

**Certification MSECB – ISO/IEC 27001:2013**

*Rapport d’audit du système de management*

*de* ***la Société ABC***





**DISTRIBUTION**

Le contenu du présent rapport ne doit pas être divulgué à un tiers sans l'accord du client de MSECB MS.

**CLAUSE DE NON-RESPONSABILITÉ**

Le présent rapport a été préparé par MSECB MS pour donner suite à la demande d'évaluation d'un client à MSECB MS. L’objectif de ce rapport est de vérifier la conformité du client aux normes du système de management ou d'autres critères spécifiés. Le contenu du présent rapport ne s'applique qu'aux éléments qui étaient évidents pour MSECB MS au moment de l'audit et qui faisaient partie de son périmètre. MSECB MS ne garantit ni ne commente la pertinence du contenu du rapport ou du certificat à des fins ou utilisations particulières. MSECB MS n'accepte aucune responsabilité, quelle qu'elle soit, à l'égard des conséquences ou des mesures prises par des tiers à la suite de l'information contenue dans le présent rapport ou certificat ou en fonction de cette information.

Le présent audit est basé sur un processus d'échantillonnage de l'information disponible et ni les auditeurs ni MSECB MS ne peuvent garantir que toutes les non-conformités, le cas échéant, ont été détectées.

1. Information sur l'audit 5

1.1. Information sur l'organisation rganization information 5

1.2. Information sur l'audit 5

1.3. Périmètre de l'audit 6

2. Préparation et méthodologie d'audit 6

2.1. Objectifs d'audit 6

2.2. Critères d'audit 6

2.3. Méthodologie d'audit 7

2.4. Résultats des audits précédents 7

2.5. Planification d'audit 8

2.6. Principales personnes interviewées 8

2.7. Processus de plainte et d'appel de MSECB MS 8

3. Importantes pistes d'audit suivies 9

4. Constatations d'audit 30

4.1. Définition des constations d'audit 30

4.2. Non-conformités majeurs (voir aussi l'Annexe A) 31

4.3. Non-conformités mineures (voir aussi l'Annexe A) 31

4.4. Observations 31

4.5. Opportunités d'amélioration 31

4.6. Activités de suivi approuvées 31

4.7. Incertitude/obstacles qui pourraient avoir une incidence sur la fiabilité des conclusions d’audit 31

4.8. Divergences d’opinions non résolues entre l'équipe d’audit et la société auditéee 32

5. Conclusions et recommandations d'audit 33

5.1. Conformité et capacité du système de management 33

5.2. Conclusions d'audit 33

5.3. Recommandation 33

6. Annexe A : Rapport de non-conformité 34

6.1. Rapport de non-conformité 34

7. Annexe B : Informations sur la certification 35

8. Annexe C : Plan de surveillance 36

Lieu et date

M. John Smith (exemple)

Nom de l'organisation

J'ai audité le système de management (SM) de l’organisation ABC (nom de l'organisation) du 12 mai au 15 mai 2019.L'objectif principal de cet audit était d'évaluer si le système de management a été mis en œuvre avec succès et s'il est efficace, et d'évaluer la conformité de l'organisation aux exigences d'ISO/IEC 27001:2013. Sur la base de ces évaluations, il a été décidé de recommander ou non votre organisation pour la certification ISO/IEC 27001:2013.

L'équipe d'audit a effectué l'audit en fonction des processus définis dans l'organisation, conformément au plan d'audit. Cet audit, effectué par une équipe professionnelle, était un audit des processus et se concentrait sur les aspects, les risques et les objectifs importants. L'audit a été réalisé conformément aux normes ISO 19011 et ISO/IEC 17021, qui sont acceptées dans le monde entier. Ces normes exigent que notre équipe d'audit planifie et réalise l'audit afin d'acquérir l'assurance raisonnable que le système de management de votre organisation est efficace et que toutes les exigences de la norme ISO/IEC 27001:2013 ont été respectées.

Au cours du processus d'audit, le système de management s'est révélé globalement conforme aux exigences de la norme. L'équipe d’audit a conclu que votre organisation a établi et préservé son système de management conformément aux exigences de la norme et a prouvé la capacité du système à satisfaire de façon constante aux exigences approuvées pour les services inclus dans le périmètre de votre organisation et également à sa politique et à ses objectifs.

Le niveau de conformité à la norme peut encore être amélioré malgré le fait que (aucune non-conformité ou une seule non-conformité) ait été constatée lors de l'audit. Il s'agissait d'un audit par échantillonnage. Des non-conformités et d'autres opportunités d'amélioration peuvent encore être trouvées dans les domaines audités et non audités.

Se référant aux résultats du processus d'audit et à la preuve du développement et de la maturité de l'organisation, l'équipe d'audit recommande la certification du système de management de votre organisation à ISO/IEC 27001:2013.

Prénom et Nom

Auditeur principal

# Informations sur l’audit

## Informations sur l’organisation

|  |  |
| --- | --- |
| Nom de l’organisation : |  |
| Numéro de contrat : |  |
| Téléphone : |  |
| Site Web : |  |
| Nombre total d'employés : |  |
| Nombre total d'employés dans le périmètre :Veuillez justifier les employés non inclus dans le périmètre de la certification. |  |
|  |
| Nom du contact : |  |
| E-mail du contact : |  |
| Téléphone de contact : |  |

|  |
| --- |
| Sites : |
| **Site no** | **Adresse** | **Ville** | **État, Province, Pays** | **Code postal** | **Nombre d’employés dans le périmètre** |
| 1 (principal) |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |

## Informations sur l’audit

|  |  |
| --- | --- |
| Normes d’audit : |  |
| Type d’audit : | [ ]  Audit initial | [ ]  Surveillance 1 |
| [ ]  Recertification | [ ]  Surveillance 2 |
| Autre : |
| Dates d’audit : |  |
| Durée : |  |
| Auditeur principal : |  |
| Autres membres de l’équipe : |  |
| Autres intervenants et rôles : |  |

|  |  |
| --- | --- |
| **Site no** | **Sites audités** |
| 1 (principal) | [ ]  |
| 2 | [ ]  |
| 3 | [ ]  |
| 4 | [ ]  |

## Périmètre de l’audit

|  |  |
| --- | --- |
| Périmètre de la certification : |  |
| Date et version de la déclaration du périmètre : |  |
| Le périmètre a-t-il changé depuis le dernier audit ?  |  |
| Toutes les exclusions du périmètre sont appropriées et justifiées :Note importante : Les articles exclus du système de management audité doivent figurer sur le certificat. |  |

# Préparation et méthodologie d’audit

## Objectifs d’audit

L'objectif principal du présent audit est d'évaluer la mise en œuvre et l'efficacité du système de management de la sécurité de l'information (SMSI), y compris l'évaluation de la conformité aux exigences de la norme ISO/IEC 27001:2013.

