[Logo de l'organisation]

[Nom de l'organisation]

# PROCEDURE D'AUDIT INTERNE

| | |
|---|---|
| Code : | |
| Version : | |
| Date de la version : | |
| Créé par : | |
| Approuvée par : | |
| Niveau de confidentialité : | |

**Commented [AES1]:** Pour apprendre à remplir ce document et pour consulter des exemples concrets de ce que vous devez rédiger, regardez ce tutoriel vidéo : "How to Write ISO 27001/ISO 22301 Internal Audit Procedure and Audit Program".

Pour accéder au tutoriel : dans votre boîte de réception, consultez l'e-mail que vous avez reçu au moment de l'achat. Vous y trouverez un lien et un mot de passe qui vous permettront d'accéder au tutoriel vidéo.

**Commented [AES2]:** Remplissez tous les champs entre crochets [ ] dans ce document.

**Commented [AES3]:** Si vous avez besoin d'aide pour réaliser l'audit interne ISO 27001 / ISO 22301 dans votre organisation, consultez le ISO Consultant Directory pour trouver l'expert adapté.

**Commented [AES4]:** Pour en savoir plus sur ce sujet, consultez ces articles :

- Dilemmas with ISO 27001 internal auditors
https://advisera.com/27001academy/blog/2010/03/22/dilemmas-with-iso-27001-bs-25999-2-internal-auditors/

- How to prepare for an ISO 27001 internal audit
https://advisera.com/27001academy/knowledgebase/how-to-make-an-internal-audit-checklist-for-iso-27001-iso-22301/#section4

Pensez à suivre cette formation gratuite en ligne :
ISO 27001 Internal Auditor Course
https://advisera.com/training/iso-27001-internal-auditor-course/

Par ailleurs, jetez un œil à ce livre :
ISO Internal Audit: A Plain English Guide
https://advisera.com/books/iso-internal-audit-lain-english-guide/

**Commented [AES5]:** Le système de codage des documents doit être aligné avec le système existant de l'organisation pour la codification des documents ; au cas où un tel système n'est pas en place, cette ligne peut être supprimée.

## Historique des modifications

| Date | Version | Créé par | Description de la modification |
|---|---|---|---|
| | 0.1 | Advisera | Structure documentaire de base |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Table des matières

## 1. But, domaine d'application et utilisateurs

Cette Procédure a pour but de décrire toutes les activités relatives à l'audit – rédaction du programme d'audit, sélection d'un auditeur, réalisation d'audits individuels et établissement de rapports.

Cette Procédure s'applique à toutes les activités réalisées au sein du Système de management de la sécurité de l'information (SMSI) [Système de management de la continuité des activités (SMCA)].

Les utilisateurs de ce document sont les [membres de la direction] de [nom de l'organisation], ainsi que les auditeurs internes.

**Commented [AES6]:** Ce doit être inséré à la place du SMSI dans le cas où la Procédure se réfère exclusivement au management de la continuité des activités.

**Commented [AES7]:** L'organe de direction dans le domaine d'application du SMSI/SMCA.

**Commented [AES8]:** Indiquez le nom de votre organisation.

## 2. Documents référencés

- Norme ISO/IEC 27001, clauses 9.2, A.5.30, A.5.35 et A.8.34
- Norme ISO 22301, clause 9.2
- Politique de sécurité de l'information
- Politique de continuité des activités
- Procédure relative à l'action corrective

**Commented [AES9]:** Effacer ceci si la Procédure se réfère uniquement au management de la continuité des activités.

**Commented [AES10]:** Effacer ceci si vous ne mettez pas en œuvre la continuité des activités.

**Commented [AES11]:** Effacer ceci si la Procédure se réfère uniquement au management de la continuité des activités.

**Commented [AES12]:** Effacer ceci si vous ne mettez pas en œuvre la continuité des activités.

**Commented [AES13]:** Vous pouvez consulter un modèle pour ce document dans le dossier "14_Actions_correctives" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

## 3. Audit interne

### 3.1. But de l'audit interne

Le but de l'audit interne est de déterminer si les procédures, les mesures, les processus, les dispositions et les autres activités au sein du SMSI [SMCA] sont conformes des normes ISO 27001 et ISO 22301, aux règlements applicables et à la documentation interne de l'organisation ; si ces éléments sont effectivement mis en œuvre et préservés, et s'ils respectent les exigences de la politique et les objectifs fixés.

L'audit interne est également utilisé pour évaluer de façon régulière la capacité des fournisseurs et partenaires essentiels, à assurer la continuité des activités.

**Commented [AES14]:** Effacer ceci si la Procédure se réfère

**Commented [AES15]:** Effacer ceci si vous ne mettez pas en

**Commented [AES16]:** Supprimer ce paragraphe si l'auditeur

### 3.2. Planification de l'audit interne

[Titre du poste] approuve un programme annuel d'audits internes, rédigé comme indiqué dans le formulaire de l'Annexe 1 – Programme annuel d'audit interne.

Un ou plusieurs audits internes doivent être réalisés au cours d'une année, afin d'assurer une couverture cumulée de la totalité du domaine d'application du SMSI [SMCA]. Les audits internes sont planifiés en fonction de l'évaluation des risques, ainsi que des résultats des audits précédents. Ils sont généralement menés avant la Revue de direction.

