TIC ; • Revue des procédures de réponse et de reprise.	• Fiches de postes ; • Plan de continuité des TIC ; • Procédures de réponse et de reprise.

5.31	Exigences légales, statutaires, réglementaires et contractuelles	Les exigences légales, statutaires, réglementaires et contractuelles pertinentes pour la sécurité de l'information, ainsi que l'approche de l'entité auditée pour respecter ces exigences doivent être identifiées, documentées et tenues à jour.	• Si les exigences externes, y compris les exigences légales, statutaires, réglementaires ou contractuelles, sont prises en compte lors de : - l'élaboration des politiques et des procédures de sécurité de l'information ; - la conception, la mise en œuvre ou le changement des mesures de sécurité de l'information ; - la classification des informations et autres actifs associés dans le cadre du processus d'établissement des exigences de sécurité de l'information pour les besoins internes ou pour les accords avec les fournisseurs ; - la réalisation d'appréciations des risques de sécurité de l'information et la détermination des activités de traitement des risques de sécurité de l'information ; - la détermination des processus et des fonctions et responsabilités relatives à la sécurité de l'information associées ; - la détermination des exigences contractuelles des fournisseurs pertinentes pour l'entité auditée et du périmètre de fourniture des produits et des services ; • Si l'entité auditée : - identifie toutes les législations et réglementations pertinentes pour la sécurité de l'information afin de prendre connaissance des exigences concernant son type d'activité ; - se tient régulièrement à jour des législations et réglementations qui lui sont applicables, afin de pouvoir identifier des changements et en tirer des conséquences, en effectuant des revues ou mises à jour des procédures internes le cas échéant ; - définit et documente les processus spécifiques et les responsabilités individuelles pour respecter ces exigences.	• Revue des documents relatifs aux exigences réglementaires, contractuelles et légales ; • Revue du document des mesures spécifiques et des responsabilités individuelles mises en place pour répondre à ces exigences ; • Interviews du DSI, du RSSI, du responsable juridique et du DRH ; • Revue de la procédure de vérification de la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires.	• Procédures et documents relatifs aux exigences réglementaires, contractuelles et légales ; • Historique des mises à jour de ces documents ; • Document des mesures spécifiques et des responsabilités individuelles mises en place pour répondre à ces exigences.

5.32	Droits de propriété Intellectuelle	Des procédures appropriées doivent être mises en œuvre pour garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires.	• Si une procédure est élaborée et mise en œuvre pour garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires ; • Si un inventaire des logiciels officiellement installés et déclarés sur chaque équipement informatique (serveurs, postes de travail, équipement réseau et de sécurité, ...) est tenu à jour en permanence ; • S'il est procédé à des contrôles fréquents visant à vérifier que les logiciels installés sont conformes aux logiciels déclarés ou qu'ils possèdent une licence en règle ; • Si une sensibilisation en matière de protection des droits de propriété intellectuelle est réalisée et si le personnel est prévenu de l'intention de prendre des mesures disciplinaires à l'encontre des personnes enfreignant la réglementation relative à la propriété intellectuelle ; • Si les preuves tangibles de la propriété des licences, des disques maîtres, des manuels, etc. sont conservés ; • Si des contrôles, permettant de s'assurer que le nombre maximal d'utilisateurs autorisé par la licence n'est pas dépassé, sont mis en œuvre.	• Revue de la procédure de vérification de la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires ; • Revue de l'inventaire des logiciels officiellement installés et déclarés sur chaque équipement informatique (serveurs, postes de travail, équipement réseau et de sécurité, ...) ; • Revue du rapport d'audit de la conformité des logiciels installés aux logiciels déclarés ; • Revue du programme de sensibilisation réalisé et la liste des bénéficiaires ; • Interviews du DSI et du RSSI et d'un échantillon d'utilisateurs ; • Vérification sur un échantillon de serveurs du nombre d'utilisateurs réels et comparaison avec le nombre d'utilisateurs autorisés par la licence ; • Vérification sur un échantillon d'équipements informatiques des licences de logiciels installés.	• Procédure de vérification de la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires ; • Inventaire des logiciels officiellement installés et déclarés sur chaque équipement informatique (serveurs, postes de travail, équipement réseau et de sécurité, ...) ; • Rapport d'audit de la conformité des logiciels installés aux logiciels déclarés ; • Programme de sensibilisation réalisé et liste des bénéficiaires ; • Échantillon de licences de logiciels.

5.33	Protection des enregistrements	Les enregistrements doivent être protégés de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées, conformément aux exigences légales, réglementaires, contractuelles et aux exigences métier.	• Si une procédure de stockage et de manipulation des enregistrements est élaborée et mise en œuvre ; • Si des mesures de protection des enregistrements sont mises en place conformément à leur classification telle que définie par le plan de classification de l'entité auditée ; • Si le système de stockage et de manipulation des enregistrements garantit l'identification des enregistrements et de leur durée de conservation telles que définies par la législation nationale ou par les réglementations en vigueur.	• Revue de la procédure de stockage et de manipulation des enregistrements ; • Interviews du DAF, DRH DSI et RSSI ; • Audit des droits d'accès aux enregistrements au niveau des bases de données.	• Procédure de stockage et de manipulation des enregistrements ; • Rapport d'audit des droits d'accès aux enregistrements.
5.34	Protection de la vie privée et des DCP	Les exigences relatives à la protection de la vie privée et des DCP doivent être identifiées et respectées conformément à la législation, aux réglementations et aux clauses contractuelles applicables.	• Si l'entité auditée a procédé à l'octroi des déclarations/autorisations nécessaires auprès de l'autorité en charge de l'a protection des données à caractère personnelles ; • Si une politique spécifique à la protection de la vie privée et des DCP ainsi que des procédures associées sont élaborées et mises en œuvre ; • Si cette politique et ces procédures sont communiquées à toutes les parties intéressées impliquées dans le traitement des données à caractère personnel ; • Si un délégué à la protection des données (DPO) est désigné ; • Si un recueil regroupant l'ensemble des dispositions légales et réglementaires relatives à la protection des données à caractère personnel est élaboré ; • Si le DPO fournit des recommandations au personnel, aux fournisseurs de services et à d'autres parties intéressées sur leurs responsabilités individuelles et les procédures spécifiques qu'il convient de suivre ; • Si un programme de sensibilisation et de formation en matière de protection des données à caractère personnel est élaboré et mis en œuvre ; • Si des mesures techniques et organisationnelles appropriées sont mises en œuvre pour protéger les DCP.	• Revue de la politique et des procédures spécifiques à la protection de la vie privée et des DCP ; • Revue du recueil regroupant l'ensemble des dispositions légales et réglementaires ; • Revue du programme de sensibilisation et de formation en matière de protection des DCP et liste des bénéficiaires ; • Interviews du DPO, du DSI, du RSSI et d'un échantillon des personnes impliquées dans le traitement des données à caractère personnel ; • Vérification des mesures techniques et organisationnelles mises en place pour protéger les DCP.	• Déclaration ou demande d'autorisation de traitement des DCP déposée auprès de l'autorité en charge de l'a protection des données à caractère personnelles • Politique et des procédures spécifiques à la protection de la vie privée et des DCP approuvée par le niveau de direction approprié ; • Décision de nomination du DPO ; • Échantillon de décharges (ou courriers électroniques) attestant que toutes les personnes impliquées dans le traitement des DCP ont reçu une copie de cette politique et des procédures associées ; • Recueil regroupant l'ensemble des dispositions légales ou

					réglementaires ; • Programme de sensibilisation et de formation en matière de protection des DCP et liste des bénéficiaires.
5.35	Révision indépendante de la sécurité de l'information	Des revues régulières et indépendantes de l'approche retenue par l'entité auditée pour gérer et mettre en œuvre la sécurité de l'information (à savoir le suivi des objectifs de sécurité, les mesures, les politiques, les procédures et les processus relatifs à la sécurité de l'information) doivent être effectuées à intervalles définis ou lorsque des changements importants sont intervenus.	• Si une procédure de mise à jour des notes d'organisation relatives à la sécurité des systèmes d'information en fonction des évolutions de structures ou à intervalles planifiés est élaborée et mise en œuvre ; • Si des audits indépendants sont réalisés pour veiller à la pérennité de l'applicabilité, de l'adéquation et de l'efficacité de l'approche de l'entité auditée en matière de management de la sécurité de l'information.	• Revue de la procédure de mise à jour des notes d'organisation relatives à la sécurité de l'information ; • Revue des rapports d'audit.	• Procédure de mise à jour des notes d'organisation relatives à la sécurité de l'information ; • Rapports d'audit.
5.36	Conformité aux politiques, règles et normes de sécurité de l'information	La conformité à la politique de sécurité de l'information, aux politiques spécifiques, aux règles et aux normes de l'entité auditée doit être régulièrement vérifiée.	• Si les managers et les propriétaires de produits, de services ou d'informations identifient la manière de vérifier que les exigences de sécurité de l'information définies dans la politique de sécurité de l'information, les politiques spécifiques, les règles, les normes et autres réglementations applicables, sont respectées ; • Si des outils automatisés de mesure et de génération de rapports sont envisagés pour réaliser des révisions régulières efficaces ; • Si, au cas où une non-conformité est détectée à l'issue de la révision, les responsables : - identifient les causes de la non- conformité ; - évaluent le besoin d'actions correctives pour établir la conformité ; - mettent en œuvre les actions correctives appropriées ; - analysent les actions correctives choisies pour vérifier leur efficacité et identifier toutes les défaillances ou faiblesses.	• Revue des rapports d'audit de conformité ; • Interviews du DSI et du RSSI.	• Rapports d'audit de conformité.

5.37	Procédures d'exploitation Documentées	Les procédures d'exploitation doivent être documentées et mises à la disposition de tous les utilisateurs concernés.	• Si les procédures opérationnelles d'exploitation (systèmes, applications, BD, équipements et solutions réseau et sécurité, etc.) sont documentées ; • Si la documentation des procédures opérationnelles d'exploitation est maintenue à jour ; • Si les modifications des procédures d'exploitation sont approuvées par les responsables concernés ; • Si les procédures opérationnelles d'exploitation sont rendues disponibles à toute personne en ayant besoin ; • Si ces procédures sont protégées contre des altérations illicites ; • Si l'authenticité et la pertinence des procédures opérationnelles font l'objet d'un audit régulier.	• Revue des procédures opérationnelles d'exploitation (systèmes, applications, équipements et solutions réseau et sécurité, etc.) ; • Interviews du DSI, du RSSI et des différents administrateurs (système, réseau, BD, ...) ; • Interview d'un échantillon d'utilisateurs supposés utiliser ces procédures ; • Vérification du rapport d'audit de l'authenticité et la pertinence des procédures opérationnelles.	• Procédures opérationnelles d'exploitation ; • Historique des mises à jour des procédures opérationnelles ; • Rapports d'audit de l'authenticité et la pertinence des procédures opérationnelles.
6	**Contrôles de sécurité applicables aux personnes**				
6.1	Sélection des candidats	Des vérifications doivent être effectuées sur tous les candidats à l'embauche conformément aux lois, aux règlements et à l'éthique, et être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés.	• Si un processus de sélection du personnel à plein temps, à temps partiel et temporaire est établi ; • Si des exigences de sélection pour les personnes embauchées par l'intermédiaire de fournisseurs de services sont précisées dans les accords contractuels entre l'entité auditée et les fournisseurs ; • Si des contrôles de vérification de fond pour tous les candidats à l'emploi ont été réalisés conformément à la réglementation en vigueur ; • Si la vérification comprend le certificat de moralité, la confirmation des qualifications académiques et professionnelles prétendues et des contrôles indépendants d'identité ; • Si un candidat pour un poste spécifique de sécurité de l'information possède les compétences nécessaires pour ce poste et s'il est digne de confiance, surtout si le poste est critique pour l'entité auditée.	• Revue du processus de sélection du personnel ; • Revue d'un échantillon des accords contractuels entre l'entité auditée et les fournisseurs ; • Revue du statut et du règlement intérieur ; • Revue de la procédure de recrutement ; • Revue du dossier du RSSI et d'un échantillon de personnes impliquées dans la sécurité ; • Interview du DRH.	• Les accords contractuels entre l'entité auditée et les fournisseurs ; • Statut et règlement intérieur ; • Fiches de postes des personnes impliquées directement dans la sécurité de l'information ; • Procédure de recrutement ; • Dossier du RSSI et des personnes impliquées dans la sécurité de l'information.

6.2	Termes et conditions du contrat de travail	Les contrats de travail doivent préciser les responsabilités du personnel et celles de l'entité auditée en matière de sécurité de l'information.	• Si le personnel est invité à signer un accord de confidentialité ou de non-divulgation avant d'obtenir l'accès aux informations confidentielles et autres actifs associés ; • Si cet accord de confidentialité couvre la responsabilité de l'entité auditée, ainsi que des employés et contractants concernant la sécurité de l'information.	• Revue d'un échantillon des accords de confidentialité ; • Interviews du DRH et du DAF.	• Échantillon des accords de confidentialité signés par le personnel.
6.3	Sensibilisation, enseignement et formation en sécurité de l'information	L'ensemble des salariés de l'entité auditée et les parties intéressées doivent bénéficier d'une sensibilisation, d'un enseignement et des formations en sécurité de l'information appropriés et recevoir régulièrement les mises à jour des politiques et procédures de l'entité auditée s'appliquant à leurs fonctions.	• Si les nouvelles recrues de l'entité auditée reçoivent systématiquement des sessions de sensibilisation, d'enseignement et de formation à la sécurité de l'information ; • Si tous les employés et les sous-traitants reçoivent périodiquement des sessions de sensibilisation sur les risques liés à l'utilisation des moyens IT et les tendances en la matière ; • Si tous les employés et les sous-traitants sont informés des mises à jour régulières appliquées aux politiques et procédures organisationnelles en ce qui concerne leurs fonctions ; • Si les employés dont les missions sont liées directement à la sécurité du SI (RSSI, DSI, Administrateurs, développeurs) ont reçu les formations spécialisées sur la sécurité des produits utilisés, et sur la gestion de la sécurité de manière générale pendant les 3 dernières années.	• Revue des programmes de formation et des sessions de sensibilisation ; • Interview du DRH pour l'identification des sujets des sessions de sensibilisation et de formation ; • Interview d'un échantillon d'employés ayant participé à ces sessions.	• Programme de formation des années précédentes et de l'année en cours ; • Programme de sessions de sensibilisation réalisées et planifiées et leurs bénéficiaires ; • Listes des participants aux sessions de formation et de sensibilisation.
6.4	Processus disciplinaire	Un processus disciplinaire formel et communiqué doit exister pour prendre des mesures à l'encontre du personnel et d'autres parties intéressées qui ont commis une violation de la politique de sécurité de l'information.	• S'il existe un processus disciplinaire formel pour les utilisateurs du SI qui ont commis une violation de la politique de sécurité ; • Si le processus disciplinaire formel apporte une réponse graduée qui tienne compte de facteurs tels que : - la nature (qui, quoi, quand, comment) et la gravité de la violation et ses conséquences ; - si la violation était intentionnelle (malveillante) ou non intentionnelle (accidentelle) ; - s'il s'agit d'une première infraction ou d'une	• Revue du statut et du règlement intérieur ; • Interview du DRH.	Statut et règlement intérieur.

			récidive ; - si le contrevenant a reçu une formation adéquate.		
6.5	Responsabilités après la fin ou le changement d'un emploi	Les responsabilités et les obligations liées à la sécurité de l'information qui restent valables après la fin ou le changement d'un emploi doivent être définies, appliquées et communiquées au personnel et autres parties intéressées pertinents.	• Si les responsabilités et les obligations relatives à la sécurité de l'information à maintenir après la fin ou le changement de l'emploi ou du contrat sont définies et figurent dans les termes et conditions d'embauche du contrat ou de l'accord de la personne ; • Si l'on traite les modifications de responsabilités ou de fonctions comme la cessation d'un emploi ou de responsabilités en cours, accompagnée de l'introduction de nouvelles responsabilités ou d'un nouveau poste • Si les fonctions et responsabilités relatives à la sécurité de l'information détenues par toute personne qui quitte ou change de poste sont identifiées et transférées à une autre personne ; • Si un processus est établi pour communiquer les changements et les procédures opérationnelles au personnel, aux autres parties intéressées et aux contacts pertinents tels que les clients et les fournisseurs ; • Si le processus de fin ou de changement d'emploi est également appliqué au personnel externe des fournisseurs ; • S'il existe un processus en place qui garantit que tous les employés et les sous-traitants restituent à l'audité tous les biens en leur possession à la fin de leur emploi, contrat ou convention ; • Si les droits d'accès de tous les employés et les sous-traitants aux informations et aux moyens de traitement de l'information sont supprimés à la fin de leur emploi, contrat ou convention, ou sont ajustés en cas de changement.	• Revue du processus de fin ou de changement d'emploi ; • Revue du processus de restitution des biens par les employés ou sous- traitants suite à une fin de leur emploi ou contrat ; • Interview du DRH pour l'identification des responsabilités en fin ou changement d'emploi ou de contrat ; • Vérification de la suppression ou d'ajustement des droits d'accès d'un échantillon d'employés et de sous-traitants en fin ou changement d'emploi ou de contrat.	• État sur les actifs et droits d'accès restitués suite à la fin ou à la modification du contrat d'un employé ou d'un sous-traitant ; • Rapport d'audit sur les comptes utilisateurs des employés ou sous-traitants après leurs départs.

