LIVRE BLANC

ISO/IEC 27001:2022

Guide complet de mise en oeuvre du SMSI

Stratégies · Contrôles · Certification · Gouvernance

TRANSMUTE CONSULTING | 2025

TRANSMUTE
CONSULTING

TABLE DES MATIÈRES

01 Avant-propos — Pourquoi l'ISO 27001 maintenant ?

Dans un monde où les cyberattaques se multiplient, ou les obligations réglementaires s'intensifient (RGPD, NIS2, DORA), et ou la confiance numérique devient un avantage concurrentiel décisif, la certification ISO/IEC 27001 s'impose comme le standard international de référence pour la sécurité de l'information.

43 % des PME victimes d'une cyberattaque en 2023 (CESIN)	**4,45 M$** coût moyen d'une violation de données (IBM, 2023)	**70 %** de réduction des incidents pour les entreprises certifiées	**+33 %** de certifications ISO 27001 en 3 ans dans le monde

Ce livre blanc a été conçu par Transmute Consulting pour accompagner les directeurs, RSSI, responsables conformité et chefs de projet dans leur démarche de certification. Il constitue un guide de référence exhaustif, depuis la compréhension de la norme jusqu'à l'audit de certification.

02 Comprendre l'ISO/IEC 27001:2022

2.1 Historique et évolution de la norme

L'ISO/IEC 27001 est issue d'un long processus de maturation des pratiques de sécurité de l'information. Son histoire remonte aux travaux du gouvernement britannique dans les années 1990.

1995	BS 7799-1 — Publication de la norme britannique par le BSI sur les bonnes pratiques de sécurité.
1998	BS 7799-2 — Création de la partie "système de management" permettant la certification.
2000	ISO/IEC 17799 — Reconnaissance internationale de la BS 7799-1 par l'ISO.
2005	ISO/IEC 27001:2005 — Première version ISO de la norme de certification SMSI.
2013	ISO/IEC 27001:2013 — Refonte majeure avec adoption de la structure Annexe SL.
2022	ISO/IEC 27001:2022 — 11 nouveaux contrôles, 4 thèmes, attributs de contrôle.

2.2 Structure HLS (High Level Structure)

L'ISO 27001:2022 suit la structure HLS commune à toutes les normes ISO de systèmes de management. Cette harmonisation facilite l'intégration avec ISO 9001, ISO 14001, ISO 22301, etc.

Article	Titre	Contenu clé
4	Contexte de l'organisation	Enjeux internes/externes, parties prenantes, périmètre
5	Leadership	Engagement direction, politique SSI, rôles
6	Planification	Risques, opportunités, objectifs SSI
7	Support	Ressources, compétences, communication, documentation
8	Réalisation	Gestion des risques opérationnels, PTR
9	Evaluation des performances	Surveillance, mesures, audits internes, revue direction
10	Amélioration	Non-conformités, actions correctives, amélioration continue
Annexe A	93 Controles de securite	4 thèmes : Organisationnel, Humain, Physique, Technologique

2.3 Les principaux changements de la version 2022

Réorganisation de l'Annexe A	114 contrôles en 14 catégories → 93 contrôles en 4 thèmes (organisationnel, humain, physique, technologique)
11 nouveaux contrôles	Menaces physiques, sécurité cloud, threat intelligence, DLP, filtrage web, sécurité du code, etc.
Attributs de contrôle	Chaque contrôle dispose désormais d'attributs (propriété, capacité, domaine, concept, type) facilitant le filtrage.
Modifications textuelles	Clarifications dans les articles 4 à 10, notamment sur la planification des changements (article 6.3).
Suppression de doublons	Certains contrôles ont été fusionnés ou supprimés pour éliminer les redondances.

03 Le Système de Management de la Sécurité de l'Information (SMSI)

Un SMSI est un système de management qui, sur la base d'une analyse des risques, permet d'établir, de mettre en œuvre, d'exploiter, de surveiller, de réexaminer, de tenir à jour et d'améliorer la sécurité de l'information. Il repose sur le cycle PDCA (Plan-Do-Check-Act).

PLAN (Planifier)	DO (Faire)	CHECK (Vérifier)	ACT (Agir)
Analyse du contexte Évaluation des risques Objectifs SSI Plan de traitement	Mise en oeuvre des contrôles Formation Sensibilisation	Audits internes Mesure des KPI Revue de direction Conformité	Actions correctives Améliorations Mise à jour du SMSI

3.1 Périmètre et contexte (Article 4)

La définition du périmètre du SMSI est l'une des décisions les plus stratégiques du projet. Elle détermine quels actifs, processus, sites et entités organisationnelles sont couverts par la certification.

