

Boîte à outils de documentation ISO 27001

<https://advisera.com/27001academy/fr/boite-a-outils-de-documentation-iso-27001/>

Remarque : La documentation doit de préférence être mise en œuvre suivant l'ordre dans lequel les documents sont ici énumérés. L'ordre d'implémentation de la documentation relative à l'Annexe A est défini dans le Plan de traitement des risques.

N.	Code du document	Nom du document	Clauses correspondantes au sein de la norme ISO 27001	Obligatoire conformément à la norme ISO 27001
	01	Gestion des documents		
1	01	Procédure pour le contrôle des documents et enregistrements	7.5 ; A.5.33	
	02	Préparatifs du projet		
2	02	Plan de projet		
	03	Identification des exigences		
3	03	Procédure pour l'identification des exigences	4.2 ; A.5.31	
4	03.1	Annexe 1 – Liste des exigences légales, réglementaires, contractuelles et autres	4.2 ; A.5.29 ; A.5.31	✓ *
	04	Domaine d'application du SMSI		
5	04	Document du domaine d'application du SMSI	4.3	✓
	05	Politiques générales		
6	05	Politique de sécurité de l'information	5.2 ; 5.3** ; 6.2 ; 7.4 ; A.6.3	✓
	06	Evaluation et traitement des risques		
7	06	Méthodologie d'évaluation et de traitement des risques	6.1.2 ; 6.1.3 ; 8.2 ; 8.3	✓

N.	Code du document	Nom du document	Clauses correspondantes au sein de la norme ISO 27001	Obligatoire conformément à la norme ISO 27001
8	06.1	Annexe 1 – Tableau d'évaluation des risques	6.1.2 ; 8.2	✓
9	06.2	Annexe 2 – Tableau de traitement des risques	6.1.3 ; 8.3	✓
10	06.3	Annexe 3 – Rapport d'évaluation et de traitement des risques	8.2 ; 8.3	✓
	07	Applicabilité des mesures		
11	07	Déclaration d'applicabilité	6.1.3 d)	✓
	08	Plan d'implémentation		
12	08	Plan de traitement des risques	6.1.3 ; 6.2 ; 7.1 ; 8.3 ; 9.1	✓
	09	Annexe A – Mesures de sécurité		
13	09.01	Politique de sécurité des technologies de l'information	A.5.9 ; A.5.10 ; A.5.11 ; A.5.14 ; A.5.17 ; A.5.32 ; A.6.7 ; A.7.7 ; A.7.9 ; A.7.10 ; A.8.1 ; A.8.7 ; A.8.10 ; A.8.12 ; A.8.13 ; A.8.19 ; A.8.23	✓ *
14	09.02	Politique du bureau propre et de l'écran vide (Remarque : Elle peut être mise en œuvre dans le cadre de la Politique de sécurité des technologies de l'information.)	A.7.7 ; A.8.1	
15	09.03	Politique relative aux appareils mobiles, au télétravail et au travail à distance (Remarque : Elle peut être mise en œuvre dans le cadre de la Politique de sécurité des technologies de l'information.)	A.6.7 ; A.7.9 ; A.8.1	

N.	Code du document	Nom du document	Clauses correspondantes au sein de la norme ISO 27001	Obligatoire conformément à la norme ISO 27001
16	09.04	Politique Bring Your Own Device (BYOD)	A.5.14 ; A.6.7 ; A.8.1	
17	09.05	Procédures relatives au travail dans les zones sécurisées	A.7.4 ; A.7.6	
18	09.06	Politique de classification des informations	A.5.9 ; A.5.10 ; A.5.12 ; A.5.13 ; A.5.14 ; A.7.10 ; A.8.3 ; A.8.5 ; A.8.11 ; A.8.12	✓ *
19	09.07	Inventaire des actifs	A.5.9	✓
20	09.08	Procédures de sécurité pour le service des technologies de l'information	A.5.7 ; A.5.14 ; A.5.37 ; A.7.10 ; A.7.14 ; A.8.4 ; A.8.6 ; A.8.7 ; A.8.8 ; A.8.9 ; A.8.10 ; A.8.12 ; A.8.13 ; A.8.15 ; A.8.16 ; A.8.17 ; A.8.18 ; A.8.20 ; A.8.21 ; A.8.22 ; A.8.23 ; A.8.31 ; A.8.32	✓ *
21	09.09	Politique de gestion du changement (Remarque : Elle peut être mise en œuvre dans le cadre des Procédures de sécurité pour le service des technologies de l'information.)	A.8.32	
22	09.10	Politique de sauvegarde (Remarque : Elle peut être mise en œuvre dans le cadre des Procédures de sécurité pour le service des technologies de l'information.)	A.8.13	