6.6	Accords de confidentialité ou de non- divulgation	Les exigences en matière d'accords de confidentialité ou de non- divulgation, doivent être identifiées, documentées vérifiées régulièrement et signées par le personnel et les autres parties intéressées pertinentes conformément aux besoins de l'entité auditée.	• Si le personnel et les parties intéressées signent des accords de confidentialité ou de non-divulgation ; • Si les modalités de ces accords spécifient des exigences de protection de l'information confidentielle en des termes juridiquement exécutoires ; • S'il est tenu compte des éléments suivants pour identifier les exigences en matière de confidentialité et de non-divulgation : - une définition de l'information à protéger (par exemple information confidentielle) ; - la durée prévue de l'accord, y compris les cas où il peut s'avérer nécessaire de poursuivre cette durée indéfiniment ; - les actions à entreprendre lorsqu'un accord arrive à expiration ; - les responsabilités et les actions des signataires visant à éviter une divulgation non autorisée de l'information ; - la propriété de l'information, des secrets commerciaux et la propriété intellectuelle, ainsi que leurs liens avec la protection de l'information confidentielle ; - L'utilisation autorisée des informations confidentielles et les droits du signataire relatifs à l'utilisation de ces informations ; - le droit d'auditer et de contrôler des activités impliquant l'utilisation de l'information confidentielle ; - le processus de notification et de signalement d'une divulgation non autorisée ou d'une fuite de l'information confidentielle ; - les modalités de retour ou de destruction de l'information à l'expiration d'un accord ; - les actions à entreprendre en cas de violation d'un accord ; • Si les accords de confidentialité et de non-divulgation sont revus à intervalles réguliers et en cas de changements ayant une incidence sur ces	• Revue d'un échantillon d'accords de confidentialité ou de non-divulgation ; • Interviews du DAF, du DRH et du responsable juridique.	• Échantillon d'engagements de confidentialité ou de non-divulgation ; • Historique des mises à jour de ces engagements.

			exigences.		
6.7	Travail à distance	Des mesures de sécurité doivent être mises en œuvre lorsque le personnel travaille à distance, pour protéger les informations accessibles, traitées ou stockées en dehors des locaux de l'audité.	Pour les organismes autorisant les activités de travail à distance : • Si une politique spécifique au travail à distance définissant les conditions et les restrictions appropriées est développée et mise en œuvre ; • Si des mesures de sécurité adéquates sont en place pour la protection de l'information sur des sites de travail à distance.	• Revue de la politique spécifique au travail à distance ; • Revue du rapport d'analyse des risques relatifs au domicile des utilisateurs et/ou des sites distants ; • Interviews du RSSI et des responsables métier ; • Vérification des mesures de sécurité mises en place pour la protection de l'information ; • Vérification des droits d'accès sur les systèmes qui hébergent ou traitent les services concernés par le travail à distance ; • Test d'accès d'un site distant et vérification des logs sur les solutions de contrôle d'accès sur le réseau.	• Politique spécifique au travail à distance ; • Rapport d'analyse des risques relatifs au domicile des utilisateurs et/ou des sites distants ; • Document des mesures déployées pour la protection de l'information (type de connectivité sécurisée déployé pour le télétravail (VPN, SSL, etc.), fichier de configuration de l'accès à distance) ; • Liste des droits d'accès sur les systèmes qui hébergent ou traitent les services concernés par le travail à distance ; • Logs des solutions de contrôle d'accès sur le réseau suite à un accès distant.
	Déclaration des	L'entité auditée doit fournir un mécanisme au personnel pour déclarer rapidement les événements de sécurité de l'information observés ou suspectés, à travers des canaux appropriés.	• Si l'ensemble du personnel et des utilisateurs sont informés de leur responsabilité de déclarer le plus rapidement possible les événements de sécurité de l'information afin de prévenir ou de minimiser les conséquences des incidents de sécurité de l'information ; • Si ce personnel est également informé de la procédure pour la déclaration des événements de	• Revue de la procédure de déclaration des événements de sécurité de l'information ; • Revue d'un échantillon de fiches de déclaration des	• Procédure de déclaration des événements de sécurité de l'information ; • Échantillon de fiches de déclaration des événements de sécurité de l'information.

6.8	événements de sécurité de l'information		sécurité de l'information et du point de contact auprès duquel il convient de déclarer les événements ; • Si le mécanisme de déclaration est aussi simple, accessible et disponible que possible ; • Si le personnel et les utilisateurs sont prévenus de ne pas tenter de prouver l'existence des vulnérabilités de sécurité de l'information suspectées.	événements de sécurité de l'information ; • Interviews du DSI, du RSSI et d'un échantillon d'utilisateurs.	
7	Contrôles de sécurité physique				
7.1	Périmètres de sécurité physique	Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones contenant les informations et autres actifs associés.	• Si les périmètres de sécurité sont définis et si l'emplacement et le niveau de résistance de chacun des périmètres sont fonction des exigences de sécurité de l'information relatives aux actifs situés dans le périmètre ; • Si le périmètre d'un bâtiment ou d'un site abritant des moyens de traitement de l'information est physiquement solide (le périmètre ou les zones ne présentent aucune faille susceptible de faciliter une intrusion) ; • Si les toits extérieurs, les murs, les plafonds et le sol du site sont construits de manière solide et si les portes extérieures sont convenablement protégées contre les accès non autorisés par des mécanismes de contrôle, par exemple des barres, des alarmes, des verrous ; • Si les portes et les fenêtres sont verrouillées lorsque les lieux sont sans surveillance, si une protection extérieure pour les fenêtres, particulièrement celles du rez-de-chaussée, est en place, et si des points d'aération sont envisagés ; • Si les toutes les portes coupe-feu dans un périmètre de sécurité sont équipées d'une alarme, surveillées et testées en même temps que les murs pour établir le niveau de résistance requis, et si elles fonctionnent de manière infaillible.	Revue du plan d'architecture du bâtiment de l'audité et identification des périmètres de sécurité physique ; • Revue du rapport de test des mécanismes de sécurité contre les dommages d'intrusion physiques, d'incendies, d'inondations, de perturbation des services généraux ; • Interviews du DAF, du responsable de la sécurité physique et du RSSI ; • Inspection visuelle des périmètres de sécurité.	• Plan d'architecture du bâtiment de l'audité ; • Rapport de test des mécanismes de sécurité, • Photos.

7.2	Les entrées physiques et des points d'accès appropriés.	Les zones sécurisées doivent être protégées par des mesures de sécurité des accès	• Si les points d'accès tels que les zones de livraison et de chargement et d'autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux sont surveillés et, si possible, isolés des moyens de traitement de l'information, afin d'éviter les accès non autorisés ; • Si l'accès aux sites et aux bâtiments est limité au personnel autorisé seulement ; • Si le processus de gestion des droits d'accès aux zones physiques inclut la fourniture, la révision périodique, la mise à jour et la révocation des autorisations ; • Si un journal physique ou un journal d'audit électronique de tous les accès est conservé de manière sécurisée et contrôlé régulièrement, et si l'ensemble des journaux et des informations d'authentification sensibles sont protégés ; • Si un processus et des mécanismes techniques pour la gestion des accès aux zones où les informations sont traitées ou stockées sont établis et mis en œuvre ; • Si une zone de réception surveillée par du personnel, ou d'autres moyens pour contrôler l'accès physique au site ou au bâtiment est mise en place ; • S'il est exigé de l'ensemble du personnel et des parties intéressées le port d'un moyen d'identification visible, et si le personnel de sécurité est notifié immédiatement s'ils rencontrent des visiteurs non accompagnés ou quiconque ne portant pas d'identification visible ; • S'Il est envisagé le port de badges faciles à distinguer pour mieux identifier les employés permanents, les fournisseurs et les visiteurs ; • Si un accès limité aux zones sécurisées ou aux moyens de traitement de l'information est attribué au personnel des fournisseurs seulement si c'est nécessaire ; • Si cet accès est autorisé et surveillé ; • Si un processus de gestion des clés est mis en place pour	• Revue de la procédure de contrôle d'accès physique ; • Revue d'un échantillon d'autorisations d'accès aux zones sécurisées ; • Interview du DAF, du responsable de la sécurité physique et du RSSI ; • Vérification du registre des visiteurs ; • Vérification des contrôles d'accès physiques aux périmètres sécurisés ; • Test du système de contrôle d'accès physique aux salles contenant les moyens de traitement de l'information ; • Vérification de la synchronisation des horloges des serveurs hébergeant ces systèmes ; • Vérification des logs de ces systèmes ; • Vérification sur un échantillon des salariés et des sous-traitant du port d'un moyen d'identification visible (ex : badges).	• Procédure de contrôle d'accès physique ; • Échantillon d'autorisations d'accès aux zones sécurisées ; • Logs du système de contrôle d'accès physique ; • Rapport de test du système de contrôle d'accès ; • Photos.

			assurer la gestion des clés physiques ou des informations d'authentification (par exemple, codes de verrouillage, serrures à combinaison des bureaux, salles et équipements tels que des armoires verrouillables) ; • Si l'identité des visiteurs est authentifiée par un moyen approprié ; • Si la date et l'heure d'arrivée et de départ des visiteurs est consignée ; • Si l'accès aux visiteurs est attribué uniquement à des fins spécifiques ayant fait l'objet d'une autorisation, accompagné des instructions sur les exigences de sécurité de la zone et sur les procédures d'urgence ; • Si tous les visiteurs sont surveillés, sauf si une exception explicite leur a été accordée ; • Si l'accès aux zones de livraison et de chargement depuis l'extérieur du bâtiment est limité au personnel identifié et autorisé ; • Si les portes extérieures des zones de livraison et de chargement sont sécurisées lorsque les, portes menant aux zones restreintes sont ouvertes ; • Si les livraisons entrantes sont enregistrées conformément aux procédures de gestion des actifs et dès leur arrivée sur le site ; • Si les expéditions entrantes et sortantes sont séparées physiquement, si possible.		
7.3	Sécurisation des bureaux, des salles et des installations	Des mesures de sécurité physique pour les bureaux, les salles et les installations doivent être conçues et mises en œuvre.	• Si les installations critiques sont implantées de manière à éviter l'accès au public ; • Si, dans la mesure du possible, les bâtiments sont discrets et donnent le minimum d'indications sur leur finalité, sans signe manifeste, extérieur ou intérieur du bâtiment, qui permette d'identifier la présence d'activités de traitement de l'information ; • Si les installations sont configurées de manière à empêcher que les informations ou les activités confidentielles soient visibles et audibles depuis l'extérieur ; • Si les répertoires et annuaires téléphoniques internes	• Revue du plan d'architecture du bâtiment de l'entité auditée ; • Interview du DSI ; • Inspection visuelle.	Plan d'architecture du bâtiment de l'entité auditée.

			et les plans accessibles en ligne identifiant l'emplacement des moyens de traitement des informations confidentielles ne sont pas facilement accessibles à toute personne non autorisée.		
7.4	Surveillance de la sécurité physique	Les locaux doivent être continuellement surveillés pour empêcher l'accès physique non autorisé.	• Si les locaux physiques sont contrôlés à l'aide de systèmes de surveillance, qui peuvent inclure des vigiles, des alarmes anti-intrusion ou des systèmes de vidéosurveillance ; • Si l'accès aux bâtiments qui hébergent des systèmes critiques sont continuellement surveillés afin de détecter les accès non autorisés ou les comportements suspects au moyen de : - l'installation de systèmes de vidéosurveillance tels que des télévisions en circuit fermé permettant de visionner et d'enregistrer l'accès aux zones sensibles à l'intérieur et à l'extérieur des locaux de l'entité auditée ; - l'installation, conformément aux normes applicables pertinentes, et le test périodique de détecteurs de contact, de son ou de mouvement permettant de déclencher une alarme anti-intrusion ; - l'utilisation de ces alarmes pour couvrir toutes les portes extérieures et les fenêtres accessibles ; • Si les zones inoccupées sont équipées d'alarmes activées en permanence ; • Si d'autres zones (par exemple, les salles informatiques ou de télécommunications) sont couvertes par ces alarmes ; • Si les systèmes de surveillance sont protégés des accès non autorisés afin d'empêcher que des personnes non autorisées aient accès aux informations de surveillance, telles que les enregistrements vidéo, ou que les systèmes sont désactivés à distance.	• Vérification des emplacements des caméras de surveillances et des alarmes ; • Vérification du système de vidéosurveillance ; • Vérification des différents détecteurs et des alarmes.	Photos.