Les objectifs spécifiques du présent audit sont de confirmer que :

* L'organisation a déterminé les limites et l'applicabilité du système de management concerné ;
* Le système de management est conforme à toutes les exigences des normes d'audit (articles 4 à 10 de la norme ISO/IEC 27001:2013) ;
* Le système de management est conforme à toutes les exigences légales et réglementaires applicables ;
* Le système de management est capable d'atteindre les objectifs des politiques de l'organisation ;
* L'organisation a établi, mis en œuvre, maintenu et amélioré continuellement son système de management, y compris les processus nécessaires et leurs interactions, conformément aux exigences de la norme ISO\IEC 27001:2013.

## Critères d’audit

Les critères d'audit (exigences) sont toutes des clauses normatives de la norme ISO/IEC 27001:2013 :

* Article 4 – Contexte de l'organisme
* Article 5 – Leadership
* Article 6 – Planification
* Article 7 – Support
* Article 8 – Fonctionnement
* Article 9 – Évaluation des performances
* Article 10 – Amélioration
* Annexe A (normative) Objectifs et mesures de référence
* Exigences supplémentaires
	+ Utilisation du logo et de la marque déposée
	+ Liste des documents inclus dans le SM audité

## Méthodologie d’audit

[Veuillez expliquer la méthodologie utilisée par l'équipe d'audit pour effectuer le présent audit, en vous inspirant de l’échantillon ci-dessous.]

L'équipe d'audit a réalisé un audit axé sur les processus en mettant l’accent sur les aspects, les risques et les objectifs importants. Les auditeurs ont utilisé des procédures d'audit pour recueillir des éléments probants en quantité et en qualité suffisantes pour valider la conformité du système de management de l'organisation. L'utilisation systématique des procédures d'audit réduit les risques liés à l’audit et renforce l'objectivité des conclusions d'audit.

L'équipe d’audit a utilisé une combinaison de procédures de collecte d'éléments probants pour créer son plan d'échantillonnage. Les méthodes d’audit utilisées sont les suivantes : entrevues, observations des activités, examen de la documentation et des dossiers, essais techniques et analyse de l'échantillonnage.

La procédure d'analyse permet à l'équipe d'audit de tirer des conclusions sur un ensemble en examinant une partie. Elle permet à l'auditeur d'estimer les caractéristiques d'une population en observant directement une partie de l'ensemble de cette population. La méthode d'échantillonnage utilisée au cours du présent audit était une technique d'échantillonnage systématique (ou échantillonnage par intervalles) avec une marge d’erreur de 3 à 5 %.

Les auditeurs eux-mêmes n'ont pas effectué d'essais techniques, incluant l'essai de l'efficacité d'un processus ou d'un contrôle. Les opérations ont toujours été effectuées par le personnel de la société auditée.

## Résultats des audits précédents

En préparation à cet audit, les résultats du dernier audit de ce système ont été revus, en particulier pour s'assurer que les actions correctives appropriées ont été mises en œuvre afin de corriger toute non-conformité identifiée. La présente revue a conclu que :

[ ]  Toutes les non-conformités identifiées lors d'audits précédents ont été corrigées et les actions correctives prises sont toujours efficaces.

[ ]  Toutes les non-conformités identifiées lors d'audits précédents n'ont pas été traitées de manière adéquate et le problème spécifique a été redéfini dans la section sur les non-conformités.

[ ]  Non applicable (aucun audit antérieur ou aucune non-conformité identifiée à l’audit précédent)

## Planification d’audit

[Décrivez comment l'équipe d'audit a planifié le présent audit. Veuillez consulter l'exemple ci-dessous.]

*L’auditeur principal a établi un premier contact avec la société auditée pour prendre des dispositions en vue du présent audit, y compris pour fixer les dates. L’auditeur principal a validé la faisabilité de l'audit, les objectifs, son périmètre, le lieu et les critères d'audit.*

*Le plan d'audit a été envoyé à la société auditée et il a été confirmé avant la réunion d'ouverture entre l'équipe d'audit et la société auditée.*

*L'audit sur site a débuté par une réunion d'ouverture à laquelle ont assisté le directeur général et le responsable SMSI. Le profil de MSECB MS, l'objet d’audit, la méthodologie, le système de rapport, le processus d'appel et la confidentialité ont été brièvement présentés au client lors de la réunion d'ouverture.*

## Principales personnes interviewées

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nom** | **Titre** | **Département/ Processus** | **Réunion d’ouverture (Oui ou non)** | **Réunion de clôture (Oui ou non)** | **Dates d’entrevue** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Processus de plainte et d’appel de MSECB MS

Tout client peut contester toute décision prise par l'équipe d'audit. Ces contestations doivent être interjetées par écrit et sont traitées selon la procédure de traitement des appels et des différends de MSECB. Si la direction de MSECB MS ne parvient pas à résoudre à l’interne le problème à la satisfaction du client, l’appel sera examiné par le Comité consultatif de MSECB.

Processus de plainte et d'appel de MSECB MS : [https://MSECB-ms.com/en/complaintAndAppealProcedure](https://pecb-ms.com/en/complaintAndAppealProcedure)

# Importantes pistes d'audit suivies

**Notes à l'usage de l'auditeur :**

*Dans la colonne « Statut », veuillez utiliser la légende suivante pour enregistrer les résultats de votre appréciation pour chaque article :*

***A*** *= Acceptable*

***N/A*** *= Non applicable (hors du domaine d'application)*

***MaNC*** *= Non-conformité majeure*

***MiNC*** *= Non-conformité mineure*

***OBS*** *= Observation*

***OFI*** *= Opportunité d'amélioration (Opportunity for improvement)*

*\*Les non-conformités sont expliquées à la « Section 4 : Constatations d'audit ».*

*Il convient que des preuves soient également fournies pour les articles « acceptables ».*

*Si une non-conformité est identifiée (mineure ou majeure), veuillez indiquer le numéro de la non-conformité dans la colonne « N° de NC ». Il convient qu'une description détaillée de la non-conformité soit fournie dans l'Annexe A – Rapport de non-conformité.*

