Boîte à outils ISO 27001 et ISO 22301 Premium

https://advisera.com/27001academy/fr/boite-a-outils-iso-27001-iso-22301-premium/

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*	*Obligatoire conformément à la norme ISO 27001*	*Obligatoire conformément à la norme ISO 22301*
	01	**Gestion des documents**			
1	01	Procédure pour le contrôle des documents et enregistrements	ISO 27001 7.5 ; A.5.33 ISO 22301 7.5		
	02	**Préparatifs du projet**			
2	02	Plan de projet			
	03	**Identification des exigences**			
3	03	Procédure pour l'identification des exigences	ISO 27001 4.2 ; A.5.31 ISO 22301 4.2		
4	03.1	Annexe 1 – Liste des exigences légales, réglementaires, contractuelles et autres	ISO 27001 4.2 ; A.5.29 ; A.5.31 ISO 22301 4.2	✓*	✓
	04	**Domaine d'application du SMSI**			
5	04	Document du domaine d'application du SMSI	ISO 27001 4.3	✓	
	05	**Politiques générales**			
6	05	Politique de sécurité de l'information	ISO 27001 5.2 ; 5.3** ; 6.2 ; 7.4 ; A.6.3	✓	

N.	*Code du document*	*Nom du document*	*Clauses correspondantes au sein de la norme*	*Obligatoire conformément à la norme ISO 27001*	*Obligatoire conformément à la norme ISO 22301*
	06	**Evaluation et traitement des risques**			
7	06	Méthodologie d'évaluation et de traitement des risques	ISO 27001 6.1.2 ; 6.1.3 ; 8.2 ; 8.3 ISO 22301 8.2.1 ; 8.2.3	✓	
8	06.1	Annexe 1 – Tableau d'évaluation des risques	ISO 27001 6.1.2 ; 8.2 ISO 22301 8.2.3	✓	
9	06.2	Annexe 2 – Tableau de traitement des risques	ISO 27001 6.1.3 ; 8.3 ISO 22301 8.2.3	✓	
10	06.3	Annexe 3 – Rapport d'évaluation et de traitement des risques	ISO 27001 8.2 ; 8.3 ISO 22301 8.2.3	✓	
	07	**Applicabilité des mesures**			
11	07	Déclaration d'applicabilité	ISO 27001 6.1.3 d)	✓	
	08	**Plan d'implémentation**			
12	08	Plan de traitement des risques	ISO 27001 6.1.3 ; 6.2 ; 7.1 ; 8.3 ; 9.1	✓	
	09	**Annexe A de la norme ISO 27001 – Mesures de sécurité**			

N.	Code du document	Nom du document	Clauses correspondantes au sein de la norme	Obligatoire conformément à la norme ISO 27001	Obligatoire conformément à la norme ISO 22301
13	09.01	Politique de sécurité des technologies de l'information	ISO 27001 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.)	ISO 27001 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.)	ISO 27001 A.6.7 ; A.7.9 ; A.8.1		
16	09.04	Politique Bring Your Own Device (BYOD)	ISO 27001 A.5.14 ; A.6.7 ; A.8.1		
17	09.05	Procédures relatives au travail dans les zones sécurisées	ISO 27001 A.7.4 ; A.7.6		

N.	*Code du document*	*Nom du document*	*Clauses correspondantes au sein de la norme*	*Obligatoire conformément à la norme ISO 27001*	*Obligatoire conformément à la norme ISO 22301*
18	09.06	Politique de classification des informations	ISO 27001 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	ISO 27001 A.5.9	✔*	
20	09.08	Procédures de sécurité pour le service des technologies de l'information	ISO 27001 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.)	ISO 27001 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.)	ISO 27001 A.8.13		

N.	Code du document	Nom du document	Clauses correspondantes au sein de la norme	Obligatoire conformément à la norme ISO 27001	Obligatoire conformément à la norme ISO 22301
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.)	ISO 27001 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.)	ISO 27001 A.7.10 ; A.7.14 ; A.8.10		
25	09.13	Politique sur l'utilisation du cryptage	ISO 27001 A.5.31 ; A.8.24		
26	09.14	Politique de contrôle d'accès	ISO 27001 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.)	ISO 27001 A.5.16 ; A.5.17 ; A.5.18		

N.	*Code du document*	*Nom du document*	*Clauses correspondantes au sein de la norme*	*Obligatoire conformément à la norme ISO 27001*	*Obligatoire conformément à la norme ISO 22301*
28	09.16	Politique de développement sécurisé	ISO 27001 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	ISO 27001 A.8.26		
30	09.18	Politique de sécurité des fournisseurs	ISO 27001 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	ISO 27001 A.5.20 ; A.5.21 ; A.6.2 ; A.6.6 ; A.8.30		
32	09.20	Procédure de gestion des incidents	ISO 27001 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	ISO 27001 A.5.27		
34	09.22	Déclaration de confidentialité	ISO 27001 A.5.20 ; A.6.2 ; A.6.5 ; A.6.6	✔*	
35	09.23	Déclaration d'acceptation des documents du SMSI	ISO 27001 A.6.2		