7.5	Protection contre les menaces physiques et environnementales	Une protection contre les menaces physiques et environnementales telles que les catastrophes naturelles et autres menaces physiques, intentionnelles ou non intentionnelles, impactant l'infrastructure doit être conçue et mise en œuvre.	• Si des appréciations du risque sont réalisées à intervalles réguliers pour d'identifier les conséquences potentielles des menaces physiques et environnementales avant de commencer des opérations critiques sur un site physique, et ce à intervalles réguliers. • Si les protections nécessaires sont mises en œuvre et les changements des menaces sont surveillés. • Si les conseils de spécialistes sont sollicités concernant la manière de gérer les risques provenant des menaces physiques et environnementales, telles que les incendies, les inondations, les tremblements de terre, les explosions, les troubles sociaux, les déchets toxiques, les émissions polluantes et autres formes de catastrophes naturelles ou de désastres d'origine humaine. • Si l'emplacement et la construction des locaux physiques tiennent compte de : - la topographie locale, telle que l'élévation appropriée, les plans d'eau et les failles tectoniques ; - les menaces urbaines, telles que les lieux ayant une forte probabilité d'attirer de l'agitation politique, des activités criminelles ou des attaques terroristes. • Si des détecteurs d'humidité ont été installés à proximité des ressources sensibles (en particulier dans les faux planchers le cas échéant), reliés à un poste permanent de surveillance ; • Si des détecteurs de fuite d'eau ont été installés à l'étage supérieur à proximité des locaux abritant des ressources sensibles, reliés à un poste permanent de surveillance ; • S'il a été procédé à une analyse systématique et approfondie de tous les risques d'incendie (par exemple : court-circuit au niveau du câblage, effet de la foudre, personnel fumant dans les locaux, appareillages électriques courants, échauffement d'équipements, propagation depuis l'extérieur, propagation par les	• Revue des rapports d'appréciation du risque ; • Revue de l'étude sur les menaces physiques et environnementales possibles ; • Revue du schéma des voies possibles d'arrivée d'eau ; • Revue des rapports de test des systèmes de détection et d'extinction d'incendie ; • Interviews du DAF, du responsable de la sécurité physique et du DSI ; • Vérification de l'emplacement des détecteurs d'humidité, de fuite d'eau et de fumée.	• Rapports d'appréciation du risque ; • Document de l'étude sur les menaces physiques et environnementales possibles ; • Schéma des voies possibles d'arrivée d'eau ; • Rapports de test des systèmes de détection et d'extinction d'incendie.

			gaines techniques ou la climatisation, etc.) ; • Si un système de détection automatique d'incendie est mis en place pour les locaux sensibles ; • Si Les locaux sensibles sont-protégés par une installation d'extinction automatique d'incendie.		
7.6	Travail dans les zones Sécurisées	Des procédures pour le travail dans les zones sécurisées doivent être conçues et appliquées.	• Si des procédures pour le travail dans les zones sécurisées sont élaborées et mises en œuvre ; • Si le personnel est informé de l'existence de zones sécurisées ou des activités qui s'y pratiquent, sur la seule base du besoin d'en connaître ; • Si le travail non supervisé/encadré en zone sécurisée, tant pour des raisons de sécurité personnelle que pour prévenir toute possibilité d'acte malveillant est évité ; • Si les zones sécurisées inoccupées sont verrouillées physiquement et contrôlées périodiquement ; • Si tout équipement photographique, vidéo, audio ou autres dispositifs d'enregistrement, tels que les appareils photos intégrés à des appareils mobiles sont interdits, sauf autorisation.	• Revue des procédures pour le travail dans les zones sécurisées ; • Interview du responsable de sécurité physique ; • Interview d'un échantillon du personnel ; • Inspection des zones sécurisées inoccupées.	Procédures pour le travail dans les zones sécurisées.
7.7	Bureau vide et écran vide	Les règles du bureau vide, dégagé des documents papier et des supports de stockage amovibles, et les règles de l'écran vide pour les moyens de traitement de l'information doivent être définies et appliquées de manière appropriée.	• Si une politique du bureau vide et de l'écran vide est élaborée, mise en œuvre et communiquée à toutes les parties intéressées ; • Si les informations métier sensibles ou critiques qu'elles soient sous format papier ou sur un support de stockage électronique sont mises sous clé (de préférence dans un coffre- fort, une armoire ou une autre forme de mobilier de sécurité), lorsqu'elles ne sont pas utilisées, et en particulier lorsque les locaux sont vides ; • Si les terminaux finaux des utilisateurs sont protégés par des serrures à clé ou d'autres moyens de sûreté lorsqu'ils ne sont pas utilisés ou sont laissés sans surveillance ; • Si tous les ordinateurs et systèmes sont configurés avec une fonction de temporisation ou de déconnexion automatique ; • Si des imprimantes dotées d'une fonction	• Revue de la politique du bureau vide et de l'écran vide ; • Interviews du DSI et du DAF ; • Inspection d'un échantillon de bureaux occupés par des personnes traitant des dossiers sensibles (utilisation d'armoires se fermant à clés, bureaux propres, etc.) ; • Vérification de l'écran vide sur un échantillon de postes de travail de ces personnes ; • Audit des paramètres de configuration sur un échantillon d'imprimantes	• Politique du bureau vide et de l'écran vide ; • Captures d'écrans ; • Rapport d'audit des paramètres de configuration des imprimantes.

			d'authentification sont utilisées, afin que seuls les initiateurs puissent récupérer leurs impressions, et uniquement lorsqu'ils se trouvent devant l'imprimante ; • Si les documents et les supports de stockage amovibles contenant des informations sensibles sont stockés de façon sécurisée et, lorsqu'ils ne sont plus requis, sont éliminés à l'aide de mécanismes de destruction sécurisés ; • Si les règles et les recommandations pour la configuration des fenêtres contextuelles (pop- ups) sur les écrans (par exemple désactiver les fenêtres contextuelles de notification de réception d'un nouveau courrier électronique et de messagerie, si possible, pendant les présentations, le partage d'écran ou dans un lieu public) sont établies et communiquées ; • Si les informations sensibles ou critiques sur les tableaux blancs et autres types d'affichage sont effacées, lorsqu'elles ne sont plus nécessaires ; • Si l'entité auditée dispose de procédures en place lorsque le personnel quitte les locaux et, notamment la réalisation d'une dernière inspection avant de partir pour s'assurer de ne pas laisser d'actifs de l'entité auditée (par exemple, des documents tombés derrière des tiroirs ou un meuble).	utilisées par ces personnes.	
7.8	Emplacement et protection du matériel	Un emplacement sécurisé pour le matériel doit être choisi et protégé.	• Si un emplacement pour le matériel permettant de minimiser les accès inutiles aux zones de travail et d'empêcher les accès non autorisés est choisi ; • Si les moyens de traitement de l'information manipulant des données sensibles sont positionnés avec soin, en vue de réduire le risque que cette information puisse être vue par des personnes non autorisées • Si les moyens de stockage sont sécurisés contre tout accès non autorisé ; • Si des mesures sont adoptées pour réduire au minimum les risques de menaces physiques et environnementales potentielles, comme le vol, l'incendie, les explosions, la fumée, les fuites d'eau (ou une rupture de l'alimentation en eau), la poussière, les vibrations, les effets engendrés	• Revue du rapport d'inspection de l'emplacement du matériel ; • Revue du rapport de surveillance des conditions ambiantes (température, humidité) ; • Revue des directives sur le fait de manger, boire et fumer à proximité des moyens de traitement de l'information ; • Interview du DSI ;	• Rapport d'inspection de l'emplacement du matériel ; • Rapport de surveillance des conditions ambiantes ; • Directives sur le fait de manger, boire et fumer à proximité des moyens de traitement de l'information.

			par les produits chimiques, les interférences sur le secteur électrique, les interférences sur les lignes de télécommunication, les rayonnements électromagnétiques et le vandalisme ; • Si des directives, sur le fait de manger, boire et fumer à proximité des moyens de traitement de l'information, sont fixées ; • Si les conditions ambiantes, telles que la température et l'humidité, qui pourraient nuire au fonctionnement des moyens de traitement de l'information sont surveillées ; • Si l'ensemble des bâtiments est équipé d'un paratonnerre et si toutes les lignes électriques et de télécommunication entrante sont équipées de parafoudres.	• Vérification des moyens de protection du matériel ; • Vérification des conditions ambiantes (température, humidité) ; • Inspection du paratonnerre des parafoudres.	
7.9	Sécurité des actifs hors des locaux	Des mesures de sécurité doivent être appliquées aux actifs hors des locaux de l'entité auditée pour les protéger.	• Si une politique de sécurité relative au travail hors site est élaborée et mise en œuvre ; • Si des mesures pour l'utilisation protégée, en dehors des locaux de l'entité auditée, des terminaux (appartenant à l'entité auditée ou des terminaux privés utilisés pour le compte de l'entité auditée) qui stockent ou traitent des informations (par exemple, terminal mobile), sont déterminées et mises en œuvre ; • Si l'utilisation de ces terminaux est autorisée par la direction ; • Si le matériel et les supports de stockage sortis des locaux ne sont pas laissés sans surveillance dans des lieux publics ; • Si les instructions du fabricant, visant à protéger le matériel, par exemple celles sur la protection contre l'exposition aux champs électromagnétiques forts, l'eau, la chaleur, l'humidité, la poussière sont respectées ; • Si les informations qu'il n'est pas nécessaire de transférer avec l'actif soient supprimée de façon sécurisée avant le transfert ; • Si, lorsque du matériel circule hors des locaux de l'entité auditée entre différentes personnes ou entre des tiers,	• Revue de la politique de sécurité relative au travail hors site ; • Revue d'un échantillon d'autorisations de l'organe de direction concernant l'utilisation du matériel hors site ; • Revue du rapport d'analyse des risques issus du travail hors site ; • Revue des registres de circulation du matériel hors site entre différentes personnes ou avec des tiers ; • Interview du DSI.	• Politique de sécurité relative au travail hors site ; • Échantillon d'autorisations de l'organe de direction concernant l'utilisation du matériel hors site ; • Rapport d'analyse des risques issus du travail hors site ; • Registres de circulation du matériel hors site entre différentes personnes ou avec des tiers.

			un journal détaillant la chaîne de traçabilité du matériel est tenu à jour, mentionnant au minimum les noms des personnes responsables du matériel, ainsi que les organismes dont elles relèvent ; • Si un système de traçabilité est maintenu à jour en demandant lorsque nécessaire et possible, une autorisation pour le matériel et les supports à sortir des locaux de l'entité auditée et en gardant un enregistrement concernant ces retraits afin de maintenir un système de traçabilité ; • Si les terminaux (par exemple, mobile ou ordinateur portable) sont protégés contre la consultation d'informations dans les transports publics, et contre les risques associés à la « *lecture par-dessus l'épaule* », • Si la géolocalisation et la fonction d'effacement à distance des données des terminaux est mise en œuvre ; • Si des mesures pour l'installation des équipements en dehors des locaux de l'entité auditée sont déterminées en réalisant une appréciation du risque.		
7.10	Supports de stockage	Les supports de stockage doivent être gérés tout au long de leur cycle de vie d'acquisition, d'utilisation, de transport et de mise au rebut conformément au schéma de classification et aux exigences de traitement de l'entité auditée.	• Si une politique spécifique à la gestion des supports de stockage amovibles est établie et communiquée à toute personne qui utilise ou manipule des supports de stockage amovibles ; • Si, lorsque nécessaire et possible, une autorisation pour les supports de stockage à sortir de l'entité auditée est demandé et un enregistrement concernant ces retraits est gardé afin de maintenir un système de traçabilité ; • Si tous les supports de stockage sont stockés dans un environnement sûr et sécurisé selon la classification de leurs informations, et protégés des menaces environnementales (telles que la chaleur, l'humidité, les champs électromagnétiques ou le vieillissement) conformément aux spécifications du fabricant ; • Si des techniques cryptographiques sont utilisées pour	• Revue de la politique de gestion des supports de stockage amovibles ; • Revue des enregistrements de retrait des supports de stockage ; • Inspection des lieux de stockage des supports de stockage ; • Revue du registre des supports de stockage amovibles ; • Revues des procédures de réutilisation ou d'élimination	• Politique de gestion des supports de stockage amovibles ; • Enregistrements de retrait des supports de stockage ; • Registre des supports de stockage amovibles ; • Procédures de réutilisation ou d'élimination sécurisées des supports de stockage ; • Procédures d'identification des éléments qui peuvent nécessiter

			protéger les informations qui se trouvent dans les supports de stockage amovibles ; • Si, pour atténuer les risques de dégradation des supports de stockage lorsque les informations stockées sont toujours utilisées, ces informations sont transférées sur un support de stockage neuf, avant qu'elles ne deviennent illisibles ; • Si plusieurs copies des informations importantes sont stockées sur des supports de stockage séparés pour réduire davantage les risques d'endommagement ou de perte fortuits des informations ; • Si un registre des supports de stockage amovibles est établi pour limiter les risques de perte d'informations ; • Si les ports de supports de stockage amovibles (par exemple, les emplacements pour cartes SD ou les ports bus USB) sont activés seulement si l'entité auditée a une raison de les utiliser ; • Si, lorsqu'il y a un besoin d'utiliser des supports de stockage amovibles, le transfert des informations sur ces supports de stockage est contrôlé ; • Si des procédures de réutilisation ou d'élimination sécurisées des supports de stockage sont définies pour minimiser le risque de fuite d'informations ; • Si des procédures de réutilisation ou d'élimination sécurisées des supports de stockage sont définies pour minimiser le risque de fuite d'informations confidentielles à des personnes non autorisées ; • Si les données sont effacées de manière sécurisée ou si le support de stockage est formaté avant la réutilisation des supports de stockage contenant des informations confidentielles ; • Si les supports de stockage contenant des informations confidentielles sont éliminés de manière sécurisée lorsqu'ils ne sont plus nécessaires (par exemple, par destruction, broyage ou suppression sécurisés du contenu) ; • Si des procédures sont mises en place pour identifier	sécurisées des supports de stockage ; • Revues des procédures d'identification des éléments qui peuvent nécessiter une élimination sécurisée ; • Revue du rapport d'appréciation du risque sur les terminaux endommagés contenant des données sensibles afin de déterminer s'il convient que les éléments soient détruits physiquement plutôt qu'envoyés en réparation ou mis au rebut.	une élimination sécurisée ; • Rapport d'appréciation du risque sur les terminaux endommagés contenant des données sensibles.

			les éléments qui peuvent nécessiter une élimination sécurisée ; • Si l'élimination des éléments sensibles est journalisée afin de maintenir un système de traçabilité ; • Si une appréciation du risque sur les terminaux endommagés contenant des données sensibles est réalisée afin de déterminer s'il convient que les éléments soient détruits physiquement plutôt qu'envoyés en réparation ou mis au rebut.		
7.11	Services supports	Les moyens de traitement de l'information doivent être protégés contre coupures de courant et autres perturbations causées par des défaillances des services supports.	Si les services supports (tels que l'électricité, les télécommunications, l'approvisionnement en eau, le gaz, l'assainissement, la ventilation et la climatisation): • sont conformes aux spécifications du fabricant du matériel et aux exigences légales locales ; • font l'objet d'une évaluation régulière pour vérifier leur capacité à répondre à l'augmentation des activités de l'entité auditée et aux interactions avec les autres services supports ; • sont examinés et testés de manière régulière pour s'assurer de leur fonctionnement correct ; • sont équipés, si nécessaire, d'alarmes de détection des dysfonctionnements ; • disposent, si nécessaire, d'alimentations multiples sur les réseaux physiques d'acheminement.	• Revue des rapports d'évaluation des services généraux ; • Revue des rapports de test des services supports. ; • Interview du DSI ; • Vérification de la conformité des services aux spécifications du fabricant du matériel et aux exigences légales ; • Vérification de l'existence d'alimentation redondante, d'onduleur, d'un groupe électrogène.	• Rapports d'évaluation des services généraux ; • Rapports de test des services supports.
7.12	Sécurité du câblage	Les câbles électriques transportant des données ou supportant les services d'information doivent être protégés contre des interceptions, interférences ou dommages.	• Si, dans la mesure du possible, les lignes électriques et les lignes de télécommunication branchées aux moyens de traitement de l'information sont enterrées, ou soumises à toute autre forme de protection adéquate ; • Si les câbles électriques sont séparés des câbles de télécommunication pour éviter toute interférence ; • Si, pour les systèmes sensibles ou critiques, les mesures supplémentaires comprennent : - l'installation d'un conduit de câbles blindé et de chambres ou de boîtes verrouillées aux points d'inspection et aux extrémités ; - l'utilisation d'un blindage	• Revue du schéma de câblage du réseau électrique et informatique ; • Balayages techniques et d'inspections physiques pour détecter le branchement d'appareils non autorisés sur les câbles ; • Interview du DSI ; • Inspection des conduits de câbles et des panneaux de répartition et des chambres	• Schéma de câblage du réseau électrique et informatique ; • Rapport de balayages techniques et d'inspections physiques pour détecter le branchement d'appareils non autorisés sur les câbles.