*Si des OBS ou des OFI sont identifiées, veuillez expliquer en détail les conclusions dans les sections 4.4 et 4.5.*

| **Exigence de l’article** | **Statut** | **Preuve d’audit** | **N° de NC** |
| --- | --- | --- | --- |
|  |  | Constatations/Justification des constatations/Spécificités/Notes |  |
| **4 Contexte de l’organisme** |
| 4.1 | Compréhension de l’organisation et de son contexte |  |  |  |
| 4.2 | Compréhension des besoins et des attentes des parties intéressées |  |  |  |
| 4.3 | Détermination du domaine d’application du SMSI |  |  |  |
| 4.4 | Système de management de la sécurité de l’information |  |  |  |
| **5 Leadership** |
| 5.1  | Leadership et engagement |  |  |  |
| 5.2 | Politique |  |  |  |
| 5.3  | Rôles, responsabilités et autorités au sein de l’organisation |  |  |  |
| **6 Planification** |
| 6.1 | Actions liées aux risques et opportunités |  |  |  |
| 6.1.1 | Généralités |  |  |  |
| 6.1.2 | Appréciation des risques de sécurité de l'information |  |  |  |
| 6.1.3 | Traitement des risques de sécurité de l’information |  |  |  |
| 6.2 | Objectifs de sécurité de l’information et plans pour les atteindre |  |  |  |
| **7 Support** |
| 7.1 | Ressources |  |  |  |
| 7.2 | Compétence |  |  |  |
| 7.3 | Sensibilisation |  |  |  |
| 7.4 | Communication |  |  |  |
| 7.5 | Informations documentées |  |  |  |
| 7.5.1 | Généralités |  |  |  |
| 7.5.2 | Création et mise à jour |  |  |  |
| 7.5.3 | Maîtrise des informations documentées |  |  |  |
| **Fonctionnement** |
| 8.1 | Planification et contrôle opérationnels |  |  |  |
| 8.2 | Appréciation des risques de sécurité de l'information |  |  |  |
| 8.3 | Traitement des risques de sécurité de l’information |  |  |  |
| **9 Évaluation des performances** |
| 9.1 | Surveillance, mesure, analyse et évaluation |  |  |  |
| 9.2 | Audit interne |  |  |  |
| 9.3 | Revue de direction |  |  |  |
| **10 Amélioration** |
| 10.1 | Non-conformité et actions correctives |  |  |  |
| 10.2 | Amélioration continue |  |  |  |

|  |
| --- |
| **Exigences supplémentaires** |
| Utilisation du logo et de la marque déposée |  |  |  |
| Liste des documents inclus dans le SM audité |  |  |  |