N.	Code du document	Nom du document	Clauses correspondantes au sein de la norme ISO 27001	Obligatoire conformément à la norme ISO 27001
23	09.11	Politique de transfert des informations (Remarque : Elle peut être mise en œuvre dans le cadre des Procédures de sécurité pour le service des technologies de l'information.)	A.5.14	
24	09.12	Politique d'élimination et de destruction (Remarque : Elle peut être mise en œuvre dans le cadre des Procédures de sécurité pour le service des technologies de l'information.)	A.7.10 ; A.7.14 ; A.8.10	
25	09.13	Politique sur l'utilisation du cryptage	A.5.31 ; A.8.24	
26	09.14	Politique de contrôle d'accès	A.5.15 ; A.5.16 ; A.5.17 ; A.5.18 ; A.8.2 ; A.8.3 ; A.8.4 ; A.8.5 ; A.8.11	
27	09.15	Politique des mots de passe (Remarque : Elle peut être mise en œuvre dans le cadre de la Politique de contrôle d'accès.)	A.5.16 ; A.5.17 ; A.5.18	
28	09.16	Politique de développement sécurisé	A.5.33 ; A.8.11 ; A.8.25 ; A.8.26 ; A.8.27 ; A.8.28 ; A.8.29 ; A.8.30 ; A.8.31 ; A.8.32 ; A.8.33	✓ *
29	09.17	Annexe 1 – Spécification des exigences relatives aux systèmes d'information	A.8.26	

N.	Code du document	Nom du document	Clauses correspondantes au sein de la norme ISO 27001	Obligatoire conformément à la norme ISO 27001
30	09.18	Politique de sécurité des fournisseurs	A.5.7 ; A.5.11 ; A.5.19 ; A.5.20 ; A.5.21 ; A.5.22 ; A.5.23 ; A.6.1 ; A.6.2 ; A.6.3 ; A.8.30	
31	09.19	Clauses de sécurité relatives aux fournisseurs et aux partenaires	A.5.20 ; A.5.21 ; A.6.2 ; A.6.6 ; A.8.30	
32	09.20	Procédure de gestion des incidents	7.4 ; A.5.7 ; A.5.24 ; A.5.25 ; A.5.26 ; A.5.27 ; A.5.28 ; A.6.4 ; A.6.8	✓ *
33	09.21	Annexe 1 – Journal des incidents	A.5.27	
34	09.22	Plan de reprise en cas de désastre	7.4 ; A.5.29 ; A.5.30 ; A.8.14	
35	09.23	Déclaration de confidentialité	A.5.20 ; A.6.2 ; A.6.5 ; A.6.6	✓ *
36	09.24	Déclaration d'acceptation des documents du SMSI	A.6.2	
	10	Formation et sensibilisation		
37	10	Plan de formation et de sensibilisation	7.2 ; 7.3 ; 7.4 ; A.6.3	✓
	11	Audit interne		
38	11	Procédure d'audit interne	9.2 ; A.5.30 ; A.5.35 ; A.8.34	
39	11.1	Annexe 1 – Programme annuel d'audit interne	9.2	✓
40	11.2	Annexe 2 – Rapport d'audit interne	9.2	✓

<i>N.</i>	<i>Code du document</i>	<i>Nom du document</i>	<i>Clauses correspondantes au sein de la norme ISO 27001</i>	<i>Obligatoire conformément à la norme ISO 27001</i>
41	11.3	Annexe 3 – Liste de contrôle d’audit interne	9.2	
	12	Revue de direction		
42	12.1	Rapport de mesure	6.2 ; 9.1	✓
43	12.1	Comptes-rendus de Revue de direction	9.3	✓
	13	Actions correctives		
44	13	Procédure relative à l’action corrective	10.1 ; A.5.27	
45	13.1	Annexe 1 – Formulaire d’action corrective	10.1 ; 10.2	✓

*Les documents énumérés sont uniquement obligatoires si les mesures correspondantes sont jugées applicables dans la Déclaration d’applicabilité.

**Les fonctions et les responsabilités générales sont décrites dans la Politique de sécurité de l’information, alors que les fonctions et les responsabilités détaillées sont décrites dans chaque document de cette Boîte à outils.