			électromagnétique pour assurer la protection des câbles ; - le déclenchement de balayages techniques et d'inspections physiques pour détecter le branchement d'appareils non autorisés sur les câbles ; - un accès contrôlé aux panneaux de répartition et aux chambres de câblage ; - l'utilisation de câbles à fibre optique.	de câblage.	
7.13	Maintenance du matériel	Le matériel doit être entretenu correctement pour assurer la disponibilité, l'intégrité et la confidentialité de l'information.	• Si le matériel est entretenu selon les spécifications et la périodicité recommandées par le fournisseur ; • Si un programme de maintenance est mis en œuvre et si sa supervision par l'entité auditée est assurée ; • Si seul un personnel de maintenance autorisé assure les réparations et l'entretien du matériel ; • Si un dossier de toutes les pannes suspectées ou avérées et de toutes les tâches de maintenance préventives ou correctives est conservé, • Si des mesures appropriées sont mises en œuvre lorsque la maintenance d'un matériel est planifiée en prenant en compte le fait qu'elle soit effectuée par du personnel sur site ou extérieur à l'entité auditée ; et si, lorsque cela est nécessaire, l'information confidentielle contenue dans le matériel est effacée ou le personnel de maintenance a reçu les autorisations suffisantes ; • Si toutes les exigences de maintenance qu'imposent les polices d'assurance sont respectées ; • Si le matériel est inspecté avant de le remettre en service à l'issue de sa maintenance, pour s'assurer qu'il n'a pas subi d'altérations et qu'il fonctionne correctement. • Si le personnel de maintenance est surveillé lors de la réalisation de la maintenance sur site ; • Si les accès à la maintenance à distance sont autorisés et contrôlés.	• Revue des contrats de maintenance des matériels ; • Revue du dossier de toutes les pannes suspectées ou avérées ; • Revue des rapports d'intervention de maintenance préventive et curative ; • Revue des contrats d'assurance des matériels ; • Revue des rapports d'inspection du matériel avant de le remettre en service à l'issue de sa maintenance ; • Interview du DSI ; • Vérification des mesures mises en œuvre avant la maintenance du matériel.	• Contrats de maintenance des matériels ; • Dossier de toutes les pannes suspectées ou avérées ; • Rapports d'intervention de maintenance préventive et curative ; • Contrats d'assurance des matériels ; • Rapports d'inspection du matériel avant de le remettre en service à l'issue de sa maintenance ; • Liste des mesures mises en œuvre avant la maintenance du matériel.

7.14	Élimination ou recyclage sécurisé(e) du matériel	Tous les composants des matériels contenant des supports de stockage doivent être vérifiés pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant leur mise au rebut ou leur réutilisation.	• Si une procédure de mise au rebut ou de réutilisation du matériel est élaborée et mise en œuvre ; • S'il est procédé, lorsqu'il est nécessaire, à une appréciation du risque des appareils endommagés contenant des supports de stockage pour déterminer s'il convient de les détruire physiquement plutôt que de les faire réparer ou de les mettre au rebut ; • Si les supports de stockage contenant de l'information confidentielle ou protégée par le droit d'auteur sont détruits physiquement, ou bien si cette information est détruite, supprimée ou écrasée en privilégiant les techniques rendant l'information d'origine irrécupérable plutôt qu'en utilisant la fonction standard de suppression ou de formatage.	• Revue de la procédure de mise au rebut ou de réutilisation du matériel ; • Revue du rapport d'analyse des risques des appareils endommagés contenant des supports de stockage ; • Revue de l'inventaire du matériel mis au rebut ou réutilisé ; • Revue des rapports de mise au rebut ou de réutilisation du matériel ; • Interview du DSI.	• Procédure de mise au rebut ou de réutilisation du matériel ; • Rapport d'analyse des risques des appareils endommagés contenant des supports de stockage ; • Inventaire du matériel mis au rebut ou réutilisé ; • Rapports de mise au rebut ou de réutilisation du matériel.
8	Contrôles de sécurité technologiques				
8.1	Terminaux finaux des utilisateurs	Les informations stockées, traitées ou accessibles via les terminaux finaux des utilisateurs, doivent être protégées.	• Si une analyse des risques d'utilisation des terminaux finaux des utilisateurs est réalisée ; • Si une politique spécifique à la configuration et à la manipulation sécurisées des terminaux finaux des utilisateurs est élaborée, communiquée et mise en œuvre ; • Si des systèmes de protection techniques sont déployés pour s'assurer que les informations sensibles peuvent uniquement être consultées via les terminaux finaux des utilisateurs, mais ne pas être stockées sur ces terminaux ; • Si tous les utilisateurs sont sensibilisés aux exigences et aux procédures de sécurité destinées à la protection des terminaux finaux des utilisateurs, ainsi qu'aux responsabilités qui leur incombent pour assurer la mise en œuvre de ces mesures de sécurité ; • Si les utilisateurs ferment les sessions actives et arrêtent les services lorsqu'ils n'en ont plus besoin ; • Si les terminaux finaux des utilisateurs sont dotés d'une protection appropriée contre les utilisations non autorisées à l'aide des mesures de sécurité physique (par exemple, verrouillage par clé ou verrous spéciaux)	• Revue de la politique d'utilisation des terminaux finaux des utilisateurs ; • Interviews du RSSI et du DSI ; • Interview du responsable réseau ; • Test d'accès d'un terminal final et vérification des logs des solutions de contrôle d'accès sur le réseau ; • Vérification de la configuration des solutions de contrôle d'accès sur le réseau et revue des ACLs ; • Revue des programmes de sessions de sensibilisation réalisées et leurs bénéficiaires ; • Audit, sur un échantillon de	• Document de l'analyse des risques d'utilisation des terminaux finaux des utilisateurs ; • Politique d'utilisation de ces terminaux ; • Inventaire des terminaux finaux des utilisateurs ; • Inventaire des outils de détection et de contrôle de ces terminaux ; • Logs des solutions de contrôle d'accès sur le réseau ; • Programmes de sessions de sensibilisation réalisées et leurs bénéficiaires ; • Rapport d'audit des paramètres de configuration.

			et des mesures de sécurité logique (par exemple, accès par mot de passe) ; • Si les terminaux contenant des informations métier importantes, sensibles ou critiques sont surveillés ; • Si les utilisateurs se déconnectent des applications ou des services en réseau lorsqu'ils n'en ont plus besoin ; • Si une procédure spécifique prenant en compte les exigences légales, statutaires, réglementaires, contractuelles (y compris les exigences d'assurance) et autres exigences de sécurité de l'entité auditée est établie, pour les cas de vol ou de perte de terminaux finaux des utilisateurs ; • Si la séparation de l'utilisation personnelle et l'utilisation professionnelle des terminaux est assurée, notamment avec l'utilisation d'un logiciel permettant cette séparation et la protection des données métier sur un appareil privé ; • Si l'accès aux informations métier n'est autorisé que lorsque les utilisateurs ont reconnu leurs obligations (protection physique, mise à jour des logiciels, etc.), renoncé à la propriété des données métier et permis l'effacement à distance des données par l'entité auditée en cas de vol ou de perte du terminal, ou lorsque l'utilisation du service n'est plus autorisée ; • Si des procédures de configuration des connexions sans fil sur les terminaux (par exemple, désactivation des protocoles vulnérables) sont établies et mises en œuvre.	postes de travail, des paramètres de configuration ; • Interview d'un échantillon d'utilisateurs.	
		L'attribution et l'utilisation des droits d'accès privilégiés doivent être limitées et gérées.	• Si un processus d'autorisation des droits d'accès privilégiés est mis en œuvre conformément à la politique de contrôle d'accès ; • Si les utilisateurs qui ont besoin de droits d'accès privilégiés pour chaque système ou processus (par exemple, les systèmes d'exploitation, les systèmes de gestion de bases de données et les applications) sont identifiés ; • Si les droits d'accès privilégiés sont attribués aux utilisateurs au besoin et au cas par cas, conformément à la politique de contrôle d'accès et en	• Revue du processus d'attribution des droits privilégiés et la conformité de sa mise en œuvre avec la politique de contrôle d'accès ; • Revue des comptes d'accès privilégiés ; • Revue des logs des accès ;	• Politique de contrôle d'accès ; • Procédure de gestion des accès (règles d'attribution des droits d'accès à privilèges) ; • Liste des comptes d'accès à privilèges sur les applications, les BD, les serveurs et les équipements réseau et de

8.2	Droits d'accès privilégiés		respectant le principe du « *Moindre privilège* », • Si les exigences d'expiration des droits d'accès privilégiés ont été définies et mises en œuvre ; • Si des mesures sont mises en place pour s'assurer que les utilisateurs ont conscience de leurs droits d'accès privilégiés et savent quand ils sont en mode d'accès privilégié (par exemple l'utilisation d'identités utilisateur spécifiques, de paramètres d'interface utilisateur ou même d'un matériel spécifique) ; • Si les exigences d'authentification relatives aux droits d'accès privilégiés sont plus élevées que les exigences relatives aux droits d'accès normaux ; • Si, après tout changement organisationnel, la liste des utilisateurs travaillant avec des droits d'accès privilégiés est revue afin de vérifier si leurs obligations, fonctions, responsabilités et compétences justifient encore qu'ils travaillent avec des droits d'accès privilégiés ; • Si des règles spécifiques sont établies afin d'éviter l'utilisation d'identifiants utilisateurs d'administration génériques ; • Si les droits d'accès privilégiés temporaires sont accordés seulement pour la durée nécessaire pour mettre en œuvre les changements ou les activités approuvés ; • Si tous les accès privilégiés aux systèmes sont journalisés à des fins d'audit ; • Si les identités dotées de droits d'accès privilégiés ne sont ni partagées ni associées à plusieurs personnes • Si les identités dotées de droits d'accès privilégiés sont utilisées seulement pour réaliser des tâches d'administration et non dans le cadre des tâches générales quotidiennes.	• Interview des administrateurs systèmes, réseaux, BD et applications et des responsables métier pour l'identification des droits d'accès privilégiés et des conditions de leur expiration.	sécurité ; • Paramètres des comptes d'accès privilégiés (droits accordés, délai d'expiration).

8.3	Restrictions d'accès aux informations	L'accès à l'information et aux fonctions d'application système doit être restreint conformément à la politique de contrôle d'accès.	• Si les restrictions d'accès sont basées sur des exigences individuelles de l'application métier et conformément à la politique de contrôle d'accès définie ; • Si des mécanismes de configuration pour contrôler l'accès aux informations dans les systèmes, applications et services sont fournis ; • Si les informations contenues dans les sorties sont limitées ; • Si des contrôles d'accès physiques ou logiques pour l'isolation d'applications sensibles, de données d'application ou de systèmes sont mis en place ; • Si des identités sont accordées aux utilisateurs ; • Si l'accès aux informations sensibles est interdit aux utilisateurs inconnus ou anonymes ; • Si l'accès des utilisateurs aux données est contrôlé ; • Si les droits d'accès aux données (tel qu'en lecture, en écriture, en suppression et en exécution) est défini et contrôlé ; • Si des techniques et processus de gestion dynamique des accès permettant de protéger les informations sensibles qui ont une valeur importante pour l'entité auditée sont prises en considération ; • Si ces techniques de gestion dynamique des accès protègent les informations tout au long de leur cycle de vie (c'est-à-dire création, traitement, stockage, transmission et élimination), y compris : - définition de règles relatives à la gestion dynamique des accès basées sur des cas d'utilisation spécifiques ; - la mise en place de processus opérationnels, de surveillance et de notification, et d'une infrastructure technique support ; • Si les systèmes de gestion dynamique des accès protègent les informations en : - Exigeant une authentification, des identifiants appropriés ou un certificat pour accéder aux informations ; - Limitant l'accès par exemple à une période de temps	• Revue de la politique de contrôle d'accès ; • Revue des identités des utilisateurs ; • Revue de la matrice des rôles d'accès ; • Interview des administrateurs systèmes, réseaux BD et applications ; • Vérification des contrôles d'accès par rapport à la matrice ; • Vérification d'un échantillon de sorties ; • Vérification des ACL sur les équipements réseaux et de sécurité ; • Vérification des techniques de gestion dynamique des accès.	• Politique de contrôle d'accès ; • Liste des identités des utilisateurs ; • Matrice des rôles d'accès ; • Échantillon de sorties, • Logs des accès, • ACL des équipements réseau et de sécurité.

			déterminée (par exemple, après une date donnée ou jusqu'à une date donnée) ; - Utilisant le chiffrement pour protéger les informations ; - Définissant les autorisations d'impression pour les informations ; - Enregistrant qui accède aux informations et comment les informations sont utilisées ; - Générant des alertes si des tentatives d'utilisation abusive des informations sont détectées.		
8.4	Accès aux codes source	L'accès en lecture et en écriture au code source, aux outils de développement et aux bibliothèques de logiciels doit être géré de manière appropriée.	• Si des procédures pour gérer l'accès aux codes source des programmes et aux bibliothèques des codes source de programmes sont établies et mises en œuvre ; • Si l'accès en lecture et en écriture aux codes source est attribué en fonction des besoins métier et géré pour traiter les risques d'altération ou d'utilisation abusive conformément aux procédures établies ; • Si l'accès au répertoire de code source n'est pas accordé de façon directe aux développeurs mais à travers des outils de développement qui contrôlent les activités et les autorisations sur le code source ; • Si les listings de programmes sont stockés dans un environnement sécurisé ; • Si tous les accès et toutes les modifications apportées au code source sont journalisés ; • Si l'accès aux bibliothèques de codes source des programmes est restreint ; • Si les bibliothèques de codes sources ne sont pas stockées sur les systèmes en exploitation lorsque cela est possible ; • Si le personnel chargé de l'assistance technique ne dispose pas d'un accès illimité aux bibliothèques de programmes sources ; • Si la mise à jour des codes source et les éléments associés, ainsi que l'attribution de l'accès au code source conformément aux procédures de contrôle des changements ne sont réalisées qu'après attribution d'une autorisation appropriée.	• Revue de la procédure de gestion des changements afin de s'assurer que la maintenance et la duplication des bibliothèques de programmes sources sont adéquatement prises en compte ; • Revue d'un échantillon d'autorisation de mise à jour et de délivrance des programmes sources aux programmeurs ; • Interview du DSI, des programmeurs et du personnel chargé de l'assistance ; • Vérification de l'absence des bibliothèques de programmes sources sur les systèmes en exploitation ; • Vérification des droits d'accès aux bibliothèques de programmes sources ; • Vérification de l'environnement de stockage des listings de	• Procédure de gestion des changements ; • Liste des droits d'accès aux bibliothèques de programmes sources ; • Échantillon d'autorisation de mise à jour et de délivrance des programmes sources aux programmeurs ; • Paramètres de configuration de l'environnement de stockage des listings de programmes ; • Logs des accès aux bibliothèques de programmes sources.