| **Objectif et mesures de sécurité** | **Statut** | **Preuve d’audit** | **N° de NC** |
| --- | --- | --- | --- |
|  |  | Constatations/Justification des constatations/Spécificités/Notes |  |
| **A.5 Politiques de sécurité de l’information** |
| **A.5.1 Orientations de la direction en matière de sécurité de l’information**Objectif : 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** Mesure : Un ensemble de politiques de sécurité de l’information doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés. |  |  |  |
| A 5.1.2 | **Revue des politiques de sécurité de l’information** Mesure : 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.  |  |  |  |
| **A.6 Organisation de la sécurité de l’information** |
| **A.6.1 Organisation interne**Objectif : 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’organisation. |
| A 6.1.1 | **Fonctions et responsabilités liées à la sécurité de l’information** Mesure : Toutes les responsabilités en matière de sécurité de l’information doivent être définies et attribuées. |  |  |  |
| A 6.1.2 | **Séparation des tâches** Mesure : 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’organisation. |  |  |  |
| A 6.1.3 | **Relations avec les autorités** Mesure : Des relations appropriées avec les autorités compétentes doivent être entretenues. |  |  |  |
| A 6.1.4 | **Relations avec des groupes de travail spécialisés** Mesure : Des relations appropriées avec des groupes d’intérêt, des forums spécialisés dans la sécurité et des associations professionnelles doivent être entretenues. |  |  |  |
| A 6.1.5 | **La sécurité de l’information dans la gestion de projet** Mesure : La sécurité de l’information doit être considérée dans la gestion de projet, quel que soit le type de projet concerné. |  |  |  |
| **A.6.2 Appareils mobiles et télétravail**Objectif : Assurer la sécurité du télétravail et de l’utilisation d’appareils mobiles. |
| A 6.2.1 | **Politique en matière d’appareils mobiles** Mesure : Une politique et des mesures de sécurité complémentaires doivent être adoptées pour gérer les risques découlant de l’utilisation des appareils mobiles. |  |  |  |
| A 6.2.2 | **Télétravail** Mesure : 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. |  |  |  |
| **A.7 Sécurité des ressources humaines** |
| **A.7.1 Avant l’embauche**Objectif : 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** Mesure : Des vérifications doivent être effectuées sur tous les candidats à l’embauche conformément aux lois, aux règlements et à l’éthique et être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés. |  |  |  |
| A 7.1.2 | **Termes et conditions d’embauche** Mesure : Les accords contractuels entre les salariés et les sous-traitants doivent préciser leurs responsabilités et celles de l’organisation en matière de sécurité de l’information. |  |  |  |
| **A.7.2 Pendant la durée du contrat**Objectif : 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** Mesure : La direction doit demander à tous les salariés et sous-traitants d’appliquer les règles de sécurité de l’information conformément aux politiques et aux procédures en vigueur dans l’organisation. |  |  |  |
| A 7.2.2 | **Sensibilisation, apprentissage et formation à la sécurité de l’information** Mesure : L’ensemble des salariés de l’organisation 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’organisation s’appliquant à leurs fonctions. |  |  |  |
| A 7.2.3 | **Processus disciplinaire** Mesure : 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. |  |  |  |
| **A.7.3 Rupture, terme ou modification du contrat de travail**Objectif : Protéger les intérêts de l’organisation 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** Mesure : 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. |  |  |  |
| **A.8 Gestion des actifs** |
| **A.8.1 Responsabilités relatives aux actifs** Objectif : Identifier les actifs de l’organisation et définir les responsabilités pour une protection appropriée. |  |
| A 8.1.1 | **Inventaire des actifs** Mesure : 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. |  |  |  |
| A 8.1.2 | **Propriété des actifs** Mesure : Les actifs figurant à l’inventaire doivent être attribués à un propriétaire. |  |  |  |
| A 8.1.3 | **Utilisation correcte des actifs** Mesure : Les règles d’utilisation correcte de l’information, les actifs associés à l’information et les moyens de traitement de l’information doivent être identifiés, documentés et mis en œuvre. |  |  |  |
| A 8.1.4 | **Restitution des actifs** Mesure : Tous les salariés et les utilisateurs tiers doivent restituer la totalité des actifs de l’organisation qu’ils ont en leur possession au terme de la période d’emploi, du contrat ou de l’accord. |  |  |  |
| **A.8.2 Classification de l’information**Objectif : S’assurer que l’information bénéficie d’un niveau de protection approprié conforme à son importance pour l’organisation. |
| A 8.2.1 | **Classification des informations** Mesure : 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. |  |  |  |
| A 8.2.2 | **Marquage des informations** Mesure : Un ensemble approprié de procédures pour le marquage de l’information doit être élaboré et mis en œuvre conformément au plan de classification adopté par l’organisation. |  |  |  |
| A 8.2.3 | **Manipulation des actifs** Mesure : 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’organisation. |  |  |  |
| **A.8.3 Manipulation des supports**Objectif : Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de l’information de l’organisation stockée sur des supports. |
| A 8.3.1 | **Gestion des supports amovibles** Mesure : Des procédures de gestion des supports amovibles doivent être mises en œuvre conformément au plan de classification adopté par l’organisation. |  |  |  |
| A 8.3.2 | **Mise au rebut des supports**  Mesure : Les supports qui ne sont plus nécessaires doivent être mis au rebut de manière sécurisée en suivant des procédures formelles. |  |  |  |
|  A 8.3.3 | **Transfert physique des supports**  Mesure : Les supports contenant de l’information doivent être protégés contre les accès non autorisés, les erreurs d’utilisation et l’altération lors du transport. |  |  |  |
| **A.9 Contrôle d’accès** |
| **A.9.1 Exigences métier en matière de contrôle d’accès**Objectif : Limiter l’accès à l’information et aux moyens de traitement de l’information.  |
| A 9.1.1 | **Politique de contrôle d’accès**  Mesure : Une politique de contrôle d’accès doit être établie, documentée et revue sur la base des exigences métier et de sécurité de l’information. |  |  |  |
| A 9.1.2 | **Accès aux réseaux et aux services réseau**  Mesure : Les utilisateurs doivent avoir uniquement accès au réseau et aux services réseau pour lesquels ils ont spécifiquement reçu une autorisation. |  |  |  |
| **A.9.2 Gestion de l’accès utilisateur**Objectif : 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** Mesure : Un processus formel d’enregistrement et de désinscription des utilisateurs doit être mis en œuvre pour permettre l’attribution des droits d’accès. |  |  |  |
| A 9.2.2 | **Distribution des accès aux utilisateurs** Mesure : Un processus formel de distribution des accès aux utilisateurs doit être mis en œuvre pour attribuer et retirer des droits d’accès à tous types d’utilisateurs sur l’ensemble des services et des systèmes. |  |  |  |
| A 9.2.3 | **Gestion des droits d’accès à privilèges** Mesure : L’allocation et l’utilisation des droits d’accès à privilèges doivent être restreintes et contrôlées. |  |  |  |
| A 9.2.4 | **Gestion des informations secrètes d’authentification des utilisateurs** Mesure : L’attribution des informations secrètes d’authentification doit être réalisée dans le cadre d’un processus de gestion formel. |  |  |  |
| A 9.2.5 | **Revue des droits d’accès utilisateurs**  Mesure : Les propriétaires d’actifs doivent vérifier les droits d’accès des utilisateurs à intervalles réguliers. |  |  |  |
| A 9.2.6 | **Suppression ou adaptation des droits d’accès** Mesure : Les droits d’accès aux informations et aux moyens de traitement des informations de l’ensemble des salariés et utilisateurs tiers doivent être supprimés à la fin de leur période d’emploi, ou adaptés en cas de modification du contrat ou de l’accord. |  |  |  |
| **A.9.3 Responsabilités des utilisateurs**Objectif : Rendre les utilisateurs responsables de la protection de leurs informations d’authentification.  |
| A 9.3.1 | **Utilisation d’informations secrètes d’authentification** Mesure : Les utilisateurs doivent suivre les pratiques de l’organisation pour l’utilisation des informations secrètes d’authentification. |  |  |  |
| **A.9.4 Contrôle de l’accès au système et à l’information**Objectif : Empêcher les accès non autorisés aux systèmes et aux applications.  |
| A 9.4.1 | **Restriction d’accès à l’information** Mesure : L’accès à l’information et aux fonctions d’application système doit être restreint conformément à la politique de contrôle d’accès. |  |  |  |
| A 9.4.2 | **Sécuriser les procédures de connexion**  Mesure : Lorsque la politique de contrôle d’accès l’exige, l’accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée. |  |  |  |
| A 9.4.3 | **Système de gestion des mots de passe** Mesure : Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent garantir la qualité des mots de passe. |  |  |  |
