

Boîte à outils documentaire Premium ISO 27001 & ISO 22301

<http://advisera.com/27001academy/fr/boite-a-outils-iso-27001-iso-22301-premium/>

Remarque: La documentation devrait de préférence être mise en œuvre dans l'ordre dans lequel elle est listée ici. L'ordre de mise en œuvre de la documentation relative à l'annexe A est défini dans le plan de traitement des risques. La documentation de gestion de la continuité des activités (No 8. A.17 dans le paquet) est mise en œuvre dans l'ordre dans lequel elle est listée ici.


Veillez noter que certains documents dans cette boîte à outils ne sont pas obligatoires - en fonction de la taille et de la complexité de votre entreprise, vous pouvez choisir de les mettre en œuvre ou non.

Numéro dans le paquet	Nom du document	Clause correspondante dans la norme	Obligatoire selon ISO 27001	Obligatoire selon ISO 22301	Obligatoire selon BS 25999-2
0.	Procédure pour le contrôle des documents et enregistrements	ISO/IEC 27001 7.5 ISO 22301 7.5 BS 25999-2 3.4.2, 3.4.3			✓
1.	Plan de projet				
2.	Procédure pour l'identification des exigences	ISO/IEC 27001 4.2 et A.18.1.1 ISO 22301 4.2			
2.1.	Annexe – Liste des exigences légales, réglementaires, contractuelles et autres	ISO/IEC 27001 4.2 et A.18.1.1 ISO 22301 4.2	✓*	✓	
3.	Document du domaine d'application du SMSI	ISO/IEC 27001 4.3	✓		
4.	Politique de sécurité de l'information	ISO/IEC 27001 5.2 et 5.3	✓		

<i>Numéro dans le paquet</i>	<i>Nom du document</i>	<i>Clause correspondante dans la norme</i>	<i>Obligatoire selon ISO 27001</i>	<i>Obligatoire selon ISO 22301</i>	<i>Obligatoire selon BS 25999-2</i>
5.	Méthodologie d'évaluation et de traitement des risques	ISO/IEC 27001 6.1.2, 6.1.3, 8.2, et 8.3 ISO 22301 8.2.1, 8.2.3 BS 25999-2 4.1.2.1	✓	✓	✓
5.1.	Annexe 1 – Tableau d'évaluation des risques	ISO/IEC 27001 6.1.2 et 8.2 ISO 22301 8.2.3 BS 25999-2 4.1.2	✓		
5.2.	Annexe 2 – Tableau de traitement des risques	ISO/IEC 27001 6.1.3 et 8.3 ISO 22301 8.3.3 BS 25999-2 4.1.3.1	✓		
5.3.	Annexe 3 – Rapport d'évaluation et de traitement des risques	ISO/IEC 27001 8.2 et 8.3	✓		
6.	Déclaration d'applicabilité	ISO/IEC 27001 6.1.3 d)	✓		
7.	Plan de traitement des risques	ISO/IEC 27001 6.1.3, 6.2 et 8.3	✓		
8.	(Annexe A – Mesures)				
8. A.6	Politique Bring Your Own Device (BYOD)	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.13.2.1			
8. A.6	Politique relative aux terminaux mobiles et au télétravail	ISO/IEC 27001 A.6.2 A.11.2.6			

<i>Numéro dans le paquet</i>	<i>Nom du document</i>	<i>Clause correspondante dans la norme</i>	<i>Obligatoire selon ISO 27001</i>	<i>Obligatoire selon ISO 22301</i>	<i>Obligatoire selon BS 25999-2</i>
8. A.7	Déclaration de confidentialité	ISO/IEC 27001 A.7.1.2, A.13.2.4, A.15.1.2	✓*		
8. A.7	Déclaration d'acceptation des documents du SMSI	ISO/IEC 27001 A.7.1.2	✓*		
8. A.8	Inventaire des actifs	ISO/IEC 27001 A.8.1.1, A.8.1.2	✓*		
8. A.8	Politique d'utilisation acceptable	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2	✓*		
8. A.8	Politique de classification des informations	ISO/IEC 27001 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3			
8. A.9	Politique de contrôle des accès	ISO/IEC 27001 A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3	✓*		