				programmes ; • Vérification des logs des accès aux bibliothèques de programmes sources.	
8.5	Authentification sécurisée	Des technologies et procédures d'authentification sécurisée sur la base des restrictions d'accès aux informations et de la politique de contrôle d'accès doivent être mises en œuvre.	• Si une procédure de connexion sécurisée aux systèmes et aux applications est élaborée et mise en œuvre ; • Si les informations sensibles du système ou de l'application ne sont pas affichées tant que le processus de connexion n'est pas terminé avec succès ; • Si le système affiche un message avertissant les utilisateurs l'accès n'est permis qu'aux utilisateurs autorisés ; • Si le système est protégé contre les tentatives de connexion par « brute force » ; • Si les tentatives d'accès réussies ou échouées sont journalisées ; • Si les mots de passes entrés sont masqués ; • Si les mots de passe sont transmis en mode crypté ; • Si les sessions inactives après une période d'inactivité définie sont fermées automatiquement, en particulier dans des zones à haut risque telles que des zones publiques ou externes en dehors du périmètre de gestion de la sécurité de l'entité auditée, ou sur les terminaux finaux des utilisateurs ; • Si les durées de connexion sont limitées pour fournir une sécurité supplémentaire aux applications à haut risque et réduire les possibilités d'accès non autorisé.	• Revu de la procédure de connexion sécurisée ; • Revue de la politique de contrôle d'accès ; • Interviews des responsables métiers et des administrateurs systèmes, réseaux, et BD ; • Vérification sur les systèmes des paramètres relatifs : - A l'affichage du message d'avertissement ; - Au blocage de connexion après un certain nombre de tentatives échouées ; - Aux tentatives d'accès réussies et échouées journalisées ; - Au masquage des mots de passe entrés ; - À la clôture automatique des sessions inactives après une période d'inactivité définie ; - A la limitation du temps de connexion.	• Procédure de connexion sécurisée ; • Politique de contrôle d'accès ; • Log des accès ; • Captures d'écran ; • Rapport d'audit des paramètres de configuration système.
	Dimensionnement	L'utilisation des ressources doit être surveillée et ajustée selon les besoins de dimensionnement actuels et prévus.	• Si le dimensionnement des moyens de traitement de l'information, des ressources humaines, des bureaux et autres installations a été effectué en tenant compte du niveau de criticité métier des systèmes et processus concernés ;	• Revue des indicateurs/critères de performance des serveurs et des équipements réseaux ;	• Indicateurs/critères de performance des serveurs et des équipements réseaux ; • Procédure de gestion des

8.6			• Si les systèmes sont surveillés pour assurer leur disponibilité, leur efficacité et leur amélioration ; Si les systèmes et les services sont soumis à des tests de résistance afin de s'assurer que les systèmes ont un dimensionnement suffisant pour répondre aux exigences de performance pendant les pics d'utilisation ; • Si des moyens de détection pour signaler les problèmes en temps optimal sont mis en place ; • Si les projections des besoins de dimensionnement futurs tiennent compte des nouveaux besoins métier et systèmes, et des tendances actuelles et prévues en termes de capacités de traitement de l'information de l'entité auditée ; • Si des plans pour éviter les limitations de ressources et la dépendance à l'égard du personnel clé sont mis en place (qui contiennent des solutions pour l'augmentation de la capacité ou la réduction de la demande sur les ressources) ; • Si un plan de gestion du dimensionnement pour les systèmes critiques est documenté.	• Revue de la procédure de gestion des changements ; • Interviews du RSSI et des administrateurs système, BD et réseau ; • Revue des résultats des tests de résistance ; • Vérification des moyens de détection et de signalement mis en place ; • Revue des plans de gestion du dimensionnement.	changements ; • Résultats des tests de résistance ; • Moyens de détection et de signalement ; • Plans de gestion du dimensionnement.
8.7	Protection contre les programmes malveillants (malware)	Une protection contre les programmes malveillants doit être mise en œuvre et renforcée par une sensibilisation appropriée des utilisateurs.	• Si des règles et des mesures de sécurité, qui empêchent ou détectent l'utilisation de logiciels non autorisés sont mises en œuvre ; • Si des mesures de sécurité qui empêchent ou détectent l'utilisation de sites web connus ou suspectés pour leur caractère malveillant, sont mises en œuvre (par exemple, blocklisting) ; • Si un processus de gestion des vulnérabilités est mis œuvre pour réduire les vulnérabilités qui peuvent être exploitées ; • S'il est procédé régulièrement à une validation automatique des logiciels et du contenu des données des systèmes, en particulier pour les systèmes qui gèrent des processus métier critiques ; • Si des mesures de protection contre les risques associés à l'obtention de fichiers et de logiciels soit depuis ou via des réseaux externes, soit sur tout	• Revue des règles et des mesures de sécurité pour la détection et le blocage de l'utilisation de logiciels non autorisés ; • Revue des mesures de protection contre les risques associés à l'obtention de fichiers et de logiciels malveillants via des réseaux externes ou tout autre support ; • Vérification de l'installation des logiciels de détection des programmes malveillants et de réparation ;	• Liste des règles et des mesures de sécurité pour la détection et le blocage de l'utilisation de logiciels non autorisés ; • Liste des mesures et des moyens de protection contre l'obtention de fichiers et de logiciels malveillants ; • Processus d'autorisation de la désactivation temporaire ou permanente des mesures de protection contre les programmes malveillants ;

			autre support, sont mises en place ; • Si des logiciels de détection des programmes malveillants et de réparation pour analyser les ordinateurs et les supports de stockage électroniques, sont installés et mis à jour régulièrement ; • Si des analyses régulières sont réalisées pour s'assurer de l'absence de programmes malveillants et incluent : - l'analyse de toute donnée reçue sur les réseaux ou via toute forme de support de stockage électronique ; - l'analyse des pièces jointes aux courriers électroniques et aux messages instantanés, et des fichiers téléchargés; - l'analyse des pages web au moment d'y accéder ; • Si l'emplacement et la configuration des outils de détection des programmes malveillants et de réparation sont déterminés en fonction des résultats de l'appréciation du risque et en prenant en considération les techniques de contournement des attaquants ; • Si la protection contre l'introduction de programmes malveillants pendant les procédures de maintenance et d'urgence, qui peuvent contourner les mesures de sécurité habituelles contre les programmes malveillants est assurée ; • Si un processus permettant d'autoriser la désactivation temporaire ou permanente de certaines ou de toutes les mesures de protection contre les programmes malveillants, y compris des autorités d'approbation des exceptions, des justifications documentées et les dates de révision est mis en œuvre ; • Si des plans de continuité d'activité appropriés permettant la reprise après des attaques par programmes malveillants sont élaborés ; • Si des procédures et des responsabilités pour gérer la protection des systèmes contre les programmes	• Revue du processus d'autorisation de la désactivation temporaire ou permanente des mesures de protection contre les programmes malveillants ; • Revue des plans de continuité d'activité permettant la reprise après des attaques par programmes malveillants ; • Revue des procédures et des responsabilités pour gérer la protection des systèmes contre les programmes malveillants ; • Revue des procédures de collecte régulière des informations sur les nouveaux programmes malveillants.	• Plans de continuité d'activité permettant la reprise après des attaques par programmes malveillants ; • Procédures et responsabilités pour gérer la protection des systèmes contre les programmes malveillants ; • Procédures de collecte régulière des informations sur les nouveaux programmes malveillants.

			malveillants, y compris la formation à leur utilisation, la déclaration et la reprise après des attaques par programmes malveillants, sont définies ; • Si la sensibilisation ou la formation de tous les utilisateurs sur la manière d'identifier et, éventuellement, d'atténuer la réception, l'envoi ou l'installation de courriers électroniques, fichiers ou programmes infectés par des programmes malveillants, est assurée ; • Si des procédures pour collecter régulièrement des informations sur les nouveaux programmes malveillants, telles que l'abonnement à des listes de diffusion, les bulletins d'alerte des fournisseurs de logiciels ou la consultation de sites web pertinents, sont mises en œuvre.		
8.8	Gestion des vulnérabilités techniques	Des informations sur les vulnérabilités techniques des systèmes d'information utilisés doivent être obtenues, l'exposition de l'entité auditée à ces vulnérabilités doit être évaluée et des mesures appropriées doivent être prises.	• S'il existe des procédures de gestion de vulnérabilités techniques permettant d'identifier, d'évaluer et de répondre aux vulnérabilités des systèmes, réseaux, base de données et applications ; • Si l'entité auditée dispose d'un inventaire précis des actifs pour une gestion efficace des vulnérabilités techniques ; • Si cet inventaire inclut les fournisseurs de logiciels, les noms de logiciels, les numéros de version, l'état d'utilisation en cours et la ou les personnes au sein de l'entité auditée qui sont responsables des logiciels ; • Si les ressources d'information qui seront utilisées pour identifier les vulnérabilités techniques importantes sont déterminées et la liste de ces ressources est mise à jour ; • Si les contrats avec les fournisseurs des systèmes d'information exigent la déclaration des vulnérabilités, leur traitement et leur publication ; • Si des outils d'analyse des vulnérabilités adaptés aux technologies utilisées afin d'identifier les vulnérabilités et de vérifier si l'application de correctifs visant à résoudre les vulnérabilités a été efficace sont utilisés ; • Si des tests périodiques de pénétration du réseau et	• Revue de la procédure de gestion de vulnérabilités techniques ; • Revue des rapports des audits techniques ; • Vérification de l'inventaire des actifs ; • Revue des documents résultant de l'installation des correctifs ; • Interviews du RSSI et des administrateurs système et réseau ; • Vérification du processus de veille sur les vulnérabilités techniques ; • Revue de l'historique des installations des nouvelles versions et des correctifs ; • Interviews des administrateurs système et réseau ;	• Procédure de gestion de vulnérabilités techniques, • Rapports des audits techniques, • Documentation de l'installation des correctifs, • Cellule de veille, • Abonnement au CERT national, • Historique des installations des nouvelles versions et des correctifs, Accords de services en nuage.

			des audits techniques spécialisés approfondis sont réalisés ; • Si des audits techniques réguliers sont menés, • Si l'installation des correctifs de sécurité se fait suite à une étude d'impact, des tests et une approbation préalable ; • Si un processus de veille sur les vulnérabilités techniques est mis en œuvre : - Si une cellule de veille est mise en place ; - Si l'entité auditée dispose de son propre centre de réponse aux urgences ou adhéré à un centre de réponse aux urgences cybernétiques public ou sectoriel ou privé pour s'informer aux vulnérabilités liées aux produits et systèmes utilisés ; • Si les correctifs de sécurité sont régulièrement appliqués ; • Si les installations des nouvelles versions et des correctifs sont tracées ; • Si les étapes entreprises lors de la gestion des vulnérabilités techniques sont journalisées ; • Si, lorsque l'entité auditée utilise un service en nuage fourni par un fournisseur de services en nuage tiers, la gestion des vulnérabilités techniques des ressources du fournisseur de services en nuage doit être assurée par ce dernier.	• Vérification des versions installées sur les serveurs, les équipements réseau et sécurité et les postes de travail ; • Vérification des accords de services en nuage.	
8.9	Gestion des configurations	Les configurations, y compris les configurations de sécurité, du matériel, des logiciels, des services et des réseaux doivent être définies, documentées, mises en œuvre, surveillées et révisées.	• Si des modèles standards pour la configuration sécurisée du matériel, des logiciels, des services et des réseaux sont définis ; • Si un journal de tous les changements de configuration du matériel, des logiciels, des services et des réseaux est défini, établi et tenu à jour.	• Revue de la politique de sécurité de l'information de l'entité auditée, ses politiques spécifiques, les normes et autres exigences de sécurité ; • Vérification des documentations des systèmes, du journal de tous les changements de configuration et des enregistrements de configuration.	• La politique de sécurité de l'information de l'entité auditée, ses politiques spécifiques, les normes et autres exigences de sécurité ; • Le journal de tous les changements de configuration.

8.10	Suppression des informations	Les informations stockées dans les systèmes d'information, les terminaux ou tout autre support de stockage, doivent être supprimées lorsqu'elles ne sont plus nécessaires.	• Si une méthode de suppression (par exemple, écrasement électronique ou effacement cryptographique) conformément aux exigences métier et en tenant compte des lois et réglementations pertinentes est prise en compte ; • Si des logiciels de suppression sécurisée approuvés pour supprimer définitivement les informations afin de contribuer à assurer que les informations ne peuvent pas être récupérées à l'aide d'outils de récupération spécialisés ou d'outils informatiques judiciaires ; • Si des mécanismes d'élimination adaptés au type de support de stockage à éliminer (par exemple, démagnétisation des disques durs et autres supports de stockage magnétiques) sont utilisés.	• Interview du RSSI ; • Interviews du responsable réseau et des responsables métier ; • Vérification des méthodes et des logiciels de suppression.	• La politique spécifique de la conservation des données de l'entité auditée • Liste des logiciels de suppression sécurisée approuvés.
8.11	Masquage des données	Le masquage des données doit être utilisé conformément à la politique de contrôle d'accès de l'entité auditée et d'autres politiques spécifiques associées, ainsi qu'aux exigences métier, tout en prenant en compte la législation applicable.	• Si des procédures de masquage des données sont mises en place conformément à la politique de contrôle d'accès et aux exigences métier, tout en prenant en compte les exigences d'ordre légal, • Si ces procédures sont mises en œuvre et permettent de limiter l'exposition de données sensibles, notamment les données à caractère personnel, et de se conformer aux exigences légales, statutaires, réglementaires et contractuelles, • Si l'accès aux outils de masquage des données n'est possible qu'aux utilisateurs autorisés, Si les restrictions d'accès ou l'utilisation des données traitées sont mises en place.	• Revue de la politique de contrôle d'accès ; • Revue des procédures de masquage des données ; • Interviews du DSI et du responsable métier ; • Revue des comptes d'accès privilégiés ; • Revue des logs des accès.	• Politique de contrôle d'accès ; • Les procédures de masquage des données ; • Log des accès.
8.12	Prévention de la fuite de données	Des mesures de prévention de la fuite de données doivent être appliquées aux systèmes, aux réseaux et à tous les autres terminaux qui traitent, stockent ou transmettent des informations sensibles.	• Si des procédures de classification des informations à protéger contre les fuites sont développées et maintenues ; • S'il existe des mesures de prévention de la fuite de données aux systèmes, réseaux et terminaux qui traitent, stockent ou transmettent de l'information sensible ; • Si ces mesures permettent de détecter et d'empêcher la divulgation et l'extraction non autorisées d'information par des personnes ou des systèmes ; • S'il existe des règles relatives à la classification des	• Revue de la PSI ; • Revue des procédures de classification à protéger contre la fuite ; • Interviews des responsables métier ; • Vérification des mesures de sécurité sur un échantillon de données à protéger contre la fuite.	• PSI ; • Procédures de classification des données à protéger contre la fuite ; • État sur les mesures de sécurité appliquées ; • Logs des actions sur ces données.

			informations à protéger contre les fuites selon leurs exigences de sécurité au niveau de la PSI ; • Si les restrictions d'accès aux données conformément aux exigences de protection pour chaque niveau de classification sont mises en place ; • Si des outils de prévention de la fuite de données sont mis en place et permettent d'identifier les données, surveiller l'usage et le déplacement des données, et prendre des mesures pour empêcher la fuite de données.		
8.13	Sauvegarde des informations	Des copies de sauvegarde de l'information, des logiciels et des systèmes doivent être réalisées et testées régulièrement conformément à une politique de sauvegarde convenue.	• Si une politique de sauvegarde, définissant : - les objets à sauvegarder ; - la fréquence des sauvegardes ; - la nature de sauvegarde (totale, différentielle) ; - les emplacements ; - les mesures de protection ; - la procédure de restauration ; - les synchronismes nécessaires entre différentes sauvegardes ; - les tests périodiques des supports de sauvegarde ; - les tests périodiques de restauration ; - les rôles et les responsabilités, période/cycle de conservation, etc. ; • Si cette politique couvre : - les données applicatives ; - les programmes (sources et/ou exécutables) ; - les paramètres de configuration des applications et des logiciels de base (les différents fichiers de paramétrages) ; - clonage OS des Serveurs métiers ou mise en place d'une infrastructure virtuelle avec acquisition des sauvegardes des machines virtuelles ; - l'ensemble des configurations des équipements réseau et sécurité ;	• Revue de la politique de sauvegarde ; • Revue des rapports d'audit du processus de sauvegarde ; • Interviews des responsables métier ; • Interview du RSSI et des administrateurs système, BD et réseau ; • Revue du plan de sauvegarde ; • Revue du registre de sauvegarde.	• Politique de sauvegarde ; • Liste des responsables de sauvegardes ; • Rapports d'audit du processus de sauvegarde ; • Plan de sauvegarde ; • Registre de sauvegarde.