|  A 9.4.4 | **Utilisation de programmes utilitaires à privilèges** Mesure : L’utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d’un système ou d’une application doit être limitée et étroitement contrôlée. |  |  |  |
| A 9.4.5 | **Contrôle d’accès au code source des programmes** Mesure : L’accès au code source des programmes doit être restreint.  |  |  |  |
| **A.10 Cryptographie** |
| **A.10.1 Mesures cryptographiques**Objectif : Garantir l’utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l’authenticité et/ou l’intégrité de l’information. |
| A 10.1.1 | **Politique d’utilisation des mesures cryptographiques**  Mesure : Une politique d’utilisation des mesures cryptographiques en vue de protéger l’information doit être élaborée et mise en œuvre. |  |  |  |
| A 10.1.2 | **Gestion des clés**  Mesure : Une politique sur l’utilisation, la protection et la durée de vie des clés cryptographiques doit être élaborée et mise en œuvre tout au long de leur cycle de vie. |  |  |  |
| **A.11 Sécurité physique et environnementale** |
| **A.11.1 Zones sécurisées**Objectif : Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l’information et les moyens de traitement de l’information de l’organisation. |
| A 11.1.1 | **Périmètre de sécurité physique**  Mesure : Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones contenant l’information sensible ou critique et les moyens de traitement de l’information. |  |  |  |
| A 11.1.2 | **Contrôle d’accès physique** Mesure : Les zones sécurisées doivent être protégées par des contrôles adéquats à l’entrée pour s’assurer que seul le personnel autorisé est admis. |  |  |  |
| A 11.1.3 | **Sécurisation des bureaux, des salles et des équipements** Mesure : Des mesures de sécurité physique aux bureaux, aux salles et aux équipements doivent être conçues et appliquées. |  |  |  |
| A 11.1.4 | **Protection contre les menaces extérieures et environnementales** Mesure : Des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents doivent être conçues et appliquées. |  |  |  |
| A 11.1.5 | **Travail dans les zones sécurisées**  Mesure : Des procédures pour le travail dans les zones sécurisées doivent être conçues et appliquées. |  |  |  |
| A 11.1.6 | **Zones de livraison et de chargement** Mesure : Les points d’accès tels que les zones de livraison et de chargement et les autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux doivent être contrôlés et, si possible, isolés des moyens de traitement de l’information, de façon à éviter les accès non autorisés. |  |  |  |
| **A.11.2 Matériels**Objectif : Empêcher la perte, l’endommagement, le vol ou la compromission des actifs et l’interruption des activités de l’organisation.  |
| A 11.2.1 | **Emplacement et protection des matériels** Mesure : Les matériels doivent être localisés et protégés de manière à réduire les risques liés à des menaces et des dangers environnementaux et les possibilités d’accès non autorisé. |  |  |  |
| A 11.2.2 | **Services généraux**  Mesure : Les matériels doivent être protégés des coupures de courant et autres perturbations dues à une défaillance des services généraux. |  |  |  |
| A 11.2.3 | **Sécurité du câblage**  Mesure : Les câbles électriques ou de télécommunication transportant des données ou supportant les services d’information doivent être protégés contre toute interception ou tout dommage. |  |  |  |
| A 11.2.4 | **Maintenance des matériels** Mesure : Les matériels doivent être entretenus correctement pour garantir leur disponibilité permanente et leur intégrité. |  |  |  |
| A 11.2.5 | **Sortie des actifs**  Mesure : Les matériels, les informations ou les logiciels des locaux de l’organisation ne doivent pas sortir sans autorisation préalable. |  |  |  |
| A 11.2.6 | **Sécurité des matériels et des actifs hors des locaux** Mesure : Des mesures de sécurité doivent être appliquées aux matériels utilisés hors des locaux de l’organisation en tenant compte des différents risques associés au travail hors site. |  |  |  |
| A 11.2.7 | **Mise au rebut ou recyclage sécurisé(e) des matériels** Mesure : 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. |  |  |  |
| A 11.2.8 | **Matériels utilisateur laissés sans surveillance**  Mesure : Les utilisateurs doivent s’assurer que les matériels non surveillés sont dotés d’une protection appropriée. |  |  |  |
| A 11.2.9 | **Politique du bureau propre et de l’écran verrouillé** Mesure : Une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l’écran verrouillé pour les moyens de traitement de l’information doivent être adoptées. |  |  |  |
| **A.12 Sécurité liée à l’exploitation** |
| **A.12.1 Procédures et responsabilités liées à l’exploitation**Objectif : Assurer l’exploitation correcte et sécurisée des moyens de traitement de l’information. |
| A 12.1.1 | **Procédures d’exploitation documentées**  Mesure : Les procédures d’exploitation doivent être documentées et mises à disposition de tous les utilisateurs concernés. |  |  |  |
| A 12.1.2 | **Gestion des changements**  Mesure : Les changements apportés à l’organisation, aux processus métier, aux systèmes et moyens de traitement de l’information ayant une incidence sur la sécurité de l’information doivent être contrôlés. |  |  |  |
| A 12.1.3 | **Dimensionnement**  Mesure : 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. |  |  |  |
| A 12.1.4 | **Séparation des environnements de développement, de test et d’exploitation** Mesure : 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. |  |  |  |
| **A.12.2 Protection contre les logiciels malveillants**Objectif : 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**  Mesure : 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. |  |  |  |
| **12.3 Sauvegarde**Objectif : Se protéger de la perte de données. |
| A 12.3.1 | **Sauvegarde des informations**  Mesure : 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. |  |  |  |
| **A.12.4 Journalisation et surveillance**Objectif : Enregistrer les événements et générer des preuves. |
| A 12.4.1 | **Journalisation des événements** Mesure : 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 jour et vérifiés régulièrement. |  |  |  |
| A 12.4.2  | **Protection de l’information journalisée**  Mesure : Les moyens de journalisation et d’information journalisée doivent être protégés contre les risques de falsification ou d’accès non autorisé. |  |  |  |
| A 12.4.3 | **Journaux administrateur et opérateur** Mesure : Les activités de l’administrateur système et de l’opérateur système doivent être journalisées, protégées et vérifiées régulièrement.  |  |  |  |
| A 12.4.4 | **Synchronisation des horloges** Mesure : Les horloges de l’ensemble des systèmes de traitement de l’information concernés d’une organisation ou d’un domaine de sécurité doivent être synchronisées sur une source de référence temporelle unique. |  |  |  |
| **A.12.5 Maîtrise des logiciels en exploitation**Objectif : Garantir l’intégrité des systèmes en exploitation.  |
| A 12.5.1 | **Installation de logiciels sur des systèmes en exploitation** Mesure : Des procédures doivent être mises en œuvre pour contrôler l’installation de logiciel sur des systèmes en exploitation. |  |  |  |
| **A.12.6 Gestion des vulnérabilités techniques** Objectif : Empêcher toute exploitation des vulnérabilités techniques.  |
| A 12.6.1  | **Gestion des vulnérabilités techniques**  Mesure : Des informations sur les vulnérabilités techniques des systèmes d’information en exploitation doivent être obtenues en temps opportun, l’exposition de l’organisation à ces vulnérabilités doit être évaluée et les mesures appropriées doivent être prises pour traiter le risque associé. |  |  |  |
| A 12.6.2 | **Restrictions liées à l’installation de logiciels** Mesure : Des règles régissant l’installation de logiciels par les utilisateurs doivent être établies et mises en œuvre. |  |  |  |
| **A.12.7 Considérations sur l’audit des systèmes d’information**Objectif : 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**  Mesure : 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. |  |  |  |
| **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**  Mesure : Les réseaux doivent être gérés et contrôlés pour protéger l’information contenue dans les systèmes et les applications. |  |  |  |
| A 13.1.2 | **Sécurité des services de réseau** Mesure : 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 les accords de services de réseau, que ces services soient fournis en interne ou externalisés. |  |  |  |
| A 13.1.3 | **Cloisonnement des réseaux**  Mesure : Les groupes de services d’information, d’utilisateurs et de systèmes d’information doivent être cloisonnés sur les réseaux. |  |  |  |
| **A.13.2 Transfert de l’information**Objectif : 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** Mesure : 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. |  |  |  |
| A 13.2.2 | **Accords en matière de transfert d’information** Mesure : Des accords doivent traiter du transfert sécurisé de l’information liée à l’activité entre l’organisation et les tiers. |  |  |  |
| A 13.2.3 | **Messagerie électronique** Mesure : L’information transitant par la messagerie électronique doit être protégée de manière appropriée. |  |  |  |
| A 13.2.4 | **Engagements de confidentialité ou de non-divulgation**  Mesure : Les exigences en matière d’engagements de confidentialité ou de non-divulgation, doivent être identifiées, vérifiées régulièrement et documentées conformément aux besoins de l’organisation. |  |  |  |
