

ANNEXE A

Référentiel d’Audit de la Sécurité des Systèmes d’Information

Évolutions du document

|  |  |  |
| --- | --- | --- |
| Version | Date | Nature des modifications |
| 1.0 | 19/12/2018 | Version initiale |
| 1.1 | 05/01/2015 | Version mise à jour |
| 1.2 | 03/06/2015 | MAJ des intitulés des domaines |
| 2.0 | 10/05/2018 | Alignement avec la norme ISO/IEC 27002 :2013 |

Pour toute remarque

|  |  |  |
| --- | --- | --- |
| Contact | @ Mail | Téléphone |
| Direction de l’Audit de la Sécurité des Systèmes d’Information | [Audit@ansi.tn](mailto:Audit@ansi.tn) | 71 846 020 |

Critère de diffusion

|  |  |  |  |
| --- | --- | --- | --- |
| Public | Interne | Diffusion restreinte | Hautement confidentiel |

# 1. Avant-propos

L’audit de la sécurité des systèmes d’information en Tunisie est stipulé par la loi n° 5 de 2004 et organisé par les décrets applicatifs 2004-1249 et 2004-1250. Les décrets cités identifient les organismes soumis à l’obligation de l’audit, les experts auditeurs habilités à mener des missions d’audit, la démarche de certification de ces experts auditeurs, ainsi que les étapes clés de la mission d’audit et les livrables à fournir à l’organisme audité à la fin de la mission. Cependant, les contrôles de sécurité à vérifier n’ont pas été identifiés au niveau de ces décrets.

Ainsi, l’ANSI estime qu’il est nécessaire d’identifier les critères d’audit à travers un document de référentiel qui permettra d’accompagner les experts auditeurs dans la réalisation des missions d’audit de sécurité des systèmes d’information, aux organismes audités de disposer de garanties sur la qualité des audits effectués et aux services de suivi de l’audit au sein de l’ANSI de mener efficacement l’étude et l’évaluation des rapports d’audit.

Ce référentiel comprend les contrôles de sécurité nécessaires pour le maintien d’un système de gestion de la sécurité et que l’expert auditeur est appelé à vérifier lors de la mission d’audit.

# 2. Objectif

Le présent document détaille les critères par rapport auxquels l’audit est réalisé conformément aux exigences de la loi 2004-05 et ses décrets applicatifs.

Le présent document est un document de référence pour :

* L’ANSI, organisme certificateur des experts auditeurs et garant de la qualité des missions d’audit, pour la validation des rapports d’audit,
* Les experts auditeurs qui réalisent les missions d’audit, pour les accompagner à conduire la mission conformément aux exigences du présent référentiel
* Les audités, bénéficiaires de la mission d’audit, pour assurer un meilleur suivi de ladite mission.

# 3. Domaine d’application

Ce référentiel est applicable à tous les organismes soumis à l’obligation de l’audit conformément aux exigences de de la loi 2004-05 et ses décrets applicatifs.

# 4. Références

* Loi n° 2004-5 du 3 février 2004, relative à la sécurité informatique et portant sur l'organisation du domaine de la sécurité informatique et fixant les règles générales de protection des systèmes informatiques et des réseaux,
* Décret n° 2004-1250 du 25 mai 2004, fixant les systèmes informatiques et les réseaux des organismes soumis à l'audit obligatoire périodique de la sécurité informatique et les critères relatifs à la nature de l'audit et à sa périodicité et aux procédures de suivi de l'application des recommandations contenues dans le rapport d'audit,
* La norme ISO 18045, qui fournit une méthodologie pour l’évaluation de la sécurité IT,
* La norme ISO 19011 :2011, qui fournit les lignes directrices sur l’audit interne ou externe d’un système de management et l’évaluation des compétences des équipes d’audit,
* La norme ISO 22301 :2012, Gestion de la continuité des affaires,
* La norme ISO 27001 :2013, Système de management de la sécurité de l’information,
* La norme ISO 27002 :2013, Code de bonnes pratiques pour le management de la sécurité de l'information,
* La norme ISO 27005 :2008, Gestion du risque en sécurité de l’information,
* ITIL (Information Technology Infrastructure Library (« Bibliothèque pour l'infrastructure des technologies de l'information ») est un ensemble d'ouvrages recensant les bonnes pratiques (« best practices ») du management du système d'information.

# 5. Termes et définitions

**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 peuvent être classées en 4 catégories :

* La preuve physique : c'est ce que l'on voit, constate = observation,
* La preuve testimoniale : témoignages. C'est une preuve très fragile qui doit toujours être recoupée et validée par d'autres preuves,
* La preuve documentaire : procédures écrites, comptes rendus, notes,
* La preuve analytique : résulte de calculs, rapprochements, déductions et comparaisons diverses. **Critères d’audit** : Ensemble de politiques, procédures ou exigences déterminées par rapport auxquelles la conformité du système est évaluée (contrôles au niveau de la norme ISO/IEC 27002 :2013).

**Plan d’audit** : Description des activités et des dispositions nécessaires pour réaliser un audit, préparé par le responsable de l’audit, en commun accord entre l’équipe de l’audit et l’audité pour faciliter la programmation dans le temps et la coordination des activités d’audit.

**Champ d’audit** : Etendu et limites d’un audit, le champ décrit généralement les lieux, les unités organisationnelles, les activités et les processus ainsi que la période de temps couverte.

**Constats d’audit** : Résultats de l'évaluation des preuves d'audit recueillies, par rapport aux critères d'audit.

# 6. Documents requis pour la revue

Les documents requis pour la revue sont, sans s’y limiter :

* L’ensemble des politiques de sécurité de l’information de l’audité, approuvées par la direction,
* Le manuel de procédures relatif à la sécurité de l’information, qui doit comprendre 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
  + La procédure d’autorisation pour l’ajout d’outil 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, …)
  + La procédure de développement, test et 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

# 7. Domaines couverts par l’audit de la sécurité des systèmes d’information

L’audit de la sécurité des systèmes d’information est un jalon de l’amélioration de la maturité de la sécurité du système d’information en vue d’établir un équilibre entre les risques et les bénéfices de l’utilisation des moyens de traitement de l’information et d’assurer une amélioration quantifiable, efficace et efficiente des processus qui s’y rapporte. Le référentiel d’audit repose sur la norme ISO/IEC 27002 :2013.

S’agissant d’un audit réglementaire et non pas d’un audit de la politique de sécurité des systèmes d’information (PSSI), ni d’un audit de la mise en œuvre de cette PSSI, l’auditeur est tenu de vérifier pour chaque domaine :

* la conformité par rapport aux critères d’audit au niveau des documents de référence de l’audité (PSSI, procédures, etc.) le cas échéant,
* la conformité des pratiques de sécurité par rapport à ces critères d’audit.

# 8. Echantillonnage

Les critères d’échantillonnage pour chaque type de composante du système d’information à auditer doivent être bien définis et justifiés.

# 9. Types de vérification

Les vérifications à effectuer tout au long de la mission d’audit sont de type organisationnel, physique ou technique présentés par la légende suivante :