			- les données utilisateurs ; - l'ensemble des paramètres de configuration des postes utilisateurs ; • Si la politique de sauvegarde est mise à jour à chaque changement de contexte d'exploitation ; • Si les responsabilités de sauvegarde sont définies ; • Si le processus de sauvegarde fait l'objet d'un audit régulier ; • Si un plan de sauvegarde est élaboré et mis en œuvre ; • Si les exigences de sauvegarde des informations sont définies dans le cas d'utilisation du service en nuage ; • Si les copies de sauvegarde sont conservées dans un local sécurisé et protégé des risques accidentels et d'intrusion. Si un tel local est protégé par un contrôle d'accès renforcé et, en outre, est protégé contre les risques d'incendie et de dégâts des eaux ; • Si la politique de sauvegarde est appliquée ; • Si l'ensemble des sauvegardes permettant de reconstituer l'environnement de production est également sauvegardé en dehors du site de production (sauvegardes de recours) ; • Si les sauvegardes sont protégées par des mécanismes de haute sécurité contre toute modification illicite ou indue ; • S'il y-a des tests périodiques de restauration : tests réguliers pour s'assurer que les sauvegardes réalisées, leur documentation et leur paramétrage permettent effectivement de reconstituer à tout moment l'environnement de production ; • S'il y a des tests réguliers des supports de sauvegardes.		
		Des moyens de traitement de l'information doivent être mis en œuvre avec suffisamment de redondance pour répondre aux exigences de disponibilité.	• Si les exigences relatives à la disponibilité des services métier et des systèmes d'information sont identifiées ; • Si une architecture de systèmes avec une redondance appropriée est conçue et mise en œuvre	• Revue du document d'analyse des exigences en continuité d'activité, • Revue de l'architecture réseau,	• document d'analyse des exigences en continuité d'activité, • L'architecture réseau • Inventaire du matériel,

8.14	Redondance des moyens de traitement de l'information		pour satisfaire à ces exigences ; • Si des procédures sont élaborées et mise en œuvre pour l'activation des composants et moyens de traitement redondants ; • Si ces composants et moyens de traitement de l'information redondants assurent le même niveau de sécurité que les composants et moyens de traitement principaux ; • Si des mécanismes pour alerter l'entité auditée de toute défaillance des moyens de traitement de l'information sont mis en place ; • Si un contrat est conclu avec deux ou plusieurs fournisseurs de réseaux et de moyens de traitement de l'information critiques, tels que les fournisseurs de services Internet ; • Si des réseaux redondants sont utilisés ; • Si deux centres de données séparés géographiquement, avec des systèmes en miroir sont utilisés ; • Si des sources d'alimentation physiquement redondantes sont utilisées ; • Si plusieurs instances parallèles des composants logiciels, avec équilibrage de charge automatique entre eux (entre les instances d'un même centre de données ou de plusieurs centres de données), sont utilisées.	• Revue de l'inventaire du matériel, • Revue des rapports de tests de la solution de secours, • Interview du DSI et du RSSI.	• Rapports de tests de la solution de secours.
8.15	Journalisation	Les journaux qui enregistrent les activités, les exceptions, les pannes et autres événements pertinents doivent être générés, conservés, protégés et analysés.	• Si une analyse spécifique des besoins en termes de journalisation est réalisée : quelles données sont collectées et journalisées et toute exigence spécifique aux journaux pour la protection et le traitement des données de journalisation ; • Si les règles résultant de cette analyse font l'objet d'une politique de journalisation formalisée ; • Si cette politique couvre les applications, les bases de données, les systèmes et les équipements ; • Si le répertoire de stockage des fichiers journaux se trouve dans une partition non-système,	• Revue du rapport d'analyse des besoins en termes de journalisation ; • Revue de la politique de journalisation ; • Interview des responsables métier ; • Interview du RSSI et des administrateurs système, BD et	• Rapport d'analyse des besoins en termes de journalisation ; • Politique de journalisation ; • Mécanismes de protection du processus de journalisation ; • Rapports d'audit du processus d'enregistrement ;

			• Si les fichiers de journalisation sont déplacés dans un serveur de journalisation dédié ; • S'il y a application d'une stratégie de rétention (puisque taille max config du fichier journal) ; • S'il y a utilisation des mécanismes d'analyse et de corrélation des fichiers journaux ; • S'il y a utilisation des outils ou une application de contrôle permettant de journaliser et d'enregistrer les appels systèmes sensibles et les accès aux ressources sensibles (applications, fichiers applicatifs, bases de données, systèmes, etc.) ; • S'il y a utilisation des mécanismes de protection des fichiers journaux : exemples : chiffrement, un système de détection de modification, contrôle d'accès etc. ; • Si les processus qui assurent la journalisation sont sous contrôle strict (droits limités et authentification forte pour la solution utilisée contre tout changement illicite des paramètres définis) ; • S'il existe un archivage (sur disque, cassette, etc.) des enregistrements, conservés sur une période bien définie et de manière infalsifiable ; • Si un audit au moins annuel du processus d'enregistrement est réalisé (y compris des processus visant à détecter les tentatives de modification et les processus de réaction à ces tentatives de modification) ; • S'il y a une analyse des événements menés avec des droits d'administration sur les systèmes/bases de données/ équipements réseaux/solutions de sécurité/le parc de postes utilisateurs et pouvant avoir un impact sur la sécurité : configuration des ressources critiques, accès à des informations sensibles, utilisation d'outils sensibles, téléchargement ou modification d'outils d'administration, etc. • Si ces événements ainsi que tous les paramètres utiles à leur analyse ultérieure sont enregistrés (journalisés) ;	réseau ; • Revue des rapports d'audit du processus d'enregistrement ; • Interview de l'administrateur système ; • Vérification des mécanismes de protection du processus de journalisation ; • Vérification de l'archivage des enregistrements ; • Revue du rapport d'analyse des événements menés avec des droits d'administration ; • Revue des rapports d'audit du processus d'enregistrement des actions privilégiées ; • Vérification des mécanismes de protection des journaux administrateur.	• Rapport d'analyse des événements menés avec des droits d'administration ; • Mécanismes de protection des journaux administrateur.

			• Si une analyse de ces enregistrements, permettant de détecter des comportements anormaux est réalisée ; • S'il existe un système permettant de détecter toute modification du système d'enregistrement et de déclencher une alerte immédiate auprès d'un responsable ; • Si les enregistrements sont protégés contre toute altération ou destruction ; • Si les enregistrements ou les synthèses sont conservés sur une durée bien étudiée ; • Si le processus d'enregistrement des actions privilégiées et de traitement de ces enregistrements fait l'objet d'un audit régulier.		
8.16	Activités de surveillance	Les réseaux, systèmes et applications doivent être surveillés pour détecter les comportements anormaux et des mesures appropriées doivent être prises pour évaluer les éventuels incidents de sécurité de l'information.	• Si le périmètre et le niveau de surveillance est déterminé conformément aux exigences métier, légales, réglementaires et de sécurité de l'information ; • Si le système de surveillance inclut les éléments suivants : - La surveillance des réseaux, systèmes et applications critiques à savoir : trafic entrant et sortant, les accès, fichiers de configuration et journaux d'événements relatifs aux activités système ou réseau ; - les journaux générés par les solutions de sécurité (antivirus, firewall, IPS/IDS, etc.), - la surveillance de la performance des ressources (CPU, disques durs, mémoire, bande passante, etc.) ; - la vérification que seulement les codes autorisés sont en cours d'exécution dans le système ; • Si le système de surveillance est configuré par rapport à une base de référence des comportements normaux établie par l'entité auditée afin d'identifier les comportements anormaux ; • Si un système de détection d'intrusion est utilisé ; • Si la surveillance est effectuée, selon les besoins et moyens de l'entité auditée, en temps réel ou à intervalles réguliers à travers un outil de surveillance	• Interviews du DSI et du RSSI, Audit de la composition et de la couverture du système de surveillance ; • Audit de la configuration de l'outil de surveillance ; • Audit de la configuration des serveurs, des BD et des équipements réseau et de sécurité ; • Audit de la configuration du système de détection d'intrusion ; • Revue des enregistrements de surveillance ; • Revue des registres des résultats de traitement des événements liés à la sécurité ; • Revue des outils de déclaration des événements anormaux.	• Document de présentation du système de surveillance ; • Configuration de l'outil de surveillance ; • Rapport d'audit de la configuration des serveurs, des BD et des équipements réseau et de sécurité ; • Configuration du système de détection d'intrusion ; • Enregistrements de surveillance ; • Registres des résultats de traitement des événements liés à la sécurité ; • Liste des événements déclarés.

			automatisée configuré par un système d'alerte paramétré selon la base de référence établie ainsi qu'un système de notification en temps réel ; Si les enregistrements de surveillance sont conservés pendant des durées de conservation définies ; • S'il existe du personnel dédié à la réponse aux alertes et correctement formé pour traiter les éventuels incidents ; • Si les événements anormaux sont communiqués aux parties concernées ; • Si des procédures pour identifier et traiter les faux positifs, notamment le réglage du logiciel de surveillance pour réduire le nombre de faux positifs futurs sont définies.		
8.17	Synchronisation des Horloges	Les horloges des systèmes de traitement de l'information utilisés par l'entité auditée doivent être synchronisées avec des sources de temps approuvées.	• Si les exigences externes et internes pour la représentation du temps, la synchronisation fiable et la précision sont documentées et mises en œuvre ; • Si, dans le cas d'utilisation de plusieurs services en nuage ou lors de l'utilisation conjointe de services en nuage et de services sur site, les horloges sont gérées et les décalages sont enregistrés afin d'atténuer les risques découlant de ces décalages, • Si un dispositif de synchronisation des horloges des systèmes et des équipements réseau et sécurité avec un référentiel de temps précis (un serveur NTP) est mis en place.	• Interviews des administrateurs système et réseau ; • Vérification de la synchronisation des horloges des serveurs et des équipements réseau et sécurité avec un serveur NTP unique ; • Vérification des enregistrements des décalages des horloges.	• Horloges des serveurs et des équipements réseau et sécurité synchronisées avec un serveur NTP unique ; • Enregistrements des décalages des horloges.
8.18	Utilisation de programmes utilitaires à privilèges	L'utilisation des programmes utilitaires ayant la capacité de contourner les mesures de sécurité des systèmes ou des applications doit être limitée et contrôlée étroitement.	• Si une procédure d'identification, d'authentification et d'autorisation spécifiques aux programmes utilitaires à privilèges est élaborée et mise en œuvre ; • Si les programmes utilitaires à privilège sont séparés des logiciels d'application, et que les communications réseau de ces programmes sont séparées du trafic des applications ; • Si l'utilisation des programmes utilitaires à privilège est limitée à un nombre minimal acceptable d'utilisateurs de confiance bénéficiant d'une autorisation ;	• Revue de la procédure d'identification, d'authentification et d'autorisation spécifiques aux programmes utilitaires à privilège ; • Revue du document définissant les niveaux d'autorisation relatifs aux programmes utilitaires à privilège ;	• Procédure d'identification, d'authentification et d'autorisation spécifiques aux programmes utilitaires ; • Document définissant les niveaux d'autorisation relatifs aux programmes utilitaires à privilège ; • logs d'utilisation des programmes utilitaires à

			• Si toutes les utilisations de programmes utilitaires à privilège sont journalisées, • Si les niveaux d'autorisation relatifs aux programmes utilitaires à privilège sont définis et documentés ; • Si tous les programmes utilitaires à privilège inutiles sont désinstallés ou désactivés ; • Si les programmes utilitaires ne sont pas mis à la disposition des utilisateurs ayant accès à des applications relatives à des systèmes pour lesquels la séparation des tâches est requise.	• Interview du DSI ; • Vérification sur les serveurs et sur un échantillon de postes de travail de l'existence de programmes utilitaires à privilège et de leur utilité ; • Vérification sur un échantillon de postes de travail des utilisateurs ayant accès à des applications relatives à des systèmes pour lesquels la séparation des tâches est requise, de l'existence de programmes utilitaires à privilège ; • Vérification des logs d'utilisation des programmes utilitaires à privilège.	privilège.
8.19	Installation de logiciels sur des systèmes opérationnels	Des procédures et des mesures doivent être mises en œuvre pour gérer de manière sécurisée l'installation de logiciels sur les systèmes opérationnels.	• Si une procédure d'installation sur les systèmes opérationnels de nouvelles versions de systèmes/logiciels/ applications est élaborée et mise en œuvre selon un processus de validation et d'autorisation bien défini ; • Si les nouvelles fonctionnalités ou changements de fonctionnalités liées à un nouveau système ou à une nouvelle version sont systématiquement décrites dans une documentation obligatoire avant tout passage en production ; • Si une revue formelle des nouvelles fonctionnalités (ou des changements de fonctionnalités) liées à un changement majeur de logiciel/système est systématiquement réalisée ; • Si cette revue comprend une analyse des risques éventuels pouvant naître à cette occasion ; • Si l'équipe d'exploitation a reçu une formation spécifique à l'analyse des risques ou fait appel à une ressource spécialisée pour de procéder à cette analyse de risques ;	• Revue de la procédure du contrôle de l'installation de logiciels sur des systèmes opérationnels ; • Interview de l'administrateur système ; • Vérification sur un échantillon d'installations sur des systèmes opérationnels, des documents résultants ; • Interview de l'administrateur système ; • Vérification sur un échantillon des postes utilisateurs ;	• Procédure du contrôle de l'installation de logiciels sur des systèmes opérationnels ; • Historique des installations sur des systèmes opérationnels ; • Documentation des changements sur des systèmes opérationnels ; • Outil ou document de gestion des versions de références pour les produits installés sur les postes utilisateurs, • Politique de contrôle d'accès ; • Matrice des droits d'accès ;