N.	*Code du document*	*Nom du document*	*Clauses correspondantes au sein de la norme*	*Obligatoire conformément à la norme ISO 27001*	*Obligatoire conformément à la norme ISO 22301*
	10	**Documents fondamentaux sur la continuité des activités ISO 22301**			
36	10.01	Politique de continuité des activités	ISO 22301 4.1 ; 4.3 ; 5.2 ; 5.3 ; 6.2 ; 6.3 ; 9.1.1 ISO 27001 A.5.29		✓
37	10.02	Méthodologie du Bilan d'impact sur les activités	ISO 22301 8.2.1 ; 8.2.2 ISO 27001 A.5.29		
38	10.03	Annexe 1 – Questionnaire de Bilan d'impacts sur les activités	ISO 22301 8.2.1 ; 8.2.2 ISO 27001 A.5.29		
39	10.04	Stratégie de continuité des activités	ISO 22301 8.3, 8.4.2 ISO 27001 A.5.5 ; A.5.29		
40	10.05	Annexe 1 – Objectifs de temps de reprises pour les activités	ISO 22301 8.2.2 ISO 27001 A.5.29		
41	10.06	Annexe 2 – Exemples de scénarios d'incidents perturbateurs	ISO 22301 8.5 ISO 27001 A.5.29		
42	10.07	Annexe 3 – Plan de préparation pour la continuité des activités	ISO 22301 6.2		

N.	Code du document	Nom du document	Clauses correspondantes au sein de la norme	Obligatoire conformément à la norme ISO 27001	Obligatoire conformément à la norme ISO 22301
43	10.08	Annexe 4 – Stratégie de reprise des activités	ISO 22301 8.3 ISO 27001 A.5.29		
44	10.09	Plan de continuité des activités	ISO 22301 8.4 ISO 27001 A.5.29		✓
45	10.10	Annexe 1 – Plan de réponse aux incidents	ISO 22301 8.4.3 ; 8.4.4 ISO 27001 A.5.5 ; A.5.26 ; A.5.29		✓
46	10.11	Annexe 2 – Journal des incidents	ISO 22301 8.4.3		✓
47	10.12	Annexe 3 – Liste des sites de continuité des activités	ISO 22301 8.4.4 ISO 27001 A.5.29		✓
48	10.13	Annexe 4 – Plan de transport	ISO 22301 8.3.2 ISO 27001 A.5.29		
49	10.14	Annexe 5 – Contacts clés	ISO 22301 8.4.3 ISO 27001 A.5.29		✓
50	10.15	Annexe 6 – Plan de reprise en cas de désastre	ISO 22301 8.4.5 ISO 27001 7.4 ; A.5.29 ; A.5.30 ; A.8.14	✓*	✓

N.	*Code du document*	*Nom du document*	*Clauses correspondantes au sein de la norme*	*Obligatoire conformément à la norme ISO 27001*	*Obligatoire conformément à la norme ISO 22301*
51	10.16	Annexe 7 – Plan de reprise des activités	ISO 22301 8.4.5 ISO 27001 A.5.29		✓
52	10.17	Plan d'exercice et de tests	ISO 22301 8.5 ISO 27001 A.5.29		
53	10.18	Annexe 1 – Rapport d'exercice et de tests	ISO 22301 8.5 ISO 27001 A.5.29		
54	10.19	Plan de maintenance et de revue du SMCA	ISO 22301 8.6 ISO 27001 A.5.29		
55	10.20	Formulaire de revue post-incident	ISO 22301 8.6 ISO 27001 A.5.27 ; A.5.29		
	11	**Formation et sensibilisation**			
56	11	Plan de formation et de sensibilisation	ISO 27001 7.2 ; 7.3 ; 7.4 ; A.6.3 ISO 22301 7.2 ; 7.3	✓	✓
	12	**Audit interne**			
57	12	Procédure d'audit interne	ISO 27001 9.2 ; A.5.30 ; A.5.35 ; A.8.34 ISO 22301 9.2		

N.	*Code du document*	*Nom du document*	*Clauses correspondantes au sein de la norme*	*Obligatoire conformément à la norme ISO 27001*	*Obligatoire conformément à la norme ISO 22301*
58	12.1	Annexe 1 – Programme annuel d'audit interne	ISO 27001 9.2 ISO 22301 9.2	✓	✓
59	12.2	Annexe 2 – Rapport d'audit interne	ISO 27001 9.2 ISO 22301 9.2	✓	✓
60	12.3	Annexe 3 – Liste de contrôle d'audit interne	ISO 27001 9.2 ISO 22301 9.2		
	13	**Revue de direction**			
61	13.1	Rapport de mesure	ISO 27001 6.2 ; 9.1 ISO 22301 9.1 ; 9.3	✓	
62	13.2	Comptes-rendus de Revue de direction	ISO 27001 9.3 ISO 22301 9.3	✓	✓
	14	**Actions correctives**			
63	14	Procédure relative à l'action corrective	ISO 27001 10.1 ; A.5.27 ISO 22301 10.1		
64	14.1	Annexe 1 – Formulaire d'action corrective	ISO 27001 10.1 ; 10.2 ISO 22301 10.1	✓	✓

*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.