**Commented [AES17]:** Par ex. Responsable continuité d'activité,

Le Programme annuel d'audit interne doit comprendre les informations suivantes concernant chaque audit interne individuel :

- la durée de l'audit (préciser les dates ou le mois durant lequel l'audit est planifié)
- le domaine d'application de l'audit (services, processus, clauses de la norme, etc.)
- les critères de l'audit (normes, lois et règlements, documentation interne, normes de l'entreprise et / ou obligations contractuelles)
- [illegible]
- [illegible]

Commented [AES18]: Ces informations sont toutes [illegible]

Les auditeurs internes désignés doivent enregistrer les audits réalisés dans le Programme annuel d'audit interne.

### 3.3. Désignation des auditeurs internes

[Titre du poste] doit désigner des auditeurs internes.

Commented [AES19]: Par ex. Responsable sécurité, [illegible]

Un auditeur interne peut faire partie ou non de l'organisation. Les critères de désignation d'un auditeur interne sont :

Commented [AES20]: Il s'agit de critères conseillés pour la désignation d'auditeurs internes et conformes à la clause 7.2 de la norme ISO.

[illegible]

- la maîtrise des normes ISO/IEC 27001 et ISO 22301
- [illegible]
- [illegible]

Commented [AES21]: Effacer ceci si la Procédure se réfère [illegible]

Commented [AES22]: Effacer ceci si vous ne mettez pas en [illegible]

[Titre du poste] doit sélectionner les auditeurs internes en tenant compte de leur objectivité et de leur impartialité, pour éviter les conflits d'intérêts, parce que les auditeurs ne sont pas autorisés à évaluer leur propre travail.

Commented [AES23]: Par ex. Responsable sécurité, [illegible]

[illegible]

Commented [AES24]: Ou ISO 22301

### 3.4. Réalisation d'audits internes individuels

Commented [AES25]: Pour apprendre à réaliser des audits efficaces, consultez cet article :

[illegible]

Les personnes responsables des audits internes individuels sont indiquées dans le Programme annuel d'audit interne. Si un audit est mené par une équipe constituée de plusieurs auditeurs, la personne responsable de l'audit est celle désignée comme le Chef de l'équipe d'audit.

Les éléments suivants doivent être pris en considération lors d'un audit interne :

- les critères fixés dans le Programme annuel d'audit interne
- les résultats des audits internes et externes précédents
- [illegible]
- [illegible]

Les éléments suivants doivent être consignés dans les résultats d'audit interne :

- Rapport d'audit interne – il doit être envoyé à [titre du poste]
- [illegible] comme exigé par la Procédure relative à l'action corrective.

Commented [AES26]: Par ex. Responsable continuité d'activité, [illegible]

Commented [AES27]: Vous pouvez consulter un modèle pour [illegible]

## 4. Gestion des enregistrements conservés sur la base de ce document

| *Nom de l'enregistrement* | *Lieu de conservation* | [illegible] | [illegible] | *Temps de rétention* |
|---|---|---|---|---|
| Programme annuel d'audit interne (sous forme électronique) | Ordinateur de [titre du poste] | [illegible] | [illegible] | Les programmes sont conservés pendant une durée de 3 ans. |
| Rapport d'audit interne (sous forme électronique) | Ordinateurs de l'auditeur interne et de [titre du poste] | [illegible] | [illegible] | Les rapports sont conservés pendant une durée de 3 ans. |
| Liste de contrôle d'audit interne (formulaire rempli lors de l'audit interne) | Ordinateur de l'auditeur interne | [illegible] | [illegible] | La liste de contrôle est conservée pendant une durée de 3 ans. |

Commented [AES28]: Adaptez la durée dans cette colonne à [illegible]

Commented [AES29]: Habituellement la personne qui [illegible]

Commented [AES30]: Habituellement au format PDF.

Commented [AES31]: Habituellement au format PDF.

Seul [titre du poste] peut accorder à d'autres employés le droit d'accès au Programme annuel d'audit interne, au Rapport d'audit interne et à la Liste de contrôle d'audit interne.

## 5. Validité et gestion documentaire

Ce document est valide à compter du [date].

Le propriétaire de ce document est [titre du poste], qui doit vérifier et, si nécessaire, mettre à jour le document au moins [illegible].

Commented [AES32]: Par ex. Responsable continuité d'activité, [illegible]

Commented [AES33]: Il ne s'agit que d'une recommandation ; [illegible]

Lors de l'évaluation de l'efficacité et de la pertinence de ce document, les critères suivants doivent être considérés :

- le nombre d'actions correctives identifiées lors de l'audit
- le nombre d'actions correctives identifiées lors de l'audit de certification mené après l'audit interne
- si la fréquence des audits internes est conforme au Programme annuel d'audit interne

## 6. Annexes

- Annexe 1 – Programme annuel d'audit interne
- Annexe 2 – Rapport d'audit interne
- Annexe 3 – Liste de contrôle d'audit interne

[titre du poste]
[nom]

[signature]

**Commented [AES34]:** Nécessaire uniquement si la Procédure pour le contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.