|  |  |
| --- | --- |
| Type | Couleur |
| Organisationnel |  |
| Physique |  |
| Technique |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
| **A.5** | **Politiques de sécurité de l’information** | | | | | | |
| **A.5.1** | Orientations de la direction en matière de sécurité de  l’information | Apporter à la sécurité de l’information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur. | | | | | |
| **A.5.1.1** | Politiques de sécurité de l’information | Un ensemble de politiques de sécurité de  l’information (PSI) doit être défini,  approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés. | S'il existe des documents de politiques de sécurité de  l’information, qui sont approuvées par la direction, publiées et communiquées, à tous les utilisateurs du SI et aux tiers concernés | * Revue des documents de PSI, * Entretien avec le DG, * Interviews d’un échantillon des utilisateurs, * Revue des PVs de réunion du comité de sécurité |  |  | |
| **A.5.1.2** | Revue des politiques de sécurité de  l’information | Les politiques de sécurité de l’information doivent être revues à intervalles programmés ou en cas de changements majeurs pour garantir leur pertinence, leur adéquation et leur effectivité dans le temps. | * Si ces politiques sont passées en revue par un comité de sécurité de haut niveau à intervalles planifiés, ou si des changements importants se produisent pour s'assurer qu'elles sont toujours pertinentes, adéquates et efficaces, * S’il existe des procédures en place pour le réexamen des politiques de sécurité de   l’information |
| **A.6** | **Organisation de la sécurité de l’information** | | | | | | |
| **A.6.1** | Organisation interne | Établir un cadre de management pour lancer et vérifier la mise en place et le fonctionnement opérationnel de la sécurité de  l’information au sein de l’organisme. | | | | | |
| **A.6.1.1** | Fonctions et  responsabilités | Toutes les responsabilités  en matière de sécurité de | * Si un RSI, doté d’un pouvoir décisionnel et assurant le | * Revue de l’organigramme, des fiches de poste, des décisions et notes |  | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  | liées à la sécurité de l’information | l’information doivent  être définies et attribuées. | reporting directement à la direction, 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. | internes en relation avec la sécurité du SI,   * Entretien avec le DG, * Interview du RSI (le cas échéant). |  |  |
| **A.6.1.2** | Séparation des tâches | Les tâches et les domaines de responsabilité incompatibles doivent être cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l’organisme. | * Si les tâches incompatibles Sont identifiées et les responsabilités sont 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 poste, * Entretien 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 concernés, * Vérification des contrôles compensatoires en cas en cas d’attribution des tâches   incompatibles à la même personne. |  |  |
| **A.6.1.3** | Relations avec les autorités | Des relations appropriées avec les autorités compétentes doivent être entretenues. | * Si les autorités avec lesquelles l’organisme 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'échange | * Revue de la liste de ces autorités, * Revue de la procédure d’échange, * Entretien avec les responsables des différents services pour   l’identification des autorités compétentes. |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | entre l’organisme et ces autorités est définie et mise en œuvre. |  |  |  |
| **A.6.1.4** | Relations avec des groupes de travail spécialisés | Des relations appropriées avec des groupes d’intérêt, des forums spécialisés dans la sécurité et des associations professionnelles doivent être entretenues. | * Si des groupes d’intérêt, des forums spécialisés dans la sécurité et des associations professionnelles ont été identifiés, * Si des relations sont entretenues 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 RSI pour l’identification de ces groupes et les relations éventuelles entretenues avec eux. |  |  |
| **A.6.1.5** | La sécurité de l’information dans la gestion de projet | La sécurité de l’information doit être considérée dans la gestion de projet,  quel que soit le type de projet concerné. | * 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, * Si l'expression des besoins de sécurité (confidentialité, intégrité, disponibilité), est prise en considération dans la gestion des projets, * Si une coordination entre les différents services concernés par | * 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 RSI, * Interview des responsables métier. |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **MOYEN DE VERIFICATION** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  |  | ces projets est mise en place dès la phase d'expression de ces besoins et maintenue pendant toutes les phases des projets pour la planification de l'allocation des ressources  nécessaires, |  |  | |  |
| **A.6.2** | Appareils mobiles et  télétravail | Assurer la sécurité du télétravail et de l’utilisation d’appareils mobiles. | | | | | |
| **A.6.2.1** | Politique en matière d’appareils mobiles | Une politique et des mesures de sécurité complémentaires doivent être adoptées pour gérer les risques découlant de  l’utilisation des appareils mobiles. | * Si une analyse des risques d'utilisation des appareils mobiles est réalisée, * Si une politique d'utilisation des appareils mobiles est élaborée et mise en œuvre, | * Revue de la politique d’utilisation des appareils mobiles, * Interview du RSI, * Interview du responsable réseau, |  |  | |
|  |
| **A.6.2.2** | Télétravail | Une politique et des mesures de sécurité complémentaires doivent être mises en œuvre pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail. | Pour les organismes autorisant les activités de télétravail :   * Si une politique définissant les conditions et les restrictions à l’utilisation du télétravail, * Si une procédure organisant le télétravail est développée et   mise en œuvre. | * Revue de la politique sur l’utilisation du télétravail, * Revue de la procédure organisant le télétravail, * Revue du rapport d’analyse des risques relatifs au domicile des utilisateurs et/ou des sites distants, |  |  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.7** | **Sécurité des ressources humaines** | | | | | |
| **A.7.1** | Avant l’embauche | S’assurer que les salariés et les sous-traitants comprennent leurs responsabilités et sont qualifiés  pour les rôles qu’on envisage de leur donner. | | | | |
| **A.7.1.1** | 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 | * 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 | * Revue du statut et du règlement intérieur, * Revue de la procédure de recrutement, * Revue du dossier du RSI et d'un échantillon de personnes impliqués dans la sécurité, |  |  |
| **9** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** | |
|  |  | classification des informations accessibles et aux risques identifiés. | 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’organisme | * Interview du DRH. |  |  | |
| **A.7.1.2** | Termes et conditions d’embauche | Les accords contractuels entre les salariés et les sous-traitants doivent préciser leurs responsabilités et celles de l’organisme en matière de sécurité de l’information. | * Si les employés et les sous- traitants sont invités à signer un engagement de confidentialité ou de non-divulgation dans le cadre de leurs termes et conditions initiaux du contrat de travail, * Si cet engagement de confidentialité couvre la responsabilité de l'audité et des employés et des sous-traitants concernant la sécurité de   l’information. | * Revue d’un échantillon des engagements de confidentialité, * Interview du DRH et du DAF. |  |  | |
| **A.7.2** | Pendant la durée du  contrat | S’assurer que les salariés et les sous-traitants sont conscients de leurs responsabilités en matière de  sécurité de l’information et qu’ils assument ces responsabilités. | | | | | |
| **A.7.2.1** | Responsabilités de la direction | La direction doit demander à tous les salariés et sous- traitants d’appliquer  les règles de sécurité de l’information | * Si la direction exige explicitement (par une note interne signée par le DG) que les employés et les sous-traitants appliquent les | * Revue de la note interne signée par le DG, * Revue d’un échantillon de contrats avec les sous-traitants, |  | |  |
| **10** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  | conformément aux politiques et aux procédures en vigueur dans l’organisme. | exigences de sécurité conformément aux politiques et procédures établies par l’audité. | * Entretien avec le DG, * Interview du DRH et du DAF. |  |  |
| **A.7.2.2** | Sensibilisation, apprentissage et formation à la sécurité de  l’information | L’ensemble des salariés de l’organisme et, quand cela est pertinent, des sous- traitants, doit bénéficier d’une sensibilisation et de formations adaptées et recevoir régulièrement les mises à jour des politiques et procédures de  l’organisme s’appliquant à leurs fonctions. | * Si les nouvelles recrues de l'audité, et le cas échéant, les nouveaux sous-traitants reçoivent systématiquement des sessions de sensibilisation à la sécurité du système   d’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 et 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 (RSI, DSI, Administrateurs, développeurs) ont reçus les formations spécialisées sur la sécurité des produits utilisés et sur la gestion   de la sécurité de manière | * Revue des programmes de formation et de 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. |  |  |
| **11** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  |  | générale pendant les 3 dernières  années. |  |  | |  |
| **A.7.2.3** | Processus disciplinaire | Un processus disciplinaire formel et connu de tous doit exister pour prendre des mesures à l’encontre des salariés ayant enfreint les règles liées à la 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. | * Revue du statut et du règlement intérieur, * Interview du DRH. |  | |  |
| **A.7.3** | Rupture, terme ou modification du contrat  de travail | Protéger les intérêts de l’organisme dans le cadre du processus de modification, de rupture ou de terme d’un contrat de travail. | | | | | |
| **A.7.3.1** | Achèvement ou modification  des responsabilités associées au contrat de travail | Les responsabilités et les missions liées à la sécurité de l’information qui  restent valables à l’issue de la rupture, du terme ou de la modification du  contrat de travail, doivent être définies, communiquées au salarié ou au sous-traitant, et appliquées. | * Si les responsabilités en fin ou modification de contrat sont clairement définies et attribuées, * 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, | * 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 modification de contrat, |  |  | |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
| **A.8** | **Gestion des actifs** | | | | | |
| **A.8.1** | Responsabilités  relatives aux actifs | Identifier les actifs de l’organisme et définir les responsabilités pour une protection appropriée. | | | | |
| **A.8.1.1** | Inventaire des actifs | Les actifs associés à l’information et aux  moyens de traitement de l’information  doivent être identifiés et un inventaire de ces actifs doit être dressé  et tenu à jour. | * S’il existe des règles relatives à   l’inventoring des actifs au niveau de la PSI, qui exigent le maintien d’un inventaire des actifs,   * Si des procédures d’inventoring des actifs sont développées et maintenues, * Si un inventaire ou registre est maintenu pour tous les actifs de   l’audité. | * Revue de la PSI pour l’identification des règles relatives à l’inventoring, * Revue des procédures d’inventoring des actifs, * Revue de l’inventaire et vérification de son exhaustivité, * Interview du DAF, * Interview du DSI. |  |  |
| **A.8.1.2** | Propriété des actifs | Les actifs figurant à  l’inventaire doivent être attribués à un propriétaire. | * Si chaque actif identifié a un propriétaire | * Revue de l’inventaire et vérification de l’existence du nom du propriétaire de chaque actif. |  |  |
| **A.8.1.3** | Utilisation correcte des actifs | Les règles d’utilisation  correcte de l’information, les actifs associés à  l’information et les moyens de traitement de  l’information doivent être identifiées, documentées et mises en œuvre. | * Si une politique d'utilisation correcte de l'information, des actifs associés et des moyens de son traitement est élaborée et mise en œuvre, * Si les employés et les sous- traitants ont été sensibilisés aux exigences de sécurité comprises dans cette politique et de leur   responsabilité de l’utilisation de ces actifs. | * Revue de la politique d’utilisation correcte de l’information, * Revue d’un échantillon de contrats avec les sous-traitants ayant l’accès aux moyens de traitement de   l’information,   * Interview du RSI et du DSI, * Interview du DRH et du DAF. |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
| **A.8.1.4** | Restitution des actifs | Tous les salariés et les utilisateurs tiers doivent restituer la totalité des actifs de l’organisme qu’ils ont en leur possession au terme de la période  d’emploi, du contrat ou de l’accord. | * Si la restitution des actifs en possession des salariés et des utilisateurs tiers au terme de la période de l’emploi ou de   l’accord est documentée, | * Revue des documents relatifs aux fins de période de l’emploi et des contrats des sous-traitants (ex : PVs de passation, PVs de réception   définitives, …), |  | |  |