			• Si la mise en production de nouvelles versions de systèmes/logiciels/ applications n'est possible que par le personnel d'exploitation ; • Si la production informatique gère une version de référence pour chaque produit installé sur les postes utilisateurs ; • Si les droits d'accès distincts sont définis, pour chaque système, en fonction des profils et des projets ; • Si les types de logiciels dont l'installation est autorisée (par exemple l'installation des mises à jour ou de correctifs à des logiciels existants) et les types d'installation qui sont interdits (par exemple, l'installation de logiciels destinés uniquement à un usage personnel) sont déterminés.	• Revue de la liste des types de logiciels dont l'installation est autorisée et des types d'installation qui sont interdits.	• Fiches de postes d'un échantillon d'utilisateurs ; • Liste des types de logiciels dont l'installation est autorisée et des types d'installation qui sont interdits.
8.20	Sécurité des réseaux	Les réseaux et les terminaux réseau doivent être sécurisés, gérés et contrôlés pour protéger les informations des systèmes et des applications.	• Si des mesures de sécurité sont mises en œuvre pour assurer la sécurité des informations dans les réseaux et pour protéger les services connectés contre les accès non autorisés, en prenant en considération le type et le niveau de classification des informations que le réseau peut prendre en charge, • Si les responsabilités et les procédures de gestion des équipements et des terminaux réseau sont définies ; • Si la documentation, y compris les diagrammes de réseau et les fichiers de configuration des équipements (par exemple, les routeurs, les commutateurs) est tenue à jour ; • Si la responsabilité opérationnelle des réseaux et les activités sur les systèmes TIC est séparée ; • Si des mesures de sécurité sont définies pour préserver la confidentialité et l'intégrité des données transitant sur des réseaux publics, des réseaux de parties tierces ou sur des réseaux sans fil et pour protéger les systèmes et applications connectés ; • Si une journalisation et une surveillance appropriées sont assurées pour permettre l'enregistrement et la détection d'actions qui	• Revue de la procédure de gestion des équipements et des terminaux réseau ; • Revue du schéma synoptique de l'architecture du réseau ; • Revue du diagramme des flux réseau ; • Revue des fiches de postes des administrateurs réseau ; • Revue de l'inventaire des équipements réseau et de sécurité ; • Interview des administrateurs réseau ; • Audit des comptes d'administration des équipements réseaux et	• Procédure de gestion des équipements et des terminaux réseau ; • Schéma synoptique de l'architecture du réseau ; • Diagramme des flux réseau ; • Fiches de postes des administrateurs réseau ; • Inventaire des équipements réseau et de sécurité ; • Rapport d'audit des comptes d'administration des équipements réseaux et de sécurité ; • Fichiers de configuration et ACL des équipements réseau et de sécurité ; • Logs de ces équipements.

			peuvent affecter, ou qui sont pertinentes pour la sécurité de l'information ; • Si les systèmes sont authentifiés sur le réseau ; • Si la connexion des systèmes au réseau est restreinte et filtrée (par exemple, en utilisant des pare-feu) ; • Si la connexion d'équipements et de terminaux au réseau est détectée, restreinte et authentifiée ; • Si les terminaux réseau sont durcis ; • Si les canaux d'administration réseau sont séparés des autres trafics réseau ; • Si les protocoles réseau vulnérables sont désactivés ; • Si les mesures de sécurité appropriées sont appliquées pour l'utilisation de réseaux virtuels.	de sécurité (compte partagé par tous les administrateurs ou comptes nominatifs) ; • Audit des configurations de ces équipements ; • Revue des ACLs sur ces équipements ; • Revue des logs de ces équipements et identification des actions éventuelles pouvant avoir un impact sur la sécurité des réseaux (ex : accès par des outils non sécurisé tel que Telnet).	
8.21	Sécurité des services Réseau	Les mécanismes de sécurité, les niveaux de service et les exigences de services des services réseau doivent être identifiés, mis en œuvre et surveillés.	• Si la capacité du fournisseur de services de réseau à gérer ses services de façon sécurisée est déterminée et surveillée régulièrement ; • Si un accord sur le droit à auditer est conclu avec le fournisseur ; • Si les dispositions de sécurité nécessaires à des services en particulier, telles que les fonctions de sécurité, les niveaux de service et les exigences de gestion sont identifiées et documentées ; • Si l'audité s'assure que les fournisseurs de services de réseau mettent ces mesures en œuvre.	• Revue des accords de niveau de service (SLA) conclus avec les fournisseurs de service internes ou externes ; • Revue de l'accord sur le droit à auditer ; • Revue des rapports de surveillance de la capacité des connexions et des équipements (bande passante contractée vs bande passante réelle, etc.) ; • Revue des rapports d'audit de la capacité des fournisseurs à respecter l'accord de niveau de service ; • Interview des administrateurs réseau et des responsables	• Accords de niveau de service (SLA) conclus avec les fournisseurs de service internes ou externes ; • Accord sur le droit à auditer ; • Rapports de surveillance de la capacité des connexions et des équipements (bande passante contractée vs bande passante réelle, etc.), • Rapports d'audit de la capacité des fournisseurs à respecter l'accord de niveau de service.

				métier.	
8.22	Cloisonnement des réseaux	Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être cloisonnés dans les réseaux de l'entité auditée.	• Si le réseau est divisé en domaines réseau distincts et en le séparant du réseau public ; • Si le périmètre de chaque domaine est bien défini ; • Si les critères de cloisonnement des réseaux en domaines et les accès autorisés à travers les passerelles sont basés sur une évaluation des exigences de sécurité de chaque domaine ; • Si cette évaluation est conforme à la politique spécifique au contrôle d'accès, aux exigences d'accès, à la valeur et à la classification des informations traitées ; • Si les réseaux d'accès sans fil destinés aux invités sont séparés de ceux destinés au personnel ; • Si le Wi-Fi destiné aux invités est soumis aux mêmes restrictions au moins que le Wi-Fi du personnel, afin de dissuader le personnel d'utiliser le Wi-Fi pour invités.	• Revue du schéma synoptique de l'architecture du réseau ; • Revue du diagramme des flux réseau ; • Revue de l'inventaire des équipements réseau et de sécurité ; • Interviews des administrateurs réseau ; • Audit des configurations et des ACLs des équipements réseau et de sécurité.	• Schéma synoptique de l'architecture du réseau ; • Diagramme des flux réseau ; • Inventaire des équipements réseau et de sécurité ; • Rapport d'audit de configuration et ACLs des équipements réseau et de sécurité.
8.23	Filtrage web	L'accès aux sites web externes doit être géré pour réduire l'exposition aux contenus malveillants.	• S'il existe un mécanisme pour empêcher l'accès aux sites web contenant des informations illégales ou des contenus malveillants (exemple : blocage des adresses IP ou les domaines des sites web concernés) ; • Si les types de sites web interdits sont identifiés et bloqués par l'entité auditée, à savoir : - sites web comportant une fonction de téléchargement d'informations, sauf si cela est autorisé pour des raisons professionnelles ; - sites web connus pour être malveillants ou suspectés de l'être (par exemple, ceux qui diffusent des programmes malveillants ou du contenu d'hameçonnage), - serveurs de commande et de contrôle ; - sites web malveillants provenant des	• Revue de l'inventaire des équipements réseau et de sécurité ; • Interview des administrateurs réseau et système ; • Audit de configuration du mécanisme de filtrage web ; • Vérification de la liste des IPs et des sites web bloqués ; • Revue de la liste de formations de personnel.	• Inventaire des équipements réseau et de sécurité ; • Rapport d'audit de configuration du mécanisme de filtrage web ; • Liste des formations du personnel.

			renseignements sur les menaces ; - sites web partageant du contenu illégal ; • Si des formations au personnel sur l'utilisation sécurisée et appropriée des ressources en ligne sont effectuées.		
8.24	Utilisation de la cryptographie	Des règles pour l'utilisation efficace de la cryptographie, notamment la gestion des clés cryptographiques, doivent être définies et mises en œuvre.	• Si une politique d'utilisation de la cryptographie est élaborée et mise en œuvre ; • Si la direction adopte une approche en ce qui concerne l'utilisation de mesures cryptographiques pour la protection de l'information liée à l'activité de l'entité auditée ; • Si le niveau de protection requis et la classification des informations, en tenant compte du type, de la puissance et de la qualité de l'algorithme de chiffrement requis, est identifié sur la base d'une appréciation du risque ; • Si les liens permanents et les échanges de données devant être protégés par des solutions de chiffrement sont définis et si ces solutions sont mises en place au niveau du réseau local et du réseau étendu ; • Si les transactions sensibles devant être protégés par des solutions de chiffrement sont définies et si ces solutions sont mises en place au niveau applicatif ; • Si une politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques est élaborée et mise en œuvre ; • Si le système de gestion des clés repose sur une série convenue de normes, de procédures et de méthodes sécurisées pour : ◦ La génération des clés et l'attribution de ces clés aux utilisateurs ; ◦ leur stockage ; ◦ le traitement des clés compromises ; ◦ leur révocation ; ◦ la récupération des clés perdues ; ◦ la sauvegarde ou l'archivage ; ◦ la destruction ; • Si les activités liées à la gestion des clés sont journalisées et auditées ;	• Revue de la politique d'utilisation des mesures cryptographiques ; • Revue de rapport d'analyse des risques ; • Entrevue avec le représentant légal de l'entité auditée ; • Interviews des administrateurs systèmes, réseaux, BD et applications ; • Test des solutions de chiffrement mises en place au niveau des serveurs, des équipements réseaux et de sécurité et des applications. • Revue de la politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques ; • Interview des responsables métiers ; • Vérification de la conformité du système de gestion du cycle de vie des clés cryptographiques avec les normes en vigueur ; • Vérification des logs et du rapport d'audit des activités liées à la gestion des clés.	• Politique d'utilisation des mesures cryptographiques ; • Rapport d'analyse des risques ; • Rapports de test des solutions de chiffrement ; • Politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques ; • Normes de gestion des cycles de vie des clés cryptographiques ; • Logs des activités liées à la gestion des clés ; • Rapport d'audit des activités liées à la gestion des clés.

			• Si les équipements utilisés pour générer, stocker et archiver les clés sont protégées physiquement ; • Si toutes les clés cryptographiques sont protégées contre les modifications ou la perte.		
8.25	Cycle de vie de développement sécurisé	Des règles pour le développement sécurisé des logiciels et des systèmes doivent être établies et appliquées.	• Si une politique de développement sécurisé est élaborée et mise en œuvre ; • Si une procédure de développement est élaborée et mise en œuvre ; • Si les exigences de sécurité auprès de toutes les parties prenantes dès le début de la conception sont identifiées (en considérant les conséquences des menaces, des vulnérabilités et de la non-conformité aux lois et règlements tant sur le métier et l'image de l'audité que sur les parties prenantes externes) ; • Si une analyse de la confidentialité des applications développées, permettant d'obtenir une classification des objets mis en œuvre au cours des développements (documentation, code source, code objet, notes d'étude, etc.), est réalisée ; • Si la capacité des équipes de développement à respecter les exigences de sécurité suivantes est vérifiée lors de points de contrôle établis tout au long des travaux : - une personne ne doit jamais être seule, responsable d'une tâche, pour des fonctions sensibles ; - une vérification du code source doit être réalisée par une équipe indépendante ; - une validation de la couverture des tests fonctionnels formelle doit être réalisée par les utilisateurs ; une validation formelle, de la couverture des tests relatifs aux fonctions ou dispositifs de sécurité, doit être réalisée par la fonction sécurité ; • Si, en cas de développements confiés à des sociétés de services informatiques ou de progiciels, les conditions ci-dessus sont imposées contractuellement à l'éditeur, au partenaire ou au sous-traitant ;	• Revue de la politique de développement sécurisé ; • Revue de la procédure de développement ; • Revue du document d'identification des exigences de sécurité des parties prenantes ; • Revue du document d'analyse de la confidentialité des applications développées pour la classification des objets mis en œuvre au cours des développements ; • Revue des rapports d'audit de la capacité des équipes de développement lors des points de contrôle établis au long des travaux de développement ; • Revue des contrats avec les sous- traitants dans le cas de l'externalisation du développement ; • Interviews du DSI, du RSSI, des développeurs et d'un échantillon d'utilisateurs.	• Politique de développement sécurisé ; • Procédure de développement ; • Document d'identification des exigences de sécurité des parties prenantes, • Document d'analyse de la confidentialité des applications développées pour la classification des objets mis en œuvre au cours des développements ; • Rapports d'audit de la capacité des équipes de développement lors des points de contrôle établis tout au long des travaux de développement ; • Contrats avec les sous- traitants dans le cas de l'externalisation du développement ; • Plan de formation.

			• Si les équipes concernées par le développement sont bien formées ; • Si les exigences d'octroi de licences et autres alternatives ont été pris en considération pour bénéficier de solutions rentables tout en évitant de futures difficultés liées aux licences.		
8.26	Exigences de sécurité des applications	Les exigences de sécurité de l'information doivent être identifiées, spécifiées et approuvées lors du développement ou de l'acquisition d'applications	• Si une analyse des risques de sécurité de l'information est réalisée lors du développement ou de l'acquisition d'applications ; • Si le niveau de confiance dans l'identité des entités est identifié en utilisant l'authentification par exemple ; • Si le type et les niveaux de classification d'informations à traiter par l'application sont identifiés ; • Si l'accès et les niveaux d'accès aux données et aux fonctions de l'application sont séparés) ; • S'il y a une résilience contre les attaques malveillantes ou les perturbations involontaires ; • Si les exigences légales, statutaires et réglementaires dans la juridiction où la transaction est générée, traitée, terminée ou stockée sont respectées ; • Si la protection de la vie privée est prise en considération par toutes les parties impliquées ; • Si toutes les informations confidentielles sont protégées ; • Si les données sont protégées pendant leur traitement, leur transit, et lorsqu'elles sont au repos. • Si les communications entre toutes les parties impliquées sont chiffrées de manière sécurisée ; • Si les contrôles des données d'entrée, y compris les contrôles d'intégrité et la validation des données d'entrée ont lieu ; • Si les contrôles des données de sortie ont lieu ; • Si la journalisation et la supervision des transactions sont mis en œuvre, • Si le niveau de confiance des identités déclarées pour les	• Revue du document d'analyse des risques ; • Revue des documents de projets de développement de nouvelles applications ; • Revue des cahiers des charges pour l'acquisition de nouvelles applications ; • Revue des contrats avec les fournisseurs ; • Revue des critères d'acceptation des applications ; • Revue des rapports d'évaluation des applications avant l'achat ; • Interview des responsables métier, du DSI et du RSSI ; • Revue du processus d'autorisation des personnes pouvant traiter des documents transactionnels ; • Audit des mécanismes d'authentification aux applications et de gestion des accès ; • Vérification des mécanismes de contrôle	• Document d'analyse des risques ; • Documents de projets de développement de nouvelles applications ; • Cahiers des charges pour l'acquisition de nouvelles applications ; • Contrats avec les fournisseurs ; • Critères d'acceptation des applications ; • Rapports d'évaluation des applications avant l'achat ; • Processus d'autorisation des personnes pouvant traiter des documents transactionnels ; • Rapport d'audit des mécanismes d'authentification, des droits d'accès et de contrôle des données d'entrée sortie des applications ; • Logs des serveurs hébergeant des applications utilisées sur les réseaux publics ;

			services transactionnels est identifié et documenté, • Si le niveau de confiance requis envers l'intégrité des informations échangées ou traitées, et les mécanismes d'identification du manque d'intégrité (par exemple, contrôle de redondance cyclique, hachage, signatures numériques/électroniques) pour les services transactionnels sont identifiés et documentés, • Si les processus d'autorisation liés aux personnes qui peuvent approuver le contenu, émettre ou signer des documents transactionnels importants sont définis et documentés, • Si la protection et la vérification des transactions sont gérées de façon appropriée (Incluant la confidentialité, l'intégrité, la preuve d'envoi et de réception des documents importants, la non-répudiation et la durée pendant laquelle la transaction est gardée confidentielle), • Si des moyens pour la préservation de la confidentialité et de l'intégrité, la prévention contre la perte ou la duplication des informations pour les applications de commande et de paiement électroniques sont mises en place, • Si le stockage des détails de la transaction est situé hors de tout environnement accessible au public, à l'instar d'une plateforme de stockage en place sur l'intranet de l'entité auditée, et s'il n'est pas conservé ou exposé sur un support de stockage directement accessible depuis Internet, • Si, lorsqu'une autorité de confiance est utilisée (par exemple dans le but d'émettre et de tenir à jour des signatures ou des certificats électroniques), la sécurité est intégrée et imbriquée tout au long du processus de gestion de bout en bout des certificats ou des signatures.	des données d'entrée et de sortie des applications ; • Vérification des logs des applications ; • Vérification de l'utilisation de protocoles sécurisés (ex : certificats SSL) ; • Vérification des moyens de stockage des détails des transactions ; • Vérification du processus de gestion du cycle de vie des certificats électroniques.	• Moyens de stockage des détails des transactions ; • Document du processus de gestion du cycle de vie des certificats électroniques.
		Des principes d'ingénierie de la sécurité des systèmes doivent être établis, documentés, tenus à jour et appliqués à toutes les activités de développement	• Si des procédures d'ingénierie de la sécurité des systèmes d'information, reposant sur les principes d'ingénierie de la sécurité, sont élaborées et appliquées aux activités internes d'ingénierie des systèmes d'information ; • Si cette sécurité est conçue dès le début à tous les	• Revue des procédures d'ingénierie de la sécurité des systèmes ; • Revue du rapport de conception de la sécurité ; • Revue du rapport d'analyse	• Procédures d'ingénierie de la sécurité des systèmes ; • Rapport de conception de la sécurité ; • Rapport d'analyse des nouvelles technologies au