<i>Numéro dans le paquet</i>	<i>Nom du document</i>	<i>Clause correspondante dans la norme</i>	<i>Obligatoire selon ISO 27001</i>	<i>Obligatoire selon ISO 22301</i>	<i>Obligatoire selon BS 25999-2</i>
8. A.9	Politique relative aux mots de passe (Remarque: peut être implémentée comme partie de la politique de contrôle des accès)	ISO/IEC 27001 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3			
8. A.10	Politique sur l'utilisation des mesures cryptographiques	ISO/IEC 27001 A.10.1.1, A.10.1.2, A.18.1.5			
8. A.11	Politique de bureau propre et d'écran vide (Remarque: peut être implémentée comme partie de la politique d'utilisation acceptable)	ISO/IEC 27001 A.11.2.8, A.11.2.9			
8. A.11	Politique d'élimination et de destruction (Remarque: peut être implémentée comme partie des procédures opérationnelles des TIC)	ISO/IEC 27001 A.8.3.2, A.11.2.7			
8. A.11	Procédures relatives au travail dans les zones sécurisées	ISO/IEC 27001 A.11.1.5			

<i>Numéro dans le paquet</i>	<i>Nom du document</i>	<i>Clause correspondante dans la norme</i>	<i>Obligatoire selon ISO 27001</i>	<i>Obligatoire selon ISO 22301</i>	<i>Obligatoire selon BS 25999-2</i>
8. A.12	Procédures opérationnelles pour les technologies de l'information et des communications	ISO/IEC 27001 A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4	 *		
8. A.12	Politique de gestion des changements (Remarque: peut être implémentée comme parties des procédures opérationnelles des TIC)	ISO/IEC 27001 A.12.1.2, A.14.2.4			
8. A.12	Politique de sauvegarde (Remarque: peut être implémentée comme parties des procédures opérationnelles des TIC)	ISO/IEC 27001 A.12.3.1			
8. A.13	Politique de transfert des informations (Remarque: peut être implémentée comme parties des procédures opérationnelles des TIC)	ISO/IEC 27001 A.13.2.1, A.13.2.2			

Numéro dans le paquet	Nom du document	Clause correspondante dans la norme	Obligatoire selon ISO 27001	Obligatoire selon ISO 22301	Obligatoire selon BS 25999-2
8. A.14	Politique de développement sécurisé	ISO/IEC A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1	✓*		
8. A.14	Annexe – Spécification des exigences relatives aux systèmes d'information	ISO/IEC 27001 A.14.1.1	✓*		
8. A.15	Politique de sécurité des fournisseurs	ISO/IEC 27001 A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2			
8. A.15	Annexe – Clauses de sécurité pour les fournisseurs et les partenaires	ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3	✓*		
8. A.16	Procédure de gestion des incidents	ISO/IEC 27001 A.7.2.3, A.16.1.1, A.6.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7	✓*		
8. A.16	Annexe – Journal des incidents	ISO/IEC 27001 A.16.1.6			
8. A.17 1.	Politique de continuité des activités	ISO 22301 4.1, 4.3, 5.3, 6.2, 9.1.1 BS 25999-2 3.2.1, 3.2.2, 3.2.3 ISO/IEC 27001 A.17.1.1		✓	✓

Numéro dans le paquet	Nom du document	Clause correspondante dans la norme	Obligatoire selon ISO 27001	Obligatoire selon ISO 22301	Obligatoire selon BS 25999-2
8. A.17 2.	Méthodologie des bilans d'impact sur les activités	ISO 22301 8.2.1, 8.2.2 BS 25999-2 4.1.1 ISO/IEC 27001 A.17.1.1		✓	
8. A.17 2.1.	Questionnaire des bilans d'impacts sur les activités	ISO 22301 8.2.1, 8.2.2 BS 25999-2 4.1.1 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.	Stratégie de continuité des activités	ISO 22301 8.3, 8.4.2 BS 25999-2 4.2 ISO/IEC 27001 A.17.1.1, A.17.2.1		✓	✓
8. A.17 3.1.	Annexe 1 – Liste des activités	ISO 22301 8.2.2 BS 25999-2 4.1.1.2 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.2.	Annexe 2 – Priorités de reprises pour les activités	ISO 22301 8.2.2 BS 25999-2 4.1.1.2 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.3.	Annexe 3 – Objectifs de temps de reprises pour les activités	ISO 22301 8.2.2 BS 25999-2 4.1.1.2 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.4.	Annexe 4 – Exemples de scénarios d'incidents perturbateurs	ISO 22301 8.5 BS 25999-2 4.1.2.2 ISO/IEC 27001 A.17.1.1		✓	