|  |
| **A.8.2** | Classification de  l’information | S’assurer que l’information bénéficie d’un niveau de protection approprié conforme à son importance  pour l’organisme. | | | | | |
| **A.8.2.1** | Classification des informations | Les informations doivent être classifiées en termes d’exigences légales, de valeur, de caractère critique et de sensibilité au regard d’une divulgation ou modification non autorisée. | * S’il existe des règles relatives à la classification des actifs selon leurs exigences de sécurité au niveau de la PSI, * Si des procédures de classification des actifs sont   développées et maintenues, | * Revue de la PSI, * Revue des procédures de classification des actifs, * Interview des responsables métier, |  |  | |
|  |
| **A.8.2.2** | Marquage des informations | Un ensemble approprié de procédures pour le marquage de l’information doit être élaboré et mis en œuvre conformément au | * Si des procédures de marquage de l'information conformément à la classification établie sont élaborées et mises en œuvre. | * Revue des procédures de marquage de l’information, * Interview des responsables métier, * Vérification de marquage sur un échantillon de documents. |  |  | |
| **14** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  | plan de classification  adopté par l’organisme. |  |  |  | |  |
| **A.8.2.3** | Manipulation des actifs | Des procédures de  traitement de l’information doivent être élaborées et mises en œuvre conformément au plan de classification de  l’information  adopté par l’organisme. | * Si des procédures pour une utilisation acceptable de l'information et des actifs associés à un moyen de traitement de l'information sont élaborées et mises en œuvre, | * Revue des procédures de traitement de l’information, * Revue de la matrice des droits   d’accès aux informations et à leurs copies,   * Interview des responsables métier, * Vérification des contrôles d’accès mis en place par rapport à la matrice des droits d’accès, * Vérification des logs des actions sur un échantillon d’informations classifiées critique. |  | |  |
|  |
| **A.8.3** | Manipulation des  supports | Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de l’information de l’organisme stockée sur des  supports. | | | | | |
| **A.8.3.1** | Gestion des supports amovibles | Des procédures de gestion des supports amovibles doivent être mises en  œuvre conformément au plan de classification adopté par l’organisme. | * Si des procédures de gestion des supports amovibles sont   élaborées et mises en œuvre conformément à la classification établie, | * Revue des procédures de gestion des supports amovibles, * Interview des responsables métier, * Test de récupération du contenu d’un support devant être retiré, * Test de visualisation du contenu |  |  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.8.3.2** | Mise au rebut des supports | Les supports qui ne sont plus nécessaires doivent être mis au rebut de manière sécurisée en suivant des procédures formelles. | * Si une procédure de mise au rebut d'une manière sécurisée des supports en tenant compte de la classification adoptée (formatage bas niveau,   destruction, …) est élaborée et mise en œuvre,   * Si cette mise au rebut est journalisée. | * Revue de la procédure de mise au rebut des supports, * Revue des journaux des mises au rebut, * Interview du DSI et de l’archiviste. |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** | |
| **A.8.3.3** | Transfert physique des supports | Les supports contenant de l’information doivent être protégés contre les accès non autorisés, les erreurs d’utilisation et l’altération lors du transport. | * Si une liste des transporteurs autorisés est convenue avec la direction, * Si une procédure pour vérifier l'identification des transporteurs est élaborée et mise en œuvre, | * Revue de la procédure de vérification de l'identification des transporteurs, * Revue des registres de transport, * Revue d’un échantillon d’emballage utilisé, * Interview du DAF. |  |  | |
|  |
| * Si les informations identifiant le contenu du support, la protection appliquée ainsi que la date et l’heure de son transfert au transporteur ainsi que la date et l’heure de sa réception au lieu de destination sont journalisées   et conservées. |
| **A.9** | **Contrôle d’accès** | | | | | | |
| **A.9.1** | Exigences métier en matière de contrôle  d’accès | Limiter l’accès à l’information et aux moyens de traitement de l’information. | | | | | |
| **A.9.1.1** | Politique de contrôle d’accès | Une politique de contrôle d’accès doit être établie, documentée et revue sur | * Si les données de l’audité, leurs propriétaires, les systèmes ou personnes qui ont besoin des | * Revue de la politique de contrôle d'accès, * Revue des procédures de contrôle |  | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  | la base des exigences métier et de sécurité de l’information. | accès à ces données, leurs rôles selon le principe du "besoin de savoir" sont identifiés,   * Si les risques d'accès non autorisé aux données sont identifiés, * Si une politique de contrôle d'accès dans le cadre de la politique de sécurité de   l'information de l’audité 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. | d'accès aux différents systèmes,   * Interviews des responsables métiers pour :   + l’identification des données, de leurs propriétaires, les systèmes ou personnes qui ont besoin des accès à ces données et leurs rôles,   + l’identification des risques d’accès non autorisé à ces données. |  |  |
| **A.9.1.2** | Accès aux réseaux et aux services réseau | Les utilisateurs doivent avoir uniquement accès au réseau et aux services réseau pour lesquels ils ont spécifiquement reçu une autorisation. | * Si une procédure de contrôle d'accès au réseau de l’audité est élaborée et mise en œuvre en application de la politique de contrôle d'accès, * Si les entités qui peuvent avoir accès aux réseaux de l’audité sont identifiées, * Si les accès nécessaires pour chaque entité selon le principe du « moindre privilège » sont identifiés, * Si les rôles et les responsabilités | * 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 »,   * Revue de la définition des rôles et des responsabilités de chaque service interne dans l'attribution de |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  |  | de chaque service interne dans l'attribution de ces accès sont définis. | ces accès,   * Revue des ACL sur les équipements réseau et de sécurité (Switchs, routeurs, firewalls, …) * Interview de l’administrateur réseau. |  | |  |
| **A.9.2** | Gestion de l’accès  utilisateur | Maîtriser l’accès utilisateur par le biais d’autorisations et empêcher les accès non autorisés aux systèmes  et services d’information. | | | | | |
| **A.9.2.1** | Enregistrement et désinscription des utilisateurs |  |  |  |  |  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
| **A.9.2.2** | Distribution des accès aux utilisateurs |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.9.2.3** | Gestion des droits d’accès à privilèges |  |  |  |  |  |
| **A.9.2.4** | Gestion des informations secrètes  d’authentification des utilisateurs |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.9.2.5** | Revue des droits d’accès utilisateurs |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.9.2.6** | Suppression ou adaptation  des droits d’accès |  |  |  |  |  |
| **A.9.3** | Responsabilités des  utilisateurs | Rendre les utilisateurs responsables de la protection de leurs informations d’authentification. | | | | |
| **A.9.3.1** | Utilisation  d’informations secrètes  d’authentification |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** | |
|  |  |  |  |  |  |  | |
| **A.9.4** | Contrôle de l’accès au système et à  l’information | Empêcher les accès non autorisés aux systèmes et aux applications. | | | | | |
| **A.9.4.1** | Restriction d’accès à |  |  |  |  | |  |
| **24** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  | l’information |  |  |  | . |  |
| **A.9.4.2** | Sécuriser les procédures de connexion |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.9.4.3** | Système de gestion des mots de passe |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  | |
| **A.9.4.4** | Utilisation de programmes utilitaires à privilèges |  |  |  |  |  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.9.4.5** | Contrôle d’accès au code source des programmes |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.10** | **Cryptographie** | | | | | |
| **A.10.1** | Mesures  cryptographiques | Garantir l’utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité,  l’authenticité et/ou l’intégrité de l’information. | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
| **A.10.1.1** | Politique d’utilisation des mesures cryptographiques | Une politique d’utilisation des mesures cryptographiques en vue de protéger l’information doit être élaborée et mise en œuvre. | * Si une politique d’utilisation des mesures cryptographiques 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’organisme,   * Si le niveau de protection requis, 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, | * Revue de la politique d’utilisation des mesures cryptographiques, * Revue de rapport d’analyse des risques, * Entrevue avec le DG, * Interview 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. |  |  |
|  |
| **A.10.1.2** | Gestion des clés | Une politique sur  l’utilisation, la protection et | * Si une politique sur l’utilisation, la protection et la durée de vie | * Revue de la politique sur   l’utilisation, la protection et la durée |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** | |
|  |  | la durée de vie des clés cryptographiques doit être élaborée et mise en œuvre tout au long de leur cycle 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,   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. | 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 vigueurs, * vérification des logs et du rapport d’audit des activités liées à la gestion des clés. |  |  | |
| **A.11** | **Sécurité physique et environnementale** | | | | | | |
| **A.11.1** | Zones sécurisées | Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l’information et  les moyens de traitement de l’information de l’organisme. | | | | | |
| **A.11.1.1** | Périmètre de sécurité physique |  |  |  |  | |  |
| **31** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.11.1.2** | Contrôle d’accès physique | Les zones sécurisées doivent être protégées par des contrôles adéquats à  l’entrée pour s’assurer que seul le personnel autorisé est admis. | * Si une procédure de contrôle   d’accès physique est élaborée et mise en œuvre,   * Si la date et l’heure d’arrivée et de départ des visiteurs sont consignées et si tous les visiteurs sont encadrés, sauf si leur accès a déjà été autorisé, * Si l’accès leur est accordé uniquement à des fins précises ayant fait l’objet d’une | * 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 RSI, * Vérification du registre des visiteurs, * Vérification des contrôles d’accès physiques aux périmètres sécurisés, |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | autorisation et si les instructions relatives aux exigences de sécurité de la zone et aux  procédures d’urgence associées  leur ont été remises, | * Vérification des emplacements des caméras de surveillances et des alarmes, * Vérification du système de vidéosurveillance, |  |  |
|  |
|  |
|  |
| * S’il est exigé de l’ensemble des salariés, des contractants et des tiers le port d’un moyen   d’identification visible,   * S’il leur est demandé qu’ils informent immédiatement le personnel de sécurité s’ils |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | rencontrent des visiteurs non accompagnés ou quiconque ne portant pas d’identification  visible, |  |  |  |
|  |
| **A.11.1.3** | Sécurisation des bureaux, des salles et des équipements |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| * Si les répertoires et annuaires téléphoniques internes   identifiant l’emplacement des moyens de traitement de  l’information confidentielle ne sont pas accessibles sans autorisation. |
| **A.11.1.4** | Protection contre les menaces extérieures et environnementales |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **37** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.11.1.5** | 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, | * 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. |  |  |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.11.1.6** | Zones de livraison et de chargement |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  |  |  |  |  | |  |
| **A.11.2** | Matériels | Empêcher la perte, l’endommagement, le vol ou la compromission des actifs et l’interruption des activités de l’organisme. | | | | | |
| **A.11.2.1** | Emplacement et protection  des matériels |  |  |  |  |  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **41** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
| **A.11.2.2** | Services généraux |  |  |  |  |  |
| **A.11.2.3** | Sécurité du câblage |  |  |  |  |  |