- **Contexte interne :** Contexte interne : structure organisationnelle, culture d'entreprise, systèmes d'information, obligations contractuelles.
- **Contexte externe :** Contexte externe : environnement réglementaire, concurrence, dépendances vis-à-vis de tiers, menaces cyber du secteur.
- **Parties intéressées :** Parties intéressées : clients, fournisseurs, actionnaires, autorités de régulation, partenaires.
- **Périmètre SMSI :** Périmètre SMSI : peut être un département, un site, une filiale ou l'ensemble de l'organisation.

3.2 Leadership et gouvernance (Article 5)

L'engagement de la direction est non négociable dans ISO 27001. La norme exige une implication directe et visible du plus haut niveau hiérarchique, non pas une simple délégation au RSSI.

3.3 Planification (Article 6)

- Article 6.1 : Actions face aux risques et opportunités.
- Article 6.2 : Objectifs de sécurité SMART (Spécifiques, Mesurables, Atteignables, Réalistes, Temporels).
- Article 6.3 (nouveau 2022) : Planification des changements significatifs du SMSI.

04 Gestion des risques selon l'ISO 27001:2022

La gestion des risques est le cœur du SMSI. L'ISO 27001 n'impose pas une méthode spécifique, mais exige un processus structuré, documenté et répétable. La norme ISO 27005:2022 fournit des lignes directrices de premier plan. En France, EBIOS Risk Manager est également très utilisé.

4.1 Méthodologie d'appréciation des risques

01	**Identification des actifs** Inventaire des actifs informationnels avec désignation d'un propriétaire pour chaque actif.
02	**Identification des menaces et vulnérabilités** Pour chaque actif : menaces applicables (cyberattaque, erreur humaine...) et vulnérabilités exploitables.
03	**Evaluation de la vraisemblance** Probabilité que la menace se matérialise (échelle 1 à 4 : Rare, Possible, Probable, Quasi-certaine).
04	**Evaluation de l'impact** Conséquences sur la confidentialité, l'intégrité et la disponibilité (échelle 1 à 4).
05	**Calcul du niveau de risque** Risque = Vraisemblance x Impact. Définition d'un seuil d'acceptabilité.

4.2 Plan de traitement des risques (PTR)

Option	Description	Quand l'utiliser ?
Modifier (Réduire)	Mettre en place des contrôles de sécurité pour réduire la vraisemblance ou l'impact.	Risque traitable a un coût acceptable.
Accepter	Le risque résiduel est dans les limites d'acceptabilité définies par la direction.	Coût du traitement > impact potentiel.
Éviter	Supprimer l'activité ou le processus générateur de risque.	Risque inacceptable, alternative possible.
Partager / Transférer	Externaliser le risque (assurance cyber, sous-traitance).	Risque résiduel trop élevé malgré les contrôles.

4.3 Déclaration d'Applicabilité (SoA)

La SoA est un document pivot et obligatoire du SMSI. Elle recense les 93 contrôles de l'Annexe A et précise pour chacun s'il est applicable ou non, avec une justification documentée.

ID	Controle (exemple)	Applicable	Statut	Justification
5.1	Politiques de sécurité	Oui	Mis en oeuvre	Exigence fondamentale du SMSI
5.15	Contrôle d'accès	Oui	En cours	Réduction risque accès non autorisé
7.4	Surveillance physique	Non	N/A	Hors périmètre (sites cloud uniquement)

05 L'Annexe A — Les 93 controles de securite

L'Annexe A de l'ISO 27001:2022 liste 93 contrôles organisés en 4 thèmes. Chaque contrôle dispose désormais d'attributs (type, propriété, capacité) permettant la priorisation.

5.x	6.x	7.x	8.x
ORGANISATIONNEL	**HUMAIN**	**PHYSIQUE**	**TECHNOLOGIQUE**
37 contrôles	8 contrôles	14 contrôles	34 contrôles

Organisationnel (5.x) — 37 contrôles

ID	Controle
5.7	Threat intelligence (NOUVEAU 2022)
5.9	Inventaire des actifs informationnels
5.15	Controle d'acces
5.19–5.22	Sécurité dans les relations avec les fournisseurs
5.23	Sécurité cloud (NOUVEAU 2022)
5.30	Disponibilité ICT (NOUVEAU 2022)