8.27	Principes d'ingénierie et d'architecture des systèmes sécurisés	de systèmes d'information.	niveaux de l'architecture (activité, données, applications et technologie) « sécurité dès la conception», «défense en profondeur», «sécurité par défaut», «refus par défaut», «gestion sécurisée des erreurs», « se méfier des données provenant d'applications externes», «sécurité du déploiement», «présumer la compromission», « moindre privilège», «facilité d'utilisation et de gestion» et «moindre fonctionnalité» ; • Si les nouvelles technologies sont analysées au regard des risques de sécurité et si la conception est revue par rapport aux modèles d'attaques connus ; • Si ces principes d'ingénierie de la sécurité sont appliqués aux systèmes d'information externalisés par le biais de contrats et autres accords exécutoires passés entre l'entité auditée et le prestataire auprès duquel ces systèmes sont externalisés.	des nouvelles technologies au regard des risques de sécurité ; • Revue des contrats et accords exécutoires passés entre l'audité et le prestataire ; • Interviews du DSI et du RSSI.	regard des risques de sécurité ; • Contrats et accords exécutoires passés entre l'audité et le prestataire.
8.28	Codage sécurisé	Des principes de codage sécurisé doivent être appliqués au développement de logiciels.	• Si des processus sont définis pour s'assurer de la bonne gouvernance du codage sécurisé ; • Si une base de référence de sécurité minimale détaillant les principes et les lignes directrices sur le codage sécurisé, est établie et appliquée pour tous les composants logiciels ; • Si les principes de codage sécurisé suivent l'amélioration et l'apprentissage continus à travers la surveillance de l'évolution des menaces du monde réel et des conseils actualisés, ainsi que les informations sur les vulnérabilités logicielles ; • Si les principes de codage sécurisé sont appliqués à toute activité de développement aussi bien au sein de l'entité auditée que pour les produits et services fournis par l'entité auditée à des tiers ou provenant de parties tierces et de logiciels open source ; • Si les principes de codage sécurisé couvrent les différentes phases de codage à savoir : planification et prérequis avant le codage, pendant le codage et révision & maintenance ; • Si les principes de codage sécurisé sont utilisés à la	• Revue des processus mis en œuvre liés à la gouvernance du codage sécurisé ; • Revue de la base de référence de sécurité minimale ; • Revue des rapports d'audit applicatifs, • Interviews des administrateurs BD et applications ; • Interview d'un échantillon de développeurs et testeurs ; • Revue des rapports de tests de la sécurité des applications pendant et après le développement ;	• Processus de la gouvernance du codage sécurisé ; • Base de référence de sécurité minimale ; • Inventaire des application s ; • Rapports d'audit applicatif ; • Rapports de tests effectués.

			fois pour les nouveaux développements ainsi que pour les cas de réutilisation ; • Si des tests de la sécurité des applications sont effectués pendant et après le développement.	• Audit des applications.	
8.29	Tests de sécurité dans le développement et l'acceptation	Des processus pour les tests de sécurité doivent être définis et mis en œuvre au cours du cycle de vie de développement.	• Si des tests des fonctions de sécurité (par exemple, l'authentification des utilisateurs, les restrictions d'accès et l'utilisation de la cryptographie) sont effectués ; • Si le codage est sécurisé ; • Si les paramétrages de sécurité et règles de configuration (suppression de tout compte générique, changement de tout mot de passe générique, fermeture de tout port non explicitement demandé et autorisé) font l'objet d'une liste précise tenue à jour ; • Si un plan de test détaillé (comprenant un programme détaillé des activités et des tests, les données d'entrée et les données de sortie attendues sous un ensemble de conditions, et les critères pour évaluer les résultats) est élaboré et mise en œuvre ; • Si les tests de sécurité sont intégrés au cycle de vie de développement ; • Si des outils automatiques, tels que des outils d'analyse de code ou des scanneurs de vulnérabilités sont utilisés ; • Si des tests d'acceptation indépendants sont réalisés dans le cas des développements réalisés en interne ; • Si un processus d'acquisition est élaboré est mis en œuvre ; • Si les contrats conclus avec le fournisseur traitent les exigences de sécurité identifiées ; • Si les produits et les services sont évalués par rapport aux exigences de sécurité avant l'acquisition ; • Si les tests sont réalisés dans un environnement de test indépendant et ressemblant le plus possible à l'environnement opérationnel cible ; • Si les tests et la surveillance des environnements, outils	• Revue du plan des tests ; • Revue du programme des tests ; • Revue des rapports des tests ; • Interviews des responsables de tests, du DSI et du RSSI ; • Revue de la liste des paramètres de sécurité et règles de configuration ; • Audit de ces paramètres et règles de configuration ; • Revue des rapports des outils d'analyse de code et des scanners de vulnérabilité ; • Revue des contrats avec les fournisseurs ; • Revue de rapport d'évaluation de produit lors de l'acquisition.	• Plan des tests ; • Programme des tests ; • Rapports des tests ; • Liste des paramètres de sécurité et règles de configuration ; • Rapport d'audit de ces paramètres et règles de configuration ; • Rapports des outils d'analyse de code et des scanners de vulnérabilité ; • Les contrats avec les fournisseurs ; • Rapport d'évaluation de produit à acheter.

			et technologies de test sont effectués.		
8.30	Développement externalisé	Les activités relatives au développement externalisé des systèmes doivent être dirigées, contrôlées et vérifiées.	• Si les questions d'accords de licence et les sujets de de propriété intellectuelle du code développé ont été réglées ; • Si les exigences contractuelles relatives à la sécurité du code source sont formalisées ; • Si des tests d'acceptation pour assurer la qualité et l'exactitude des livrables sont effectués ; • Si des moyens de protection de la vie privée sont mis en place ; • Si des preuves montrant qu'il a été procédé à suffisamment de tests pour garantir l'absence de vulnérabilités connues sont communiquées ; • Si des accords de séquestre (par exemple si le code source n'est plus disponible) sont conclus ; • Si le contrat avec le sous-traitant prévoit le droit de l'audité de procéder à un audit des processus et des contrôles de développement ; • Si la législation applicable (par exemple, sur la protection des données à caractère personnel) est prise considération lors du développement des systèmes.	• Revue des licences des systèmes développés par les sous-traitants ; • Revue des contrats de développement des systèmes ; • Revue des rapports des tests communiqués par les sous-traitants ; • Revue des accords de séquestre des codes source conclus le cas échéant ; • Interview du DSI ; • Revue des rapports des tests d'acceptation.	• Licences des systèmes développés par les sous-traitants ; • Contrats de développement des systèmes ; • Rapports des tests communiqués par les sous-traitants ; • Accords de séquestre des codes source conclus ; • Rapports des tests d'acceptation.
8.31	Séparation des environnements de développement, de test et opérationnels	Les environnements de développement, de test et opérationnels doivent être séparés et sécurisés pour réduire les risques d'accès ou de changements non autorisés dans l'environnement opérationnel.	• Si des procédures de développement, de test et d'intégration sont élaborées et mises en œuvre ; • Si les niveaux de séparation entre les environnements de développement, de test et opérationnels sont définis, documentés et mis en œuvre ; • Si les règles et les autorisations pour le déploiement de logiciels depuis le développement jusqu'à l'état de production sont définies, documentées et mises en œuvre ; • Si les environnements de développement et de test sont protégés (l'application de correctifs et de mises à jour sur tous les outils de développement, d'intégration et de test, la configuration sécurisée des systèmes et des logiciels, le contrôle de l'accès aux	• Revue des procédures de développement, • Interviews de l'administrateur système, du DSI et d'un échantillon de développeurs et testeurs ; • Revue des fiches de postes ; • Revue du schéma de l'architecture réseau ; • Vérification sur les serveurs ; • Audit des comptes	• Procédures de développement ; • Inventaire des serveurs des environnements de développement, de test et opérationnels ; • Fiches de postes ; • Schéma de l'architecture réseau ; • Rapport d'audit des comptes d'accès aux environnements de

			environnements) ; • Si un processus de séparation des tâches, de vérification et d'approbation des changements est défini, documenté et mis en œuvre ; • Si des mesures de surveillance et de détection des changements non autorisés (exemple : la journalisation) sont mises en œuvre.	d'accès aux environnements de développement.	développement.
8.32	Gestion des changements	Les changements apportés aux moyens de traitement de l'information et aux systèmes d'information doivent être soumis à des procédures de gestion des changements.	• S'il existe une procédure de gestion des changements permettant de contrôler les changements à apporter aux moyens de traitement de l'information et aux systèmes d'information (mise en production de nouveaux systèmes/équipements/logiciels ou d'évolutions de systèmes existants) ; • Si cette procédure englobe la gestion des demandes de changement et leur validation, l'analyse des risques potentiels des changements, la planification et l'affectation des rôles et responsabilités, la communication à l'ensemble des personnes concernées, les tests de changements et la mise en production des changements ; • Si une procédure de contrôle des changements pendant le cycle de vie de développement de tout le système, depuis les étapes de conception initiales jusqu'aux activités de maintenance ultérieures est élaborée et mise en œuvre ; • Si les niveaux d'autorisation accordés pour les changements sont définis et tenus à jour ; • Si les propositions de changements émanent d'utilisateurs autorisés ; • Si tout logiciel, information, élément de base de données et matériel nécessitant un changement sont identifiés ; • Si un accord formel pour les propositions détaillées est obtenu avant le lancement des travaux ; • Si les utilisateurs autorisés acceptent les changements avant leur mise en œuvre ; • Si la documentation système est mise à jour après chaque changement et si l'ancienne documentation est	• Revue de la procédure de gestion des changements ; • Revue par échantillonnage, du processus de gestion des changements : gestion des demandes de changement et leur validation, analyse des risques potentiels des changements, planification et affectation des rôles et responsabilités, communication à l'ensemble des personnes concernées, test de changements et mise en production des changements ; • Interviews du RSSI, DSI et des administrateurs système, BD et réseau ; • Revue du registre des niveaux d'autorisation accordés ; • Revue de la liste des logiciels, informations, éléments de BD et matériel nécessitant un changement ; • Revue des accords pour	• Procédure de gestion des changements, • Enregistrements liés au processus de gestion des changements, • Registre des niveaux d'autorisation accordés, • Liste des logiciels, informations, éléments de BD et matériel nécessitant un changement, • Accords pour les propositions détaillées, • Liste des demandes de changements, • Rapports des changements effectués, • Documentation système, • Rapport d'analyse des risques des changements, • Plans de continuité de l'activité.

			archivée ou mise au rebut ; • Si un système de traçabilité de toutes les demandes de changement est tenu à jour ; • Si une revue et des tests de l'impact des modifications apportées à la plateforme d'exploitation sur les applications critiques sont réalisés ; • Si les plans de continuité de l'activité et les procédures de réponse et de reprise sont modifiés en conséquence.	les propositions détaillées ; • Revue des demandes de changements ; • Revue des rapports des changements effectués ; • Revue de la documentation système ; • Vérification du système de contrôle des versions de logiciels ; • Vérification des mises à jour des systèmes critiques ; • Revue des plans de continuité de l'activité.	
8.33	Informations de test	Les informations de test doivent être sélectionnées avec soin, protégées et gérées de manière appropriée.	• Si les mêmes procédures de contrôle d'accès aux environnements opérationnels sont applicables aux environnements de test ; • Si, lorsque des données personnelles ou sensibles doivent malgré tout être utilisées, on prend le soin de supprimer les détails et contenus sensibles avant de les utiliser (ou de les modifier afin de les rendre anonymes) ; • Si une nouvelle autorisation est obtenue chaque fois qu'une information d'exploitation est copiée dans un environnement de test ; • Si les informations d'exploitation sont effacées immédiatement d'un environnement de test après la fin des tests ; • Si toute reproduction et utilisation de l'information d'exploitation est journalisée, afin de créer un système de traçabilité.	• Revue de la procédure de contrôle d'accès ; • Revue des autorisations de copie des informations d'exploitation sur un environnement de test ; • Interviews du DSI, des responsables de développement et de test ; • Revue des informations de test pour l'identification des informations d'exploitation.	• Procédure de contrôle d'accès ; • Liste des autorisations de copie des informations d'exploitation sur un environnement de test ; • Logs des accès sur les systèmes de test ; • Registres de reproduction et d'utilisation de l'information d'exploitation ; • Échantillon des informations d'exploitation trouvées dans les données de test.

8.34	Protection des systèmes d'information pendant les tests d'audit	Les tests d'audit et les autres activités d'assurance impliquant l'évaluation des systèmes opérationnels devraient être planifiés et convenus entre le testeur et le niveau approprié du management.	• Si les demandes d'audit pour l'accès aux systèmes et aux données avec le niveau approprié du management ont été convenues ; • Si une procédure formelle d'audit des systèmes d'information, définissant les règles concernant les audits menés sur les systèmes opérationnels/ réseaux et les responsabilités associées, est élaborée et mise en œuvre ; • Si le périmètre des tests d'audit techniques est bien identifié et contrôlé ; • Si les tests d'audit sont limités à un accès en lecture seule aux logiciels et aux données ; • Si tous les accès à des fins d'audit et de test sont bien surveillés et journalisés.	• Revue de la procédure d'audit des systèmes d'information ; • Interview du RSSI.	• Procédure d'audit des systèmes d'information.