**42**

Référentiel d’Audit de la Sécurité des Systèmes d’Information

©ANSI 2018

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.11.2.4** | Maintenance des matériels |  |  |  |  |  |
| **43** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  | et leur intégrité. |  | 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. |  |  |
| * Si toutes les exigences de maintenance qu’imposent les polices d’assurance sont respectées, |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.11.2.5** | Sortie des actifs | Les matériels, les informations ou les logiciels des locaux de l’organisme  ne doivent pas sortir sans autorisation préalable. | * Si des règles, concernant la sortie des actifs (autorisations préalables, personnes autorisées, enregistrement de la sortie et de la rentrée, effacement des données inutiles, etc.), sont établies et documentées, * Si les salariés et les tiers, qui ont autorité pour permettre le retrait des actifs du site, sont clairement identifiés, * Si des limites dans le temps sont fixées pour la sortie des actifs et si la date de retour est respectée, * Si, le cas échéant, la sortie des actifs et leur retour dans les   locaux de l’organisme sont enregistrés,   * Si l’identité, la fonction et   l’affiliation de toute personne qui manipule ou utilise les actifs sont documentées et si ces documents accompagnent le retour du matériel, de  l’information ou des logiciels. | * Revue des règles concernant la sortie des actifs, * Revue des registres de sortie des actifs, * Revue d’un échantillon   d’autorisations de sortie des actifs,   * Interview du DAF, et du DSI. |  |  |
| **A.11.2.6** | Sécurité des matériels  et des actifs hors des locaux | Des mesures de sécurité  doivent être appliquées aux matériels utilisés hors | * Si l’utilisation de matériels de traitement et de stockage de   l’information hors des locaux de | * Revue d’un échantillon   d’autorisations de la direction de l’utilisation du matériel hors site, |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  | des locaux de l’organisme en tenant compte des différents risques associés au travail hors site. | l’organisme est autorisée par la direction,   * Si une politique de sécurité relative au travail hors site est élaborée et mise en œuvre, | * Revue du rapport d’analyse des risques issus du travail hors site, * Revue des registres de circulation du matériel hors site entre différentes personne ou tiers, * Interview du DSI. |  |  |
|  |
|  |
| * Si des mesures pour les emplacements de travail hors site, comme le travail à domicile, le télétravail et les sites temporaires, sont déterminées en réalisant une appréciation du risque, * Si, lorsque du matériel circule hors des locaux de l’organisme entre différentes personnes ou entre des tiers, un journal détaillant la chaîne de traçabilité du matériel est tenu à jour, mentionnant au minimum les   noms des personnes |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | responsables du matériel, ainsi que les organismes dont elles  relèvent. |  |  |  |
| **A.11.2.7** | Mise au rebut ou recyclage sécurisé(e) des matériels | 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, | * 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. | . |  |
|  |
| **A.11.2.8** | Matériels utilisateur  laissés sans | Les utilisateurs doivent  s’assurer que les matériels | * Si tous les utilisateurs sont sensibilisés aux exigences et aux | * Revue des programmes de sessions de sensibilisation réalisées et |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  | surveillance | non surveillés sont  dotés d’une protection appropriée. | procédures de sécurité destinées à protéger les matériels laissés sans surveillance, ainsi qu’aux responsabilités qui leur incombent pour assurer la mise  en œuvre de cette protection | bénéficiaires,   * Audit, sur un échantillon de postes de travail, des paramètres de configuration, * Interview du DSI, * Interview d’un échantillon d’utilisateurs. |  |  |
|  |
| **A.11.2.9** | Politique du bureau propre et de l’écran vide | Une politique du bureau propre pour les documents papier et les supports  de stockage amovibles, et une politique de l’écran | * Si une politique du bureau   propre et de l’écran vide, tenant compte de la classification de  l’information, des exigences  légales et contractuelles, des | * Revue de la politique du bureau propre et de l’écran vide, * Interview du DSI et du DAF, * Inspection d’un échantillon de | * Politique du bureau propre et de l’écran vide, * Captures d’écrans, * Rapport d’audit des | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  | vide pour les  moyens de traitement de l’information doivent être adoptées. | risques associés et de la culture de l’organisme, est élaborée et  mise en œuvre, | bureaux occupés par des personnes traitant des dossiers sensibles  (utilisation d’armoires fermant à clés, bureau propres, …),   * Vérification de l’écran vide sur un échantillon de postes de travail de ces personnes, |  |  |
|  |
| * Si l’utilisation non autorisée, des photocopieurs et autres appareils de reproduction (par exemple les scanneurs ou les appareils photo numériques), est interdite, * Si les documents contenant de   l’information sensible ou classée sont retirés immédiatement des  imprimantes, |
|  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  |  |  |  |  | |  |
| **A.12** | **Sécurité liée à l’exploitation** | | | | | | |
| **A.12.1** | Procédures et responsabilités liées à  l’exploitation | Assurer l’exploitation correcte et sécurisée des moyens de traitement de l’information. | | | | | |
| **A.12.1.1** | Procédures  d’exploitation documentées | Les procédures  d’exploitation doivent être documentées et mises à 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.), * Interview du DSI, du RSI 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. |  |  | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
| **A.12.1.2** | Gestion des changements | Les changements apportés à l’organisme, aux processus métier, aux systèmes et moyens de  traitement de l’information ayant une incidence sur la sécurité de l’information doivent être contrôlés. | * S’il existe une procédure de gestion des changements permettant de contrôler les décisions de changements à apporter au système 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, analyse des risques potentiels des changements, planification et affectation des rôles et responsabilités, communication à l'ensemble des personnes concernées, test des changements et mise en   production des changements. | * 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 des changements et mise en production des changements, * Interview du RSI et des administrateurs système, BD et réseau    |  | |  |
| **A.12.1.3** | Dimensionnement | L’utilisation des ressources doit être surveillée et ajustée et des projections sur les dimensionnements futurs doivent être effectuées pour garantir les performances exigées du système. | * Si les indicateurs/critères de performance des serveurs et des équipements réseaux sont définis, * Si les décisions de changement s'appuient sur des analyses de la capacité des nouveaux équipements et systèmes à   assurer la charge requise en fonction des évolutions des | * Revue des indicateurs/critères de performance des serveurs et des équipements réseaux, * Revue de la procédure de gestion des changements, * Interview du RSI et des administrateurs système, BD et réseau. |  |  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | demandes prévisibles, |  |  |  |
|  |
| **A.12.1.4** | Séparation des environnements de développement, de test  et d’exploitation | Les environnements de développement, de test et d’exploitation doivent être séparés pour réduire les  risques d’accès ou de changements non autorisés dans l’environnement en exploitation. |  | * Interview de l’administrateur système et d’un échantillon de développeurs et testeurs, * Vérification sur les serveurs. |  |  |
| **A.12.2** | Protection contre les  logiciels malveillants | S’assurer que l’information et les moyens de traitement de l’information sont protégés contre les logiciels malveillants. | | | | |
| **A.12.2.1** | Mesures contre les logiciels malveillants | Des mesures de détection, de prévention et de récupération conjuguées à une sensibilisation des utilisateurs adaptée, doivent être mises en  œuvre pour se protéger contre les logiciels malveillants. | * Si une politique est définie afin de lutter contre les risques d'attaque par des codes malveillants (virus, chevaux de Troie, spyware, vers, etc.) : interdiction d'utiliser des logiciels non préalablement autorisés, mesures de protection lors de la récupération de fichiers via des réseaux externes, revues de logiciels installés, etc, * Si les actions à mener par le personnel informatique, pour | * Revue de la politique de protection contre les logiciels malveillants, * Revue des abonnements à des centres d’alerte, * Revue des rapports d’audit de la solution antivirale, * Interview d’un échantillon du personnel informatique veillant à la protection contre les logiciels malveillants, * Interview du responsable de la protection antivirale, * Vérification au niveau des interfaces |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | prévenir, détecter et corriger les attaques par des codes malveillants sont définies,   * S’il y a abonnement à un centre d'alerte permettant d'être prévenu et d'anticiper certaines attaques massives pour lesquelles les antivirus ne   sont pas encore à jour, | d’administration des produits antivirus. |  |  |
|  |
| **53** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** | |
|  |  |  |  |  |  |  | |
| **A.12.3** | Sauvegarde | Se protéger de la perte de données. | | | | | |
| **A.12.3.1** | Sauvegarde des informations | Des copies de sauvegarde de l’information, des logiciels et des images systèmes doivent être réalisés et testés 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,   + la définition des rôles et des responsabilités, période/cycle de conservation, etc.,   est élaborée et mise en œuvre,   * 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 | * Revue de la politique de sauvegarde, * Revue des rapports d’audit du processus de sauvegarde, * Interview des responsables métier, * Interview du RSI et des administrateurs système, BD et réseau. |  | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | 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,  -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. |  |  |  |
|  |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.12.4** | Journalisation et  surveillance | Enregistrer les événements et générer des preuves. | | | |  |
| **A.12.4.1** | Journalisation des événements | Des journaux  d’événements enregistrant les activités de l’utilisateur, les exceptions, les défaillances et les événements liés à la  sécurité de l’information doivent être créés, tenus à | * Si une analyse spécifique des besoins en termes de journalisation est réalisée: les types de journaux à activer, paramètres/éléments fondamentaux concernant chaque type de journaux à conserver (par exemple pour   l’accès à une ressource | * Revue du rapport d’analyse des besoins en termes de journalisation, * Revue de la politique de journalisation, * Interview des responsables métier, * Interview du RSI et des administrateurs système, BD et réseau. |  |  |
| **56** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  | jour et vérifiés régulièrement. | sensible: l’identifiant, le service ou l'application demandée, la date et l'heure, ...), localisation des fichiers journaux, durée de rétention des fichiers journaux, mécanismes de protection, mécanisme d'analyse et de corrélation, …,   * Si les règles résultantes de cette analyse fait l'objet d'une politique formalisée, * Si cette politique couvre les applications, les bases de données, les systèmes et les   équipements, |  |  |  |
|  |
| **57** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.12.4.2** | Protection de l’information journalisée |  |  | . | . |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
| **A.12.4.3** | Journaux administrateur et opérateur | Les activités de  l’administrateur système et de l’opérateur système doivent être journalisées, protégées et vérifiées régulièrement. |  | * 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, * Interview de l’administrateur système, |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  |  |  |  |  | |  |
| **A.12.4.4** | Synchronisation des horloges | Les horloges de l’ensemble des systèmes de traitement de l’information concernés d’un organisation ou d’un domaine de sécurité doivent être  synchronisées sur une source de référence  temporelle unique. |  | * Interview des administrateurs système et réseau, * Vérification de la synchronisation des horloges des serveurs et des équipements réseau et sécurité avec un serveur NTP unique. |  | |  |
| **A.12.5** | Maîtrise des logiciels  en exploitation | Garantir l’intégrité des systèmes en exploitation. | | | | | |
