DAVIDSON

Audit de la sécurité de l'information

DAVIDSON CONSULTING

Mars 2021

Document INTERNE

DAVIDSON

CONSULTING

Classification	Interne	
Référence	SMSI 010 DAV	
Version	V2.1	
	Nom Prénom	**Fonction**
Vérifié par	Fabrice GIORDAN	Responsable ARES et co-responsable du SMSI
Rédigé par	Antoine TOUPET	Consultant sécurité
Historique des mises à jour		
Date	**Modifié par**	**Description du changement**
19/03/2021	Nicolas MANDILLE	Revue Annuelle
30/10/2018	Rafik CHABANE	Ajustement suite à audit interne
07/11/2017	Fabrice GIORDAN	Mise à jour suite au décalage de l'Audit et rajout de la politique de correction
02/06/2017	Antoine TOUPET	Revue et ajustement du document.
31/05/2017	Loïs SAMAIN	Mise à jour du nommage et revue des audits prévues
14/09/2016	Loïs SAMAIN	Création du document

Documents de référence	
Référence	**Nom du document**
ISO/CEI 27001:2013	Système de Management de la Sécurité de l'Information - Exigences
[SMSI 001 DAV]	Politique Générale de la Sécurité de l'Information
[SMSI 002 DAV]	Périmètre du SMSI
[SEC 0103 DAV]	Politique de classification de l'information

SOMMAIRE

Contexte

Cette procédure a pour objet de définir l'organisation, la planification, la réalisation et le suivi des audits sécurités couvrant l'ensemble des activités du Système de Management de la Sécurité d'information (SMSI) de Davidson consulting.

Finalité et champ d'application

Le but des dispositions prévues dans la présente procédure est d'assurer :

- Une surveillance efficace du SMSI, en particulier vérifier :
  - Sa conformité à la norme ISO 27001
  - Sa mise en œuvre effective
  - Son efficacité
  - Son évolution / amélioration,
- La correction des écarts et/ou l'amélioration du SMSI identifiés lors des audits,
- L'information pertinente à la Direction des résultats de cette surveillance et des actions de corrections et/ ou d'amélioration engagées.

On notera que les dispositions contenues dans cette procédure s'appliquent à tous les audits réalisés dans le cadre du Système de Management de la Sécurité de l'Information.

Terminologies

Audit : Processus méthodique indépendant et documenté permettant d'obtenir des preuves et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits.

Programme d'audit : Ensemble d'un ou plusieurs audits planifiés dans un laps de temps et dans un but déterminé.

Périmètre d'audit : peut-être exprimé en termes de facteurs tels qu'un emplacement géographique, unité organisationnelle, activité ou processus.

Critères d'audit : Ensemble de processus ou exigences auquel les preuves d'audit sont comparées.

Dans le cadre du SMSI les critères d'audit correspondent aux chapitres de la norme ISO27001:2013.

Preuve d'audit : Enregistrement, déclaration de faits ou autres informations vérifiés, pertinent pour l'audit.

Constatation d'audit : Résultat de l'évaluation des preuves d'audit.

Qualification : Association des qualités personnelles, du niveau d'études minimal de formation, de l'expérience des audits, de l'expérience professionnelle et des compétences que possède un auditeur.

Responsabilités

Les audits sont réalisés sous la responsabilité du RSSI.

Les auditeurs sont indépendants des personnes qui ont la responsabilité directe de l'activité auditée.

Les responsables des activités auditées ont la responsabilité d'engager les actions correctives et/ou d'amélioration identifiées.

Qualification des auditeurs

Les audits sont réalisés soit par des auditeurs internes, soit par un auditeur externe à l'entreprise.

Les auditeurs sont qualifiés par le RSSI sur la base des exigences ci-après :

- Niveau d'instruction minimum : bac+5
- Formation à l'ISO 27001
- Aptitude à la communication écrite et orale
- Expérience : 2 années dans la société (pour les audits internes)

Il est du ressort du RSSI de valider les auditeurs internes à partir des éléments ci-dessus.

Pour un auditeur externe, il sera déterminé par le RSSI selon le dossier justificatif de qualification fourni par le prestataire (CV, références, qualifications obtenues).