| **A.14 Acquisition, développement et maintenance des systèmes d’information** |
| **A.14.1 Exigences de sécurité applicables aux systèmes d’information**Objectif : 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** Mesure : 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. |  |  |  |
| A 14.1.2 | **Sécurisation des services d’application sur les réseaux publics** Mesure : 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. |  |  |  |
| A 14.1.3 | **Protection des transactions liées aux services d’application**  Mesure : Les informations impliquées dans les transactions liées aux services d’application doivent être protégées pour empêcher une transmission incomplète, des erreurs d’acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou sa réémission. |  |  |  |
| **A.14.2 Sécurité des processus de développement et d’assistance technique**Objectif : 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** Mesure : Des règles de développement des logiciels et des systèmes doivent être établies et appliquées aux développements de l’organisation. |  |  |  |
| A 14.2.2 | **Procédures de contrôle des changements de système** Mesure : Les changements des systèmes dans le cadre du cycle de développement doivent être contrôlés par le biais de procédures formelles. |  |  |  |
| A 14.2.3 | **Revue technique des applications après changement apporté à la plateforme d’exploitation** Mesure : Lorsque des changements sont apportés aux plateformes d’exploitation, les applications critiques métier doivent être vérifiées et testées afin de vérifier l’absence de tout effet indésirable sur l’activité ou sur la sécurité. |  |  |  |
| A 14.2.4 | **Restrictions relatives aux changements apportés aux progiciels** Mesure : Les modifications des progiciels ne doivent pas être encouragées, être limitées aux changements nécessaires et tout changement doit être strictement contrôlé. |  |  |  |
| A 14.2.5 | **Principes d’ingénierie de la sécurité des systèmes** Mesure : Des principes d’ingénierie 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. |  |  |  |
| A 14.2.6 | **Environnement de développement sécurisé** Mesure : Les organisations doivent établir des environnements de développement sécurisés pour les tâches de développement et d’intégration du système, qui englobe l’intégralité du cycle de vie du développement du système, et en assurer la protection de manière appropriée. |  |  |  |
| A 14.2.7 | **Développement externalisé**  Mesure : L’organisation doit superviser et contrôler l’activité de développement du système externalisée. |  |  |  |
| A 14.2.8 | **Test de la sécurité du système**  Mesure : Les tests de fonctionnalité de la sécurité doivent être réalisés pendant le développement. |  |  |  |
| A 14.2.9 | **Test de conformité du système** Mesure : Des programmes de test de conformité et des critères associés doivent être déterminés pour les nouveaux systèmes d’information, les mises à jour et les nouvelles versions. |  |  |  |
| **A.14.3 Données de test**Objectif : Garantir la protection des données utilisées pour les tests.  |
| A 14.3.1 | **Protection des données de test**  Mesure : Les données de test doivent être sélectionnées avec soin, protégées et contrôlées. |  |  |  |
| **A.15 Relations avec les fournisseurs** |
| **A.15.1 Sécurité dans les relations avec les fournisseurs**Objectif : Garantir la protection des actifs de l’organisation accessible aux fournisseurs. |
| A 15.1.1 | **Politique de sécurité de l’information dans les relations avec les fournisseurs** Mesure : Des exigences de sécurité de l’information pour limiter les risques résultant de l’accès des fournisseurs aux actifs de l’organisation doivent être acceptées par le fournisseur et documentées. |  |  |  |
| A 15.1.2 | **La sécurité dans les accords conclus avec les fournisseurs** Mesure : 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 l’infrastructure informatique destinés à l’information de l’organisation. |  |  |  |
| A 15.1.3 | **Chaîne d’approvisionnement des produits et des services informatiques** Mesure : 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. |  |  |  |
| **A.15.2 Gestion de la prestation du service**Objectif : 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**  Mesure : Les organisations doivent surveiller, vérifier et auditer à intervalles réguliers la prestation des services assurés par les fournisseurs. |  |  |  |
| A 15.2.2 | **Gestion des changements apportés dans les services des fournisseurs**  Mesure : 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. |  |  |  |
| **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**Objectif : 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** Mesure : 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. |  |  |  |
| A 16.1.2 | **Signalement des événements liés à la sécurité de l’information**  Mesure : Les événements liés à la sécurité de l’information doivent être signalés dans les meilleurs délais par les voies hiérarchiques appropriées. |  |  |  |
| A 16.1.3 | **Signalement des failles liées à la sécurité de l’information**  Mesure : Les salariés et les sous-traitants utilisant les systèmes et services d’information de l’organisation doivent noter et signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services. |  |  |  |
| A 16.1.4 | **Appréciation des événements liés à la sécurité de l’information et prise de décision** Mesure : Les événements liés à la sécurité de l’information doivent être appréciés et il doit être décidé s’il faut les classer comme incidents liés à la sécurité de l’information. |  |  |  |
| A 16.1.5 | **Tirer des enseignements des incidents liés à la sécurité de l’information**  Mesure : Les incidents liés à la sécurité de l’information doivent être traités conformément aux procédures documentées. |  |  |  |
| A 16.1.6 | **Tirer des enseignements des incidents liés à la sécurité de l’information** Mesure : Les connaissances recueillies suite à l’analyse et la résolution d’incidents doivent être utilisées pour réduire la probabilité ou l’impact d’incidents ultérieurs. |  |  |  |
| A 16.1.7 | **Collecte de preuves** Mesure : L’organisation doit définir et appliquer des procédures d’identification, de collecte, d’acquisition et de protection de l’information pouvant servir de preuve. |  |  |  |
| **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**Objectif : 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** Mesure : L’organisation doit déterminer ses exigences en matière de sécurité de l’information et de continuité de management de la sécurité de l’information dans des situations défavorables, comme lors d’une crise ou d’un sinistre |  |  |  |
| A 17.1.2 | **Organisation de la continuité de la sécurité de l’information** Mesure : L’organisation 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 défavorable. |  |  |  |
| A 17.1.3 | **Vérifier, revoir et évaluer la continuité de la sécurité de l’information**  Mesure : L’organisation doit vérifier les mesures de continuité de la sécurité de l’information mises en œuvre à intervalles réguliers afin de s’assurer qu’elles sont valables et efficaces dans des situations défavorables. |  |  |  |
| **A.17.2 Redondances**Objectif :Garantir la disponibilité des moyens de traitement de l’information  |
| A 17.2.1 | **Garantir la disponibilité des moyens de traitement de l’information**  Mesure : Des moyens de traitement de l’information doivent être mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilité. |  |  |  |
| **A.18 Conformité** |
| **A.18.1 Conformité aux obligations légales et réglementaires**Objectif : 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** Mesure : Toutes les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l’approche adoptée par l’organisation pour satisfaire à ces exigences, doivent être explicitement définies, documentées et mises à jour pour chaque système d’information et pour l’organisation elle-même. |  |  |  |
| A 18.1.2 | **Droits de propriété intellectuelle** Mesure : Des procédures appropriées doivent être mises en œuvre pour garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l’usage des licences de logiciels propriétaires. |  |  |  |
| A 18.1.3 | **Protection des enregistrements** Mesure : 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. |  |  |  |
| A 18.1.4 | **Protection de la vie privée et protection des données à caractère personnel** Mesure : 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. |  |  |  |
| A 18.1.5 | **Réglementation relative aux mesures cryptographiques**  Mesure : Des mesures cryptographiques doivent être prises conformément aux accords, législation et réglementations applicables. |  |  |  |
| **A.18.2 Revue de la sécurité de l’information**Objectif : 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**  Mesure : 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 lorsque des changements importants sont intervenus. |  |  |  |
| A 18.2.2 | **Conformité avec les politiques et les normes de sécurité** Mesure : 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. |  |  |  |
| A 18.2.3 | **Vérification de la conformité technique** Mesure : 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’organisation. |  |  |  |