| **A.12.5.1** | Installation de logiciels sur des systèmes en exploitation | Des procédures doivent  être mises en œuvre pour contrôler l’installation de  logiciel sur des systèmes en exploitation. | * Si une procédure d'installation sur l'environnement de production 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 | * Revue de la procédure du contrôle de l’installation de logiciels sur l'environnement de production, * Interview de l’administrateur système, * Vérification sur un échantillon   d’installations sur l'environnement de production, des documents résultants,   * Interview de l’administrateur système, |  |  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | 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 telle analyse de risques, * Si la mise en production de nouvelles versions de systèmes/logiciels/ applications n'est possible que par le personnel d'exploitation, | * Vérification sur un échantillon des postes utilisateurs. |  |  |
|  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
| **A.12.6** | Gestion des vulnérabilités  techniques | Empêcher toute exploitation des vulnérabilités techniques. | | | | | |
| **A.12.6.1** | Gestion des vulnérabilités techniques | Des informations sur les vulnérabilités techniques des systèmes d’information en exploitation doivent être obtenues en temps opportun, l’exposition  de l’organisme à ces vulnérabilités doit être évaluée et les mesures appropriées doivent être prises pour traiter le risque associé. | * S’il existe une procédure de gestion de vulnérabilités techniques permettant   d’identifier, d’évaluer et de répondre aux vulnérabilités des systèmes, réseaux, base de données et applications,   * 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 un abonnement au CERT national est souscrit pour s'informer aux vulnérabilités liées aux produits et systèmes   utilisés | * Revue de la procédure de gestion de vulnérabilités techniques, * Revue des rapports des audits techniques, * Revue des documents résultants de l’installation des correctifs, * Interview du RSI et des administrateurs système et réseau,     Revue de l’historique des installations des nouvelles versions et des correctifs,   * Interview des administrateurs système et réseau, |  |  | |
|  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** | |
| **A.12.6.2** | Restrictions liées à l’installation de logiciels | Des règles régissant  l’installation de logiciels par les utilisateurs doivent être établies et mises en œuvre. | * 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. | * Voir les vérifications de A.9.2.2, * Revue de la liste des types de logiciels dont l’installation est   autorisée et des types d’installation qui sont interdits. |  |  | |
| **A.12.7** | Considérations sur  l’audit des systèmes d’information | Réduire au minimum l’impact des activités d’audit sur les systèmes en exploitation. | | | | | |
| **A.12.7.1** | Mesures relatives à l’audit des systèmes d’information | Les exigences et activités d’audit impliquant des vérifications sur des systèmes en exploitation doivent être prévues avec soin et validées afin de réduire au minimum les perturbations subies par  les processus métier. | * 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 | * Revue de la procédure d’audit des systèmes d’information, * Interview du RSI. |  | |  |
| **A.13** | **Sécurité des communications** | | | | | | |
| **A.13.1** | Gestion de la sécurité  des réseaux | Objectif: Garantir la protection de l’information sur les réseaux et des moyens de traitement de l’information sur lesquels elle s’appuie. | | | | | |
| **A.13.1.1** | Contrôle des réseaux | Les réseaux doivent être  gérés et contrôlés pour | * Si les responsabilités et les procédures de gestion des | * Revue de la procédure de gestion des équipements réseau, |  |  | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  | protéger l’information contenue dans les systèmes et les applications. | équipements réseau sont définies,   * Si la responsabilité d’exploitation des réseaux est séparée de celle de l’exploitation des ordinateurs, |  |  | |  |
|  |
| **A.13.1.2** | Sécurité des services de réseau | Pour tous les services de réseau, les mécanismes de sécurité, les niveaux de service et les exigences de gestion, doivent être identifiés et intégrés dans | * 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 | * 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, |  |  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  | les accords de services de réseau, que ces services soient fournis en interne ou externalisés. | 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 rapports de surveillance de la capacité des connexions et des équipements (bande passante contracté vs bande passante   réelle,…),   * 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 métier. |  |  |
| **A.13.1.3** | Cloisonnement des réseaux |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  |  |  |  |  | |  |
| **A.13.2** | Transfert de  l’information | Maintenir la sécurité de l’information transférée au sein de l’organisme et vers une entité extérieure. | | | | | |
| **A.13.2.1** | Politiques et procédures  de transfert de l’information | Des politiques, des procédures et des mesures de transfert formelles doivent être mises en place pour protéger les transferts d’information transitant par tous types  d’équipements de communication. | * Si une politique décrivant succinctement l’utilisation acceptable des équipements de communication est élaborée et mise en œuvre, * Si une procédure de protection de l’information transférée   contre l’interception, la reproduction, la modification, les erreurs d’acheminement et la destruction est élaborée et mise en œuvre,   * Si une procédure de détection et de protection contre les logiciels malveillants qui peuvent être   transmis via l’utilisation des communications électroniques  est élaborée et mise en œuvre, | * Revue de la politique de l’utilisation acceptable des équipements de communication, * Revue de la procédure de protection de l’information transférée, * Revue de la procédure de détection et de protection contre les logiciels malveillants, * Revue des programmes de sessions de sensibilisation réalisées et bénéficiaires, * Interview du DSI et des responsables métier, * Interview d’un échantillon d’utilisateurs, * Vérification sur les serveurs et sur un échantillon de poste de travail de l’existence d’outils de détection et de protection contre les logiciels |  |  | |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  | malveillants. |  |  |
| * Si le personnel est sensibilisé de ne pas tenir de conversation confidentielle dans des lieux publics, sur des réseaux de communication non sécurisés, dans des bureaux ouverts ou des   lieux de réunion. |
| **A.13.2.2** | Accords en matière de transfert d’information | Des accords doivent traiter du transfert sécurisé de  l’information liée à  l’activité entre l’organisme et les tiers. | * Si des accords traitant du transfert sécurisé de   l’information liée à l’activité sont signé entre l’audité et les tiers,   * Si les responsabilités de gestion, pour contrôler et informer de la transmission, de la répartition et de la réception de l’information, sont identifiées et documentées, * Si une procédure de gestion la traçabilité et la non-répudiation   est élaborée et mise en œuvre, | * Revue des accords traitant du   transfert sécurisé de l’information liée à l’activité,   * Revue du document d’identification des responsabilités de gestion, de la répartition et de la réception de   l’information,   * Revue de la procédure de gestion de la traçabilité et la non-répudiation, * Revue du document d’identification des obligations et des |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | * Si les obligations et les   responsabilités, en cas d’incident lié à la sécurité de l’information,  comme la perte de données, sont identifiées et documentées, | responsabilités des uns et des autres en cas d’incident lié à la sécurité de  l’information,   * Revue des rapports de traitement des incidents liés à la sécurité de l’information, * Interview du DSI et des responsables métier, |  |  |
|  |
| **A.13.2.3** | Messagerie électronique | L’information transitant par la messagerie électronique doit être protégée de manière appropriée. | * Si une politique de sécurité 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, | * Revue de la politique de sécurité propre à la messagerie électronique définissant les précautions d'emploi et les mesures de sécurité à mettre en œuvre, * Interview du DSI et des administrateurs réseau, |  |  |
|  |
| * Si la disponibilité et la fiabilité du service sont prises en compte, * Si les questions juridiques, |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | comme les exigences en matière de signatures numériques sont prises en compte,   * S’il est exigé d’obtenir une   autorisation avant d’utiliser des services externes publics comme une messagerie instantanée, un réseau social ou le partage de  fichiers, | travail (connexion à la messagerie par mot de passe non enregistré, …). |  |  |
|  |
| **A.13.2.4** | Engagements de confidentialité ou de non-divulgation | Les exigences en matière d’engagements de confidentialité ou de non- divulgation, doivent être identifiées, vérifiées régulièrement et documentées conformément aux besoins de l’organisme. | * Si les salariés et les sous-traitants signent des engagements de confidentialité ou de non- divulgation, * Si les modalités de ces engagements 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 | * Revue d’un échantillon   d’engagements de confidentialité ou de non-divulgation,   * Interview du DAF, du DRH et du responsable juridique, |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | à protéger (par exemple information confidentielle),   * la durée prévue de   l’engagement, y compris les cas où il peut s’avérer nécessaire de poursuivre cette durée indéfiniment,   * les actions à entreprendre   lorsqu’un engagement arrive à expiration,   * les responsabilités et les tâches des signataires visant à éviter une divulgation non autorisée de l’information, * la propriété de l’information, des secrets de fabrication et la propriété intellectuelle, ainsi que leurs liens avec la   protection de l’information confidentielle,   * l’utilisation autorisée de   l’information confidentielle et les droits du signataire relatifs à l’utilisation de cette information,   * 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 |  | ` |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** | |
|  |  |  | divulgation non autorisée ou d’une fuite de l’information confidentielle,   * les modalités de retour ou de destruction de l’information à l’expiration de l’engagement, * les actions à entreprendre en cas de violation de   l’engagement.   * Si les engagements de confidentialité et de non- divulgation sont revus à intervalles réguliers et en cas de changements ayant une   incidence sur ces exigences. |  |  |  | |
| **A.14** | **Acquisition, développement et maintenance des systèmes d’information** | | | | | | |
| **A.14.1** | Exigences de sécurité  applicables aux systèmes d’information | Veiller à ce que la sécurité de l’information fasse partie intégrante des systèmes d’information tout au long de leur cycle de vie. Cela inclut également des exigences pour les systèmes d’information fournissant des services sur les réseaux publics. | | | | | |
| **A.14.1.1** | Analyse et spécification des exigences de sécurité de  l’information | Les exigences liées à la sécurité de l’information doivent être intégrées aux exigences des nouveaux systèmes d’information ou des améliorations de systèmes d’information existants. | * Si une analyse des risques de sécurité de l’information est réalisée dès la phase de conception des nouveaux systèmes d’information ou leur amélioration, * Si le niveau de confiance requis en ce qui concerne l’identité déclarée des utilisateurs est pris en compte afin d’en déduire les exigences d’authentification   utilisateur, | * Revu du document d’analyse des risques, * Revue des documents de projets de développement de nouveaux systèmes, * Revue des cahiers des charges pour l’acquisition de nouveaux systèmes, * Revue des contrats avec les fournisseurs, * Revue des critères d’acceptation des produits, |  | |  |
| **71** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | * Si la gestion des accès et des processus d’autorisation, pour les utilisateurs de l’organisme ainsi que pour les utilisateurs techniques ou dotés de privilèges, est maîtrisée, * Si les utilisateurs et les opérateurs sont informés sur les devoirs et les responsabilités qui leur incombent, * Si les exigences de protection que requièrent les actifs impliqués, notamment en ce qui concerne la disponibilité, la   confidentialité, l’intégrité sont identifiées et documentées,   * Si les exigences découlant des processus de l’organisme, tels que la journalisation et la   surveillance des transactions, les exigences de non-répudiation sont identifiées et documentées,   * Si les exigences spécifiées par les autres mesures de sécurité, telles que les interfaces pour la journalisation et la surveillance ou les systèmes de détection de fuite de données sont identifiées et documentées, * Si les exigences de sécurité | * Revue des rapports d’évaluation des produits avant l’achat, * Interview du DSI, RSI éventuellement |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | identifiées sont traitées dans les contrats conclus avec le fournisseur,   * Si les critères d’acceptation des produits (par exemple en termes de fonctionnalité, qui garantissent que les exigences de sécurité identifiées sont respectées) sont définis, * Si les produits sont évalués au regard de ces critères avant de procéder à l’achat, * Si toute nouvelle fonctionnalité est revue pour s’assurer qu’elle n’entraîne pas de risques supplémentaires inacceptables. |  |  |  |