Numéro dans le paquet	Nom du document	Clause correspondante dans la norme	Obligatoire selon ISO 27001	Obligatoire selon ISO 22301	Obligatoire selon BS 25999-2
8. A.17 3.5.	Annexe 5 – Plan de préparation pour la continuité des activités	ISO 22301 6.2 BS 25999-2 3.2.3.1		✓	✓
8. A.17 3.6.	Annexe 6 – Stratégie de reprise des activités	ISO 22301 8.3 BS 25999-2 4.2 ISO/IEC 27001 A.17.1.1, A.17.2.1		✓	✓
8. A.17 4.	Plan de continuité des activités	ISO 22301 8.4 BS 25999-2 4.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 4.1.	Annexe 1 – Plan de réponse aux incidents	ISO 22301 8.4.3, 8.4.4 BS 25999-2 4.3.2 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 4.2.	Annexe 2 – Journal des incidents	ISO 22301 8.4.3 BS 25999-2 4.3.2 ISO/IEC 27001 A.17.1.3		✓	✓
8. A.17 4.3.	Annexe 3 – Liste des sites de secours	ISO 22301 8.4.4 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 4.4.	Annexe 4 – Plan de transport	ISO 22301 8.3.2 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 4.5.	Annexe 5 – Contacts clés	ISO 22301 8.4.3 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓

Numéro dans le paquet	Nom du document	Clause correspondante dans la norme	Obligatoire selon ISO 27001	Obligatoire selon ISO 22301	Obligatoire selon BS 25999-2
8. A.17 4.6.	Annexe 6 – Plan de reprise en cas de désastre	ISO 22301 8.4.5 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2	✓*	✓	✓
8. A.17 4.7.	Annexe 7 – Plan de reprise des activités	ISO 22301 8.4.5 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 5.1.	Plan d'exercice et de tests	ISO 22301 8.5 BS 25999-2 4.4.2 ISO/IEC 27001 A.17.1.3			✓
8. A.17 5.2.	Annexe – Formulaire – Rapport d'exercice et de test	ISO 22301 8.5 BS 25999-2 4.4.2.2 ISO/IEC 27001 A.17.1.3		✓	✓
8. A.17 5.3.	Plan de maintenance et de revue du SMCA	ISO 22301 9.1.2 BS 25999-2 4.4.3 ISO/IEC 27001 A.17.1.3			✓
8. A.17 5.4.	Formulaire de revue post-incident	ISO 22301 9.1.2 BS 25999-2 4.4.3.4 ISO/IEC 27001 A.17.1.3, A.16.1.6		✓	✓
9.	Plan de formation et de sensibilisation	ISO 22301 7.2, 7.3 BS 25999-2 3.2.4, 3.3 ISO/IEC 27001 7.2, 7.3	✓	✓	✓
10.	Procédure d'audit interne	ISO/IEC 27001 clause 9.2 ISO 22301 9.2 BS 25999-2 5.1			✓

<i>Numéro dans le paquet</i>	<i>Nom du document</i>	<i>Clause correspondante dans la norme</i>	<i>Obligatoire selon ISO 27001</i>	<i>Obligatoire selon ISO 22301</i>	<i>Obligatoire selon BS 25999-2</i>
10.1.	Annexe 1 – Programme annuel d'audit interne	ISO/IEC 27001 clause 9.2 ISO 22301 9.2 BS 25999-2 5.1	✓	✓	✓
10.2.	Annexe 2 – Rapport d'audit interne	ISO/IEC 27001 clause 9.2 ISO 22301 9.2 BS 25999-2 5.1	✓	✓	✓
10.3.	Annexe 3 – Liste de contrôle d'audit interne	ISO/IEC 27001 clause 9.2 ISO 22301 clause 9.2			
11.	Comptes-rendus des revues de Direction	ISO/IEC 27001 clause 9.3 ISO 22301 9.3 BS 25999-2 5.2	✓	✓	✓
12.	Procédure pour les actions correctives	ISO/IEC 27001 clause 10.1 ISO 22301 10.1 BS 25999-2 6.1			✓
12.1.	Annexe – Formulaire d'actions correctives	ISO/IEC 27001 clause 10.1 ISO 22301 10.1 BS 25999-2 6.1	✓	✓	✓

* Les documents énumérés ne sont obligatoires que si les mesures correspondantes sont identifiées comme applicables dans la Déclaration d'applicabilité.

Pour apprendre à remplir ces documents, voir :

- 1) Notre série de tutoriels vidéo <http://advisera.com/27001academy/documentation-tutorials/>
- 2) Notre série de webinars <http://advisera.com/27001academy/webinars/>