# Constatations d’audit

Les constatations d’audit ont été communiquées à la direction générale de l'organisation au cours de la réunion de clôture. La conclusion finale des résultats d’audit et la recommandation de l'équipe d'audit ont également été communiquées à la direction au cours de la même réunion.

## Définition des constatations d’audit

L'évaluation des constatations d’audit est établie sur la base des définitions suivantes :

**Non-conformités majeures (MaNC)**

**L'absence ou la défaillance totale** d'un système à répondre à une exigence. Il peut s'agir de l'un ou l'autre des cas suivants :

* Un certain nombre de non-conformités mineures à une exigence peuvent représenter une défaillance totale du système et donc être considéré comme une non-conformité majeure ; ou
* Toute non-conformité qui entraînerait l'expédition probable d'un produit non conforme. Une condition qui peut entraîner la défaillance ou réduire de façon importante l'utilisabilité des produits ou services pour l'usage auquel ils sont destinés ; ou
* Une non-conformité que le jugement et l'expérience indiquent être susceptible soit d'entraîner la défaillance du système de qualité, soit de réduire sensiblement sa capacité à garantir des processus et des produits contrôlés.

**Non-conformités mineures (MiNC)**

Toute **non-conformité** que le jugement et l'expérience **indiquent ne pas être susceptible soit d'entraîner la défaillance du système** de qualité, soit de **réduire sensiblement sa capacité** à garantir des processus et des produits contrôlés. Il peut s'agir de :

* une défaillance d'une partie du système qualité documenté du fournisseur par rapport à un besoin ; ou
* un simple écart observé dans le suivi d'un élément du SMQ d'une entreprise.

**Observations (OBS)**

Toutes les erreurs **susceptibles de devenir des NC**, si elles ne sont pas traitées avant le prochain audit, sont marquées comme observations (OBS). Aucune réponse n'est exigée.

**Opportunités d'amélioration (OFI)**

Si **certains aspects** qui sont généralement conformes aux exigences de la norme doivent être améliorés, ils sont considérés comme des opportunités d'amélioration (*OFI – Opportunities for Improvement*). Ces OFI contribuent à améliorer le système de management dans son ensemble ou les processus désignés. Aucune réponse n'est exigée.

## Non-conformités majeures (voir aussi l’Annexe A)

Expliquez si des non-conformités majeures ont été détectées au cours de l'audit.

## Non-conformités mineures (voir aussi l'Annexe A)

Expliquez si des non-conformités mineures ont été détectées au cours de l'audit.

## Observations

Énumérez toutes les observations ou problèmes notés qui pourraient devenir des non-conformités.

## Opportunités d'amélioration

*Énumérez toutes les opportunités d'amélioration notées, sans recommandation précise de correction.*

## Activités de suivi approuvées

Les non-conformités décrites ici doivent être abordées par le biais du processus d’actions correctives de l'organisation, conformément aux exigences pertinentes de la norme d’audit, y compris les actions visant à analyser la cause de la non-conformité, à prévenir la récurrence et à compléter les registres tenus.

Les actions correctives visant à corriger les non-conformités majeures identifiées doivent être mises en œuvre immédiatement et MSECB MS doit être avisée des actions prises dans les 30 jours. Pour confirmer les actions prises, évaluer leur efficacité et déterminer si la certification peut être accordée ou maintenue, un auditeur de MSECB MS effectuera une visite de suivi dans les 90 jours.

Les actions correctives visant à corriger les non-conformités mineures identifiées doivent être documentées dans un plan d'action et envoyées dans les 30 jours par le client à l'auditeur pour revue. Si les actions sont jugées satisfaisantes, elles feront l'objet d'un suivi lors du prochain audit prévu.

Les non-conformités doivent être traitées par le processus d’actions correctives du client, notamment par :

* Les actions prises pour déterminer l'étendue et contenir la non-conformité spécifique.
* La cause fondamentale (résultats d'une enquête visant à déterminer la ou les causes les plus fondamentales de la non-conformité).
* Les actions prises pour corriger la non-conformité et, en réponse à la cause fondamentale, pour éliminer la récurrence de la non-conformité.
* La réponse aux actions correctives doit être soumise à l'auditeur principal de MSECB MS.
* Le client doit tenir des dossiers sur les actions correctives, y compris des preuves objectives, pendant au moins trois (3) ans.

## Incertitude/obstacles qui pourraient avoir une incidence sur la fiabilité des conclusions d’audit

Veuillez préciser.

## Divergences d’opinions non résolues entre l'équipe d’audit et la société auditée

Veuillez préciser.

# Conclusions et recommandations d’audit

## Conformité et capacité du système de management

*[Veuillez décrire si le système de management a démontré sa conformité aux exigences de la norme d'audit et fourni une structure adéquate pour soutenir la mise en œuvre et la maintenance du système de management.*

*C'est-à-dire :*

* *preuve de la mise en œuvre et de la maintenance efficaces du SM*
* *preuve de la définition et de la surveillance des objectifs et des objectifs de performance clés correspondants*
* *mise en œuvre du programme d'audit interne, etc.]*

## Conclusions d’audit

|  |  |
| --- | --- |
| Y a-t-il eu des écarts importants par rapport au plan d'audit ? (Si oui, veuillez préciser.) | Oui [ ]  Non [ ]  |
| Y a-t-il des problèmes importants qui ont une incidence sur le programme d’audit ? (Si oui, veuillez préciser.) | Oui [ ]  Non [ ]  |
| Y a-t-il eu des changements importants qui ont affecté le SM depuis le dernier audit ? (Si oui, veuillez énumérer les changements importants.) | Oui [ ]  Non [ ]  N/A [ ]  |
| Y a-t-il des problèmes non résolus ayant une incidence sur le système de management depuis le dernier audit ? (Si oui, veuillez énumérer les problèmes non résolus.) | Oui [ ]  Non [ ]  N/A [ ]  |
| La vérification de l'efficacité des actions correctives prises à l'égard des non-conformités relevées antérieurement a été effectuée et est satisfaisante. (Veuillez inscrire tout commentaire au besoin.) | Oui [ ]  Non [ ]  N/A [ ]  |
| Le système de management est conçu pour atteindre les objectifs stratégiques de l'organisation. | Oui [ ]  Non [ ]  |
| Le système de management est conçu pour répondre aux exigences légales, réglementaires et contractuelles. | Oui [ ]  Non [ ]  |
| Les processus d'audit interne et de revue de direction sont en place et adéquats. | Oui [ ]  Non [ ]  |
| L'audit a permis d'atteindre les objectifs énoncés. | Oui [ ]  Non [ ]  |

## Recommandation

*Recommandation de l'auditeur principal :*

*[Veuillez recommander s'il convient de certifier ou non le système de management de l'organisation auditée.]*



# Annexe A : Rapport de non-conformité

## Rapport de non-conformité

Note : Si plus d'une non-conformité a été détectée, veuillez ajouter d'autres rapports de NC.