| **A.14.1.2** | Sécurisation des services  d’application sur les réseaux publics | Les informations liées aux services d’application transmises sur les réseaux publics doivent être protégées contre les activités frauduleuses, les différents  contractuels, ainsi que la divulgation et la modification non autorisées. | * Si l’identité déclarée des parties qui échangent l’information sur les réseaux publics est vérifiée (en utilisant l’authentification par exemple), * Si les processus d’autorisation liés aux personnes qui peuvent approuver le contenu, émettre ou signer des documents transactionnels clés sont définis   et documentés, | * Revue du processus d’autorisation des personnes pouvant traiter des documents transactionnels, * Interview des responsables métier et du RSI, * Audit des mécanismes   d’authentification lors de  l’utilisation des applications sur les réseaux publics, |  |  |
|  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  | |
| **A.14.1.3** | Protection des transactions liées aux services d’application |  |  |  |  |  | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** | |
|  |  |  |  |  |  |  | |
| **A.14.2** | Sécurité des processus  de développement et d’assistance technique | S’assurer que les questions de sécurité de l’information sont étudiées et mises en œuvre dans le cadre du cycle de développement des systèmes d’information. | | | | | |
| **A.14.2.1** | Politique de développement sécurisé | Des règles de développement des logiciels et des systèmes doivent être  établies et appliquées aux développements de l’organisme. | * 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 | * 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,   * Interview du DSI, du RSSI, des |  | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | 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 les fonctions sensibles,   + une vérification du code 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 | développeurs et d’un échantillon d’utilisateurs. |  |  |
| **76** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | l'éditeur, au partenaire ou au  sous-traitant. |  |  |  |
| **A.14.2.2** | Procédures de contrôle des changements de système | Les changements des systèmes dans le cadre du cycle de développement doivent être contrôlés par le biais de procédures formelles. | * Si une procédure formelle de contrôle des changements est élaborée et mise en œuvre, * Si un enregistrement des niveaux d’autorisation accordés est tenu à jour, * Si les propositions de changements émanent d’utilisateurs autorisés, * Si les commandes et les   procédures d’intégrité sont  revues afin de s’assurer qu’elles ne seront pas compromises par les changements,   * 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 | * Revue de la procédure de contrôle des changements, * 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 les propositions détaillées, * Revue des demandes de changements, * Revue des rapports des changements effectués, * Revue de la documentation systèmes, * Interview des responsables métiers et d’un échantillon d’utilisateurs, * Vérification du système de contrôle des versions des logiciels, * Vérification des mises à jour des systèmes critiques. |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | documentation est archivée ou mise au rebut,   * Si un contrôle de version est tenu à jour pour toutes les mises à jour logicielles, * Si un système de traçabilité de toutes les demandes de changement est tenu à jour, * Si la documentation du système d’exploitation et les procédures utilisateurs sont adaptées en fonction des changements, * Si la mise en œuvre des changements est programmée en temps voulu, de manière à ne pas perturber les activités de l’organisme, * Si les mises à jour automatiques des systèmes critiques sont rendues impossibles. |  |  |  |
| **A.14.2.3** | Revue technique des applications après changement apporté à la plateforme  d’exploitation |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.14.2.4** | Restrictions relatives aux changements apportés aux progiciels | Les modifications des progiciels ne doivent pas être encouragées, être limitées aux changements nécessaires et tout changement doit être strictement contrôlé. | * Lorsqu’une modification du progiciel est nécessaire (dans la mesure du possible, il est recommandé de ne pas apporter de changements aux progiciels fournis par l’éditeur) :   + S’il n y a pas de risque de compromettre les commandes intégrées et le processus de   vérification de l’intégrité,   * + S’il est nécessaire ou non   d’obtenir le consentement de l’éditeur,   * + S’il est possible d’obtenir les changements souhaités auprès de l’éditeur, sous la forme de mises à jour de programme classiques,   + Si l’organisme est tenue responsable de la maintenance du logiciel suite à des changements,   + Si la compatibilité avec les autres logiciels en service est   prise en compte. | * Revue du rapport d’analyse des risques des changements apportés aux progiciels, * Revue des licences des progiciels. * Interview du DSI. |  |  |
| **A.14.2.5** | Principes d’ingénierie | Des principes d’ingénierie | * Si des procédures d’ingénierie de | * Revue des procédures d’ingénierie |  | |
| **79** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  | de la sécurité des systèmes | de la sécurité des systèmes doivent être établis, documentés, tenus à jour et appliqués à tous les travaux de mise en œuvre des systèmes  d’information. | 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 à   tous les niveaux de l’architecture (activité, données, applications et technologie),   * 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’audité et le prestataire auprès duquel   ces systèmes sont externalisés. | de la sécurité des systèmes,   * Revue du rapport de conception de la sécurité, * Revue du rapport d’analyse des nouvelles technologies au regard des risques de sécurité, * Revue des contrats et accords   exécutoires passés entre l’audité et le prestataire,   * Interview du DSI et du RSI. |  |  |
| **A.14.2.6** | Environnement de développement sécurisé | Les organismes doivent établir des environnements de développement sécurisés pour les tâches de développement et  d’intégration du système, | * Si des procédures de développement sont élaborées et mises en œuvre, * Si une séparation stricte des tâches entre spécification détaillée, conception, test | * Revue des procédures de développement, * Revue des fiches de postes, * Revue du schéma de l’architecture réseau, |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  | qui englobe l’intégralité du cycle de vie du développement du système, et en assurer la protection de manière appropriée. | unitaire et intégration, est  réalisée, | * Interview du DSI, * Audit des comptes d’accès aux environnements de développement.    |  |  |
|  |
| **A.14.2.7** | Développement externalisé | L’organisme doit superviser et contrôler l’activité de développement du système externalisée. | * Si les questions d'accord de licence et de propriété intellectuelle du code développé sont réglées, * Si les exigences contractuelles relatives à la sécurité du code sont formalisées, * Si un droit d'accès permettant de vérifier la qualité des travaux réalisés en sous-traitance est prévu, * 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 | * 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. |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | développement. |  |  |  |
| **A.14.2.8** | Test de la sécurité du système |  |  |  |  |  |
| **A.14.2.9** | Test de conformité du système |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  |  |  |  |  | |  |
| **A.14.3** | Données de test | Garantir la protection des données utilisées pour les tests. | | | | | |
| **A.14.3.1** | Protection des données de test | Les données de test doivent être sélectionnées avec soin, protégées et Contrôlées. | * Si, dans le cadre d'essais,   l’utilisation des bases de données de production contenant des informations personnelles ou toute autre information sensible est évitée,   * 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 la procédure de contrôle d’accès, qui s’applique aux systèmes d’applications en exploitation, s’applique également aux systèmes d’applications de test, * Si une nouvelle autorisation est obtenue chaque fois qu’une   information d’exploitation est copiée dans un environnement  de test, | * Revue de la procédure de contrôle d’accès, * Revue des autorisations de copie des informations d’exploitation sur un environnement de test, * Interview du DSI, des responsables de développement et de test, * Revue des données de test pour l’identification des informations d’exploitation. |  |  | |
|  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** | |
|  |  |  |  |  |  |  | |
| **A.15** | **Relations avec les fournisseurs** | | | | | | |
| **A.15.1** | Sécurité dans les relations avec les  fournisseurs | Garantir la protection des actifs de l’organisme accessible aux fournisseurs. | | | | | |
| **A.15.1.1** | Politique de sécurité de l’information dans les relations avec les fournisseurs | Des exigences de sécurité de l’information pour limiter les risques résultant de l’accès des fournisseurs aux actifs de l’organisme doivent être acceptées par le fournisseur et documentées. | * Si une politique identifiant et imposant des mesures de sécurité spécifiques aux accès des fournisseurs aux actifs de   l’audité est élaborée et mise en œuvre,   * Si les types de fournisseurs, (par exemple services informatiques, services logistiques, services financiers, composants de   l’infrastructure informatique), auxquels l’organisme accordera un accès à son information sont identifiés et documentés,   * Si on impose contractuellement à tout fournisseur pouvant avoir accès ou favoriser l'accès à des informations ou à des ressources | * Revue de la politique identifiant et imposant des mesures de sécurité spécifiques aux accès des fournisseurs aux actifs de l’audité, * Revue de la liste des types de fournisseurs,(par exemple services informatiques, services logistiques, services 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 |  | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | 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’organisme et  celles des fournisseurs sont identifiés et traités. | différents types de fournisseurs,   * Revue du rapport de traitement des incidents et des impondérables associés aux accès fournisseurs |  |  |
| **A.15.1.2** | La sécurité dans les accords conclus avec les fournisseurs | Les exigences applicables liées à la sécurité de  l’information doivent être établies et convenues avec chaque fournisseur pouvant accéder, traiter, stocker, communiquer ou  fournir des composants de | * 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, | * 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, |  |  |
| **85** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** | |
|  |  | l’infrastructure informatique destinés à l’information de l’organisme. | * 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. | * Interview du DAF, du responsable juridique et du RSI. |  |  | |
| **A.15.1.3** | Chaîne  d’approvisionnement des produits et  des services informatiques | Les accords conclus avec les fournisseurs doivent inclure des exigences sur le traitement des risques liés à la sécurité de  l’information associé à la chaîne  d’approvisionnement des produits et des services informatiques. | * Si une analyse des risques de la sécurité de l’information associés à la chaine 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 l’audité s'assure que les fournisseurs signalent et documentent tout incident de   sécurité touchant ces actifs. | * Revue du rapport d’analyse des risques de la sécurité de   l’information associés à la chaine d’approvisionnement,   * Revue d’un échantillon d’accords ou de contrats avec les fournisseurs, * Revue d’un échantillon de rapports d’incidents signalés par le fournisseur, * Interview du DAF et du RSI. |  |  | |
| **A.15.2** | Gestion de la  prestation du service | Maintenir le niveau convenu de sécurité de l’information et de service conforme aux accords conclus  avec les fournisseurs. | | | | | |
| **A.15.2.1** | Surveillance et revue des services des fournisseurs | Les organismes doivent surveiller, vérifier et auditer à intervalles réguliers la prestation des services assurés par les 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, | * 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, * Interview du DSI et du RSI, |  | |  |