Humain (6.x) — 8 contrôles

ID	Contrôle
6.1	Filtrage (verification des antecedents)
6.3	Sensibilisation, formation et education SSI
6.7	Travail à distance (télétravail)
6.8	Signalement d'événements SSI (NOUVEAU 2022)

Physique (7.x) — 14 contrôles

ID	Contrôle
7.1	Perimetres de securite physique
7.4	Surveillance de la sécurité physique (NOUVEAU 2022)
7.10	Supports de stockage (cycle de vie)
7.14	Mise au rebut ou utilisation sécurisée des équipements

Technologique (8.x) — 34 contrôles

ID	Contrôle
8.9	Gestion de la configuration (NOUVEAU 2022)
8.11	Masquage des données (NOUVEAU 2022)
8.12	Prévention de fuite de données DLP (NOUVEAU 2022)
8.16	Surveillance des activites (NOUVEAU 2022)
8.22	Filtrage web (NOUVEAU 2022)
8.28	Sécurité du code (NOUVEAU 2022)

06 Les 11 nouveaux contrôles de la version 2022

La version 2022 introduit 11 nouveaux contrôles qui reflètent l'évolution du paysage des menaces et des pratiques de cybersécurité : cloud, intelligence sur les menaces, confidentialité des données, code sécurisé, surveillance avancée.

5.7	**Threat Intelligence** Collecter et analyser des renseignements sur les menaces pertinentes pour adapter les défenses.
5.23	**Sécurité cloud** Définir et appliquer des processus pour la sécurité des services cloud : acquisition, utilisation, sortie.
5.30	**Disponibilité ICT** Planifier la continuité des services ICT en cas de perturbation, en lien avec les plans de continuité.
7.4	**Surveillance physique** Surveiller en continu les accès non autorisés aux zones sensibles par des systèmes de détection.
8.9	**Gestion de la configuration** Établir, documenter et maintenir les configurations sécurisées des équipements, logiciels et services.
8.10	**Suppression de l'information** Assurer la suppression sécurisée et irréversible des informations obsolètes.
8.11	**Masquage des données** Appliquer des techniques de masquage (pseudonymisation, tokenisation) pour protéger les données sensibles.
8.12	**Prévention de fuite (DLP)** Détecter et prévenir la divulgation non autorisée d'informations sensibles.
8.16	**Surveillance des activités** Surveiller les réseaux, systèmes et applications pour détecter des comportements anormaux.
8.22	**Filtrage web** Filtrer les accès aux sites web externes pour protéger contre les contenus malveillants.
8.28	**Sécurité du code** Appliquer des principes de développement sécurisés pour réduire les vulnérabilités.

Note de migration : Les organisations certifiées ISO 27001:2013 devaient migrer vers la version 2022 avant le 31 octobre 2025. Les audits de transition vérifiaient notamment la prise en compte de ces 11 nouveaux contrôles dans la SoA et le PTR.

07 Roadmap de certification ISO 27001

La certification ISO 27001 est un projet structurel qui s'étale généralement sur 12 à 24 mois selon la taille et la maturité de l'organisation.

PHASE 1	Cadrage et analyse de l'existant	2-3 mois
✓	Nomination du RSSI et constitution de l'équipe projet	
✓	Définition du périmètre du SMSI	
✓	Audit de conformité initial (gap analysis) par rapport à l'ISO 27001:2022	
✓	Inventaire des actifs informationnels	
✓	Identification du contexte et des parties intéressées	

PHASE 2	Conception du SMSI	3-4 mois
✓	Elaboration de la politique de sécurité de l'information (PSSI)	
✓	Méthodologie de gestion des risques (choix et validation)	
✓	Réalisation de l'analyse de risques complète	
✓	Elaboration du Plan de Traitement des Risques (PTR)	
✓	Rédaction de la Déclaration d'Applicabilité (SoA)	

PHASE 3	Déploiement et sensibilisation	6-9 mois
✓	Mise en oeuvre des contrôles sélectionnés dans la SoA	
✓	Rédaction et validation de la documentation obligatoire	
✓	Programme de sensibilisation et de formation des collaborateurs	
✓	Mise en place des procédures opérationnelles (incidents, accès, changements)	

PHASE 4	Audit interne et revue de direction	1-2 mois
✓	Audit interne complet de l'ensemble du SMSI	
✓	Rédaction du rapport d'audit et identification des non-conformités	
✓	Plans d'actions correctives et suivi	
✓	Revue de direction annuelle (résultats, risques, objectifs)	

PHASE 5	Audit de certification	2-4 semaines
✓	Audit de Stage 1 : revue documentaire par l'auditeur externe	
✓	Audit de Stage 2 : audit sur site, entretiens, tests de contrôles	
✓	Rapport d'audit et traitement des écarts identifiés	
✓	Obtention du certificat ISO 27001:2022 (valide 3 ans)	

08 Documentation obligatoire et recommandée

L'ISO 27001 exige un ensemble précis de documents et d'enregistrements. La distinction entre documents exigés et "recommandés" est essentielle pour calibrer l'effort documentaire.