|  |
| --- |
| **RAPPORT DE NON-CONFORMITÉ** |
| **À REMPLIR PAR L’AUDITEUR** | **DATE** | **ORGANISATION** | **No DE NC** |
|  |  |  |
| **NORME :** ISO/IEC 27001:2013 |
| **NON-CONFORMITÉ OBSERVÉE DANS LE PROCESSUS/DOMAINE** |  |
| **EXIGENCE DE LA NORME :**  | **ARTICLE :**  |
| **NON CONFORMITÉ – DESCRIPTION DES PREUVES OBJECTIVES** |
|  |
| **CATÉGORIE (Majeure/ Mineure)** | **AUDITEUR PRINCIPAL** | **AUDITEUR** | **REPRÉSENTANT PROCESSUS MÉTIERS** |
|  |  |  |  |
| **À REMPLIR AVANT** |
|  |
| **À REMPLIR PAR L’ORGANISATION** | **ANALYSE DES CAUSES (Ce qui a échoué dans le système, permettant à cette NC de se produire)** |
|  |
| **CORRECTION ET ACTION CORRECTIVE (Ce qui est fait pour résoudre ce problème et empêcher qu'il ne se reproduise)** |
| CORRECTION : ACTION CORRECTIVE :  |
| **VÉRIFICATION DES ACTIONS CORRECTIVES** | **DATE DE FINALISATION** |  |
| **REPRÉSENTANT DE L'ORGANISATION** |  |
| **À REMPLIR PAR L’AUDITEUR**  | **VÉRIFICATION DES CORRECTIONS/ACTIONS CORRECTIVES** | **DATE** | **STATUT** | **AUDITEUR PRINCIPAL** |
|  |  |  |
| **COMMENTAIRES DE L'AUDITEUR (incluant les preuves vérifiées pour accepter les actions correctives)** |  |

# Annexe B : Informations sur la certification

|  |
| --- |
| **INFORMATIONS GÉNÉRALES** |
| **Nombre de certificats** (copie papier) |  |
| **Langues** | [ ]  Anglais | [ ]  Français |
| **Nom de l'entreprise** (à inscrire sur le certificat) |  |
| **Adresse** (à indiquer sur le certificat) |  |
| **Déclaration du périmètre de certification** (à inclure sur le certificat)**Note importante\*** La déclaration du périmètre doit être précise et n'inclure **que** les processus et procédures du système de management qui ont été évalués au cours de l'audit. Le nom ou l'adresse de l'entreprise ne doit pas être écrit dans cette déclaration puisqu'ils sont mentionnés dans des espaces prévus à cet effet. Pour ISO/IEC 27001, il est obligatoire d'indiquer également la version SoA.  |  |
| **Articles exclus du système de management audité** (à inclure sur le certificat) |  |
| **ADRESSE DE LIVRAISON**  |
| Titre (M., Mme) |  |
| Prénom |  |
| Nom |  |
| Adresse |  |
| Ville |  |
| Pays |  |
| Province/État/Région |  |
| Code postal |  |
| Adresse e-mail |  |

# Annexe C : Plan de surveillance

|  |
| --- |
| **Plan de surveillanceISO/IEC 27001:2013** |
| **1** : Audit initial**2 :** Audit de surveillance 1**3** : Audit de surveillance 2**4** : Audit de recertification | **Plan** |
| **1****(202X)** | **2** **(202X)** | **3****(202X)** | **4****(202X)** |
| **Articles d’ISO/IEC 27001:2013** |
| **4 Contexte de l’organisme** |
| **4.1** | Compréhension de l’organisation et de son contexte |  |  |  |  |
| **4.2** | Compréhension des besoins et des attentes des parties intéressées |  |  |  |  |
| **4.3** | Détermination du domaine d’application du système de management de la sécurité de l’information |  |  |  |  |
| **4.4** | Système de management de la sécurité de l’information |  |  |  |  |
| **5 Leadership** |
| **5.1** | Leadership et engagement |  |  |  |  |
| **5.2** | Politique |  |  |  |  |
| **5.3** | Rôles, responsabilités et autorités au sein de l’organisation |  |  |  |  |
| **6 Planification** |
| **6.1** | Actions liées aux risques et opportunités |  |  |  |  |
| **6.2** | Objectifs de sécurité de l’information et plans pour les atteindre |  |  |  |  |
| **7 Support** |
| **7.1** | Ressources |  |  |  |  |
| **7.2** | Compétence |  |  |  |  |
| **7.3** | Sensibilisation |  |  |  |  |
| **7.4** | Communication |  |  |  |  |
| **7.5** | Informations documentées |  |  |  |  |
| **8 Fonctionnement** |
| **8.1** | Planification et contrôle opérationnels |  |  |  |  |
| **8.2** | Appréciation des risques de sécurité de l'information |  |  |  |  |
| **8.3** | Traitement des risques de sécurité de l’information |  |  |  |  |
| **9 Évaluation des performances** |
| **9.1** | Surveillance, mesure, analyse et évaluation |  |  |  |  |
| **9.2** | Audit interne |  |  |  |  |
| **9.3** | Revue de direction |  |  |  |  |
| **10 Amélioration** |
| **10.1** | Non-conformité et actions correctives |  |  |  |  |
| **10.2** | Amélioration continue |  |  |  |  |
| **Objectifs et mesures de référence** |
| **A.5** | Politiques de sécurité de l’information |  |  |  |  |
| **A.6** | Organisation de la sécurité de l’information |  |  |  |  |
| **A.7** | Sécurité des ressources humaines |  |  |  |  |
| **A.8** | Gestion des actifs |  |  |  |  |
| **A.9** | Contrôle d’accès |  |  |  |  |
| **A.10** | Cryptographie |  |  |  |  |
| **A.11** | Sécurité physique et environnementale |  |  |  |  |
| **A.12** | Sécurité liée à l’exploitation |  |  |  |  |
| **A.13** | Sécurité des communications |  |  |  |  |
| **A.14** | Acquisition, développement et maintenance des systèmes d’information |  |  |  |  |
| **A.15** | Relations avec les fournisseurs |  |  |  |  |
| **A.16** | Gestion des incidents liés à la sécurité de l’information |  |  |  |  |
| **A.17** | Aspects de la sécurité de l’information dans la gestion de la continuité de l’activité |  |  |  |  |
| **A.18** | Conformité |  |  |  |  |
| **Exigences supplémentaires** |
|  | Utilisation du logo et de la marque déposée |  |  |  |  |
|  | Liste des documents inclus dans le SM audité |  |  |  |  |
| **Notes et commentaires :** |  |

*Pour les visites terminées, marquez « X » dans la case pour chaque article/processus couvert.*

*Pour les visites planifiées, marquez « O » dans la case pour chaque article/processus à couvrir.*