**86**

Référentiel d’Audit de la Sécurité des Systèmes d’Information

©ANSI 2018

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | * Si les aspects liés à la sécurité de l’information dans les relations du fournisseur avec ses propres   fournisseurs sont revus. | * Interview d’un échantillon de fournisseurs. |  |  |
| **A.15.2.2** | Gestion des changements apportés dans les services des fournisseurs | Les changements effectués dans les prestations de service des fournisseurs, comprenant le maintien et l’amélioration des politiques, procédures et mesures existant en matière de sécurité de  l’information, doivent être gérés en tenant compte du caractère critique de  l’information, des systèmes et des processus concernés et de la réappréciation des risques. | * Si les changements apportés aux accords passés avec les fournisseurs sont gérés, * Si les changements effectués par l’audité 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’organisme sont gérés,   * Si 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 | * Revue du rapport des changements apportés aux accords passés avec les fournisseurs, * Revue des rapports des changements effectués par l’audité, * Revue des rapports des changements dans les services assurés par les fournisseurs, * Interview du DSI et du RSI. |  |  |
| **87** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** | |
|  |  |  | 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   sont gérés. |  |  |  | |
| **A.16** | **Gestion des incidents liés à la sécurité de l’information** | | | | | | |
| **A.16.1** | Gestion des incidents liés à la sécurité de  l’information et  améliorations | Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l’information, incluant la communication des événements et des failles liés à la sécurité. | | | | | |
| **A.16.1.1** | Responsabilités et procédures | Des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente doivent être  établies en cas d’incident lié à la  sécurité de l’information. | * 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 des incidents,   + procédure de traitement des incidents, | * 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, * Revue des différentes procédures de gestion des incidents, * Revue d’un échantillon de fiches d’incidents, * Interview du DSI et du RSI. |  | |  |
| **88** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | - procédure de réponse, incluant les procédures de remontée  d’information, de récupération contrôlée de l’incident et de communication aux organismes ou aux personnes internes ou  extérieures à l’audité. |  |  |  |
| **A.16.1.2** | Signalement des événements  liés à la sécurité de l’information | Les événements liés à la sécurité de l’information doivent être signalés dans les meilleurs délais par les voies hiérarchiques appropriées. | * Si tous les salariés et contractants sont informés de leur obligation de signaler les événements liés à la sécurité de l’information dans les meilleurs délais, * S’ils sont informés de l’existence d’une procédure de signalement des événements liés à la sécurité de l’information et d’un responsable servant de point de contact auprès duquel effectuer le signalement, * Si le système de déclaration et de gestion des incidents inclut-il tous les incidents (exploitation, développement, maintenance, utilisation du SI) physiques, logiques ou organisationnels et les tentatives d'actions malveillantes ou non autorisées n'ayant pas abouti, * Si le système de déclaration et de gestion des incidents s'applique à | * Revue de la procédure signalement des incidents, * Revue d’un échantillon de fiches de signalement des incidents, * Interview du DSI, du RSI et d’un échantillon d’utilisateurs. |  |  |
| **89** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | l'ensemble des structures et des personnels de l'organisme (y  compris les filiales). |  |  |  |
| **A.16.1.3** | Signalement des failles liées à la sécurité de  l’information | Les salariés et les sous- traitants utilisant les systèmes et services  d’information de l’organisme doivent noter et signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services. | * Si les salariés et les contractants utilisant les systèmes et services d’information de l’audité notent et signalent toute faille de sécurité observée ou soupçonnée dans les systèmes ou services, * S’il est recommandé aux salariés et contractants de ne pas tenter de démontrer l’existence des   failles de sécurité soupçonnées. | * Revue d’un échantillon de signalement des failles de sécurité, * Revue du programme de sensibilisation réalisé et liste des bénéficiaires, * Interview du RSI et d’un échantillon d’utilisateurs. |  |  |
| **A.16.1.4** |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  | réseau et de sécurité,   * Revue des registres des résultats de traitement des événements liés à la sécurité. |  |  |
| **A.16.1.5** | Réponse aux incidents liés à la 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, | * 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, * Interview des membres de l’équipe de réponse aux incidents et du RSI. |  |  |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.16.1.6** | Tirer des enseignements des incidents  liés à la sécurité de l’information |  |  |  |  |  |
| **A.16.1.7** | Collecte de preuves | L’organisme doit définir et | * Si une procédure d’identification, | * Revue de la procédure |  | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  | appliquer des procédures d’identification, de  collecte, d’acquisition et de protection de l’information pouvant servir de preuve. | 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, * 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’organisme. | d’identification, de collecte et de  protection de l’information pouvant servir de preuve,   * Revue d’un échantillon de preuves, * Interview du DSI, du RSI et du DRH. |  | |  |
| **A.17** | **Aspects de la sécurité de l’information dans la gestion de la continuité de l’activité** | | | | | | |
| **A.17.1** | Continuité de la sécurité de  l’information | La continuité de la sécurité de l’information doit faire partie intégrante de la gestion de la continuité de l’activité. | | | | | |
| **A.17.1.1** | Organisation de la continuité de la sécurité de  l’information | L’organisme doit déterminer ses exigences en matière de sécurité de l’information et de  continuité de management | * Si une analyse de l’impact sur l’activité des aspects liés à la sécurité de l’information est réalisée, | * Revue du rapport d’analyse de   l’impact sur l’activité des aspects liés à la sécurité de l’information,   * Revue du document des exigences |  |  | |
| **93** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  | de la sécurité de  l’information dans des situations défavorables,  comme lors d’une crise ou d’un sinistre | * Si les exigences de sécurité de l’information applicables aux situations défavorables sont déterminées, à la lumière des   résultats de l’analyse de l’impact, et documentées,   * Si les objectifs de continuité de la sécurité de l’information sont approuvés par la 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. | de sécurité de l’information applicables aux situations défavorables,   * Revue du processus de gestion de la continuité de l’activité et de gestion de la récupération après sinistre, * Interview du DSI et du RSI. |  |  |
| **A.17.1.2** | Mise en œuvre de la continuité de la sécurité  de l’information | L’organisme doit établir, documenter, mettre en œuvre et tenir à jour des  processus, des procédures et des mesures permettant de fournir le niveau requis de continuité de sécurité de l’information au cours  d’une situation | * 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 | * Revue de la note de désignation de la structure de gestion et nomination de ces 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 |  |  |
| **94** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  | défavorable. | 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 direction et les   parties prenantes concernées. | crise,   * Revue des PCA, * Revue des rapports de test des PCA, * Revue du rapport d’analyse des résultats des tests des PCS, * Interview du DSI et des membres de la structure de gestion, * Interview d’un échantillon du personnel. |  |  |
| **A.17.1.3** | Vérifier, revoir et évaluer la continuité de la sécurité de  l’information | L’organisme doit vérifier les mesures de continuité de la sécurité de  l’information mises en œuvre à intervalles | * Si les fonctionnalités des processus, des procédures et des mesures de continuité de la   sécurité de l’information sont testés à intervalles réguliers pour | * Revue du rapport de test fonctionnalités des processus, des procédures et des mesures de continuité de la sécurité de   l’information, |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  | réguliers afin de s’assurer qu’elles sont valables et efficaces dans des situations défavorables. | 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. | * Revue du rapport d’audit de la validité et l’efficacité des mesures de continuité de la sécurité de   l’information après changement dans systèmes d’information, les processus, les procédures et les mesures de sécurité de  l’information,   * Interview du RSI. |  | |  |