Planification des audits

Les audits sont planifiés annuellement par le RSSI à l'issue de la revue de Direction.

L'ensemble du SMSI doit être audité dans une période de 12 mois.

De plus, des audits supplémentaires peuvent également être planifiés si nécessaire suite à des incidents majeurs ou un changement de périmètre du SMSI.

Programme d'audit

Le programme d'audit de l'année n + 1 est validé en réunion de revue de Direction prévue à la fin de chaque année (n), il porte sur des audits internes, externes, technique, et organisationnel.

Année n +1	
S1	**S2**
Test d'intrusion / Scans / Audit ISO27001 interne	Scans / Audit ISO27001 externe

Processus d'audits

Déclenchement des audits - désignation des auditeurs

Les audits sécurité sont déclenchés par le RSSI sur la base du planning défini au chapitre précédent.

Il est de la responsabilité du RSSI de désigner les auditeurs, en fonction :

- de la difficulté de l'audit (complexité, personnalité des audités etc.…)
- des aptitudes des auditeurs.

L'auditeur est désigné au moins 2 mois avant l'audit pour lui permettre de préparer sa mission.

Préparation de l'audit

Préparation par l'auditeur interne

L'auditeur est tenu

a) De préparer / constituer son guide d'audit (questionnaire) :
- Documents du SMSI couvrant le périmètre audité : politique, objectifs sécurité, procédures, etc…
- Chapitre (sous chapitre) de la norme ISO 27001

b) D'examiner le rapport précédent et notamment la clôture des plans d'action
c) De préparer les questions principales qu'il envisage de poser en audit
d) D'établir le plan d'audit.

Le plan d'audit doit être communiqué à l'audité à l'avance.

Préparation par l'auditeur externe

Afin de lui permettre de préparer sa mission, le RSSI transmet à l'auditeur les éléments nécessaires tels que politique et objectifs, manuel et procédures.

Déroulement de l'audit

L'audit doit toujours commencer par une réunion d'ouverture et se terminer par une réunion de clôture, pour faire le bilan "à chaud" avec les audités.

Durant l'audit, l'auditeur est tenu de relever précisément les écarts constatés et de les présenter au personnel audité, afin d'éviter toute discussion ultérieure.

Rapport d'audit

Rapport réalisé par un auditeur de la Société

Chaque non-conformité fait l'objet d'un rapport rédigé par l'auditeur et soumis à l'approbation du RSSI avant diffusion à la Direction.

Rapport rédigé par un auditeur externe :

La forme du rapport est laissée à l'initiative de l'auditeur.

Actions correctives / amélioration

A la réception du rapport d'audit, le responsable de l'entité concerné doit définir les actions qu'il souhaite entreprendre (actions correctives et /ou d'amélioration).

Pour cela, il est tenu de remplir la partie concernée de la fiche de non-conformité ou de remarque.

La fiche est alors soumise au RSSI pour approbation, avant de l'adresser au responsable concerné pour application.

Suivi des actions correctives / amélioration

Le RSSI est chargé de classer les actions afin de les prioriser, et pour effectuer les relances, si nécessaire.

Le tableau ci-dessous indique les démarches à mener :

Anomalies	Actions
Anomalie critiques	Correction prioritaire obligatoire. Délai max = 1 mois.
Anomalie majeures	Correction si - 0 anomalies critiques - Compatible avec charge projets
Anomalie mineures	Correction par opportunité

Clôture des rapports d'audit

Il est du ressort du RSSI de vérifier l'efficacité des actions prévues aux échéances convenues. Il devra formaliser cette vérification (si satisfaisante).

Lorsque toutes les actions sont clôturées, le rapport d'audit est considéré comme clôturé.

Enregistrement

Les documents ci-après sont conservés par le RSSI selon les modalités de la politique de classification de l'information de Davidson consulting :

- Les attestations des auditeurs (ainsi que les documents associés : diplômes, attestation de stage etc.…), qu'il s'agisse d'un auditeur interne ou d'un auditeur externe,
- Les rapports d'audit clôturés (avec leur questionnaire).
- Les plannings d'audits internes.

Ce présent document doit être pris en compte au sein de Davidson consulting

Pour toute réclamation ou remarque, veuillez contacter securite@davidson.fr.