| **A.17.2** | Redondances | Garantir la disponibilité des moyens de traitement de l’information | | | | | |
| **A.17.2.1** |  |  |  |  |  |  | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** | |
|  |  |  |  |  |  |  | |
| **A.18** | **Conformité** | | | | | | |
| **A.18.1** | Conformité aux  obligations légales et réglementaires | Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l’information, éviter toute violation des exigences de sécurité. | | | | | |
| **A.18.1.1** | Identification de la législation et des exigences contractuelles applicables | Toutes les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l’approche adoptée par l’organisme pour satisfaire à ces exigences, doivent être explicitement définies, documentées et mises à jour pour chaque système  d’information et pour l’organisme elle-même. | * Si l'ensemble des exigences réglementaires, contractuelles, et légales applicable à l’audité sont explicitement identifiées, documentées et tenues à jour, * Si les mesures spécifiques et les responsabilités individuelles mises en place sont définies et documentées pour répondre à 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, * Interview du DSI, du RSI, du responsable juridique et du DRH. |  | |  |
| **A.18.1.2** | 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 | * 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, | * 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, |  | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  | 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, | * 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 liste de bénéficiaires, * Interview du DSI et du RSI et d’un échantillon d’utilisateurs, |  |  |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **Moyen de vérification (sans s’y limiter)** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  |  |  |  |  |
| **A.18.1.3** | 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, | * Revue de la procédure de stockage et de manipulation des enregistrements, * Interview du DAF, DRH DSI et RSI, |  |  |
|  |
| **A.18.1.4** | Protection de la vie privée et protection des données à caractère personnel | La protection de la vie privée et la protection des données à caractère personnel doivent être garanties telles que  l’exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant. | * Si l'audité a procédé à octroyer les déclarations/autorisations nécessaires auprès de l'INPDP, * Si une politique de protection de la vie privée et des données à caractère personnel est élaborée et mise en œuvre, * Si cette politique est approuvée par la direction et communiquée   à toutes les personnes | * Revue de la politique de protection de la vie privée et des données à caractère personnel, * Revue du recueil regroupant l'ensemble des dispositions légales ou réglementaires, * Revue du programme de sensibilisation et de formation en matière de protection des données   à caractère personnel et liste des |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **MOYEN DE VERIFICATION** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | impliquées dans le traitement des données à caractère personnel,   * Si un recueil regroupant l'ensemble des dispositions légales ou réglementaires relatives à la protection des données à caractère personnel est élaboré, * Si un programme de sensibilisation et de formation, en matière de protection des données à caractère personnel, est élaboré et mis en œuvre. | bénéficiaires,   * Interview du DSI, du RSI et d’un échantillon des personnes impliquées dans le traitement des données à caractère personnel. |  |  |
| **A.18.1.5** | Réglementation relative aux mesures cryptographiques | Des mesures cryptographiques doivent être prises conformément aux accords, législation et réglementations applicables. | * Si une politique d'utilisation de moyens cryptographiques est élaborée et mise en œuvre, * Si cette politique est approuvée par la direction, * Si un recueil regroupant l'ensemble des dispositions légales ou réglementaires relatives à l'utilisation de moyens   cryptologiques est élaboré, | * Revue de la politique d'utilisation de moyens cryptographiques, * Revue du recueil regroupant l'ensemble des dispositions légales ou réglementaires relatives à l'utilisation de moyens cryptologiques, * Revue du programme de sensibilisation et de formation en matière d'utilisation de moyens |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **MOYEN DE VERIFICATION** | **CONTROLE APPLICABLE?** | | **IN COMPLIANCE?** |
|  |  |  | * Si un programme de sensibilisation et de formation en matière d'utilisation de moyens cryptographiques est élaboré et mis en œuvre, * Si des sanctions en cas de non application de la politique sont prévues et communiqué au personnel. | cryptographiques et liste des bénéficiaires,   * Revue de la liste des sanctions en cas de non application de la politique. |  | |  |
| **A.18.2** | Revue de la sécurité de  l’information | Garantir que la sécurité de l’information est mise en œuvre et appliquée conformément aux politiques et procédures organisationnelles. | | | | | |
| **A.18.2.1** | Revue indépendante de la sécurité de  l’information | Des revues régulières et indépendantes de  l’approche retenue par  l’organisme 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 | * 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’organisme en matière de management de la | * Revue de la procédure de mise à jour des notes d'organisation relatives à la sécurité de l'information, * Revue des rapports d’audit. |  |  | |
| **101** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **MOYEN DE VERIFICATION** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  | lorsque des changements importants sont  intervenus. | sécurité de l’information. |  |  |  |
| **A.18.2.2** | Conformité avec les politiques et les normes de sécurité | Les responsables doivent régulièrement vérifier la conformité du traitement de l’information et des procédures dont ils sont chargés au regard des politiques, des normes de sécurité applicables et autres exigences de sécurité. | * Si les responsables déterminent la manière de vérifier que les exigences de sécurité de   l’information définies dans les politiques, les normes et autres règlementations applicables, sont respectées,   * Si, lorsque la revue détecte une non-conformité, les responsables:   + déterminent les causes de la non-conformité   + évaluent la nécessité d’engager des actions pour établir la conformité   + mettent en œuvre l’action corrective appropriée,   + revoient l’action corrective entreprise pour vérifier son efficacité et identifier toute insuffisance ou faille. | * Revue des rapports d’audit de conformité, * Interview du DSI et du RSI. |  |  |
| **A.18.2.3** | Vérification de la conformité technique | Les systèmes d’information doivent être examinés régulièrement quant à  leur conformité avec les politiques et les normes de sécurité de l’information de l’organisme. | * Si une procédure de vérification du respect des politiques et des normes de sécurité de l'information est mise en place, * Si des tests périodiques de pénétration du réseau et des | * Revue des rapports d'audits techniques spécialisés, * Revue des rapports de test des configurations, * Revue des rapports d’audit des paramètres de sécurité, |  |  |
| **102** | Référentiel d’Audit de la Sécurité des Systèmes d’Information ©ANSI 2018 | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Réf Annexe A (ISO**  **27001)** | **Titre Domaine/Objectif/Con trôle** | **Description** | **Vérifications à effectuer** | **MOYEN DE VERIFICATION** | **CONTROLE APPLICABLE?** | **IN COMPLIANCE?** |
|  |  |  | audits techniques spécialisés approfondis sont réalisés,   * Si l'intégrité des configurations par rapport aux configurations théoriquement attendues est testée régulièrement, * Si des audits réguliers des paramètres de sécurité spécifiés sont réalisés, * Si la conformité des configurations logicielles des postes de travail des utilisateurs est contrôlée régulièrement par rapport à la liste des options autorisées. | * Revue des rapports d’audit de conformité des configurations logicielles des postes de travail des utilisateurs, * Interview du DSI, des administrateurs systèmes et réseaux et du RSI. |  |  |

**103**

Référentiel d’Audit de la Sécurité des Systèmes d’Information

©ANSI 2018