Document / Enregistrement	Article ISO 27001:2022
Périmètre du SMSI	4.3
Politique de sécurité de l'information (PSSI)	5.2
Méthodologie d'appréciation des risques	6.1.2
Déclaration d'Applicabilité (SoA)	6.1.3 d)
Plan de Traitement des Risques (PTR)	6.1.3 e)
Objectifs de sécurité de l'information	6.2
Résultats de l'appréciation des risques	8.2
Résultats du traitement des risques	8.3
Programme et résultats des audits internes	9.2
Compte-rendu des revues de direction	9.3
Non-conformités et actions correctives	10.1

Documents complémentaires recommandés

- Politique de gestion des accès et des habilitations
- Procédure de gestion des incidents de sécurité
- Procédure de gestion des changements
- Plan de continuité d'activité (PCA) et plan de reprise après sinistre (PRS)
- Politique de classification de l'information
- Procédure de gestion des fournisseurs et tiers
- Chartes informatiques utilisateurs
- Registre des actifs informationnels

09 Indicateurs et tableau de bord SMSI (KPI)

L'ISO 27001 (article 9.1) exige la définition et le suivi de mesures de performance du SMSI. Ces indicateurs permettent de démontrer l'efficacité des contrôles et de prouver l'amélioration continue lors des audits.

Domaine	Indicateur (KPI)	Fréquence	Cible
Incidents	Nombre d'incidents SSI déclarés	Mensuelle	< N-1
Incidents	Délai moyen de résolution (MTTR)	Mensuelle	< 4h critique
Vulnérabilités	Taux de vulnérabilités critiques non corrigées	Mensuelle	< 5 %
Accès	Taux de revue périodique des accès	Trimestrielle	100 %
Formation	Taux de complétion formation SSI	Annuelle	>= 95 %
Formation	Taux de clic phishing simule	Semestrielle	< 5 %
Audit	Nombre de non-conformités audit interne	Annuelle	Tendance baisse
Audit	Taux de clôture des actions correctives	Trimestrielle	>= 90 %
Conformité	Taux de contrôles SoA mis en oeuvre	Trimestrielle	>= 90 %
Continuité	Taux de tests PCA réalisés	Annuelle	100 %

10 ISO 27001 et autres référentiels

10.1 ISO 27001 et RGPD

Le RGPD et l'ISO 27001 sont complémentaires. L'ISO 27001 couvre la sécurité de l'information au sens large, tandis que le RGPD se concentre spécifiquement sur la protection des données personnelles. La mise en œuvre de l'ISO 27001 contribue directement à la conformité RGPD.

Domaine	ISO 27001:2022	RGPD (Art. 32)
Chiffrement	Contrôle 8.24 (cryptographie)	Pseudonymisation et chiffrement
Incidents	Contrôles 5.24-5.28	Notification 72h CNIL
Accès	Contrôles 5.15-5.18, 8.2-8.5	Principe de minimisation
Documentation	Article 7.5	Registre des activités de traitement

10.2 ISO 27001 et NIS2

La directive NIS2, transposée en droit français depuis 2024, impose des exigences de cybersécurité aux entités essentielles et importantes. L'ISO 27001 constitue un socle solide pour répondre à ces exigences.

- Gestion des risques : NIS2 Art. 21 - directement couverte par les articles 6.1 et 8 de l'ISO 27001.
- Gestion des incidents : NIS2 impose la notification sous 24h (alerte précoce) et 72h (rapport initial).
- Chaîne d'approvisionnement : NIS2 Art. 21.2 - couverte par les contrôles 5.19-5.22 de l'ISO 27001.
- Gouvernance : NIS2 responsabilise la direction au même titre que l'ISO 27001 article 5.

10.3 ISO 27001 et SOC 2

Le SOC 2 est un référentiel américain (AICPA) très demandé par les entreprises technologiques exportant vers les marchés anglophones. Il partage de nombreux principes avec l'ISO 27001 (environ 70% de chevauchement).

Critere	ISO 27001	SOC 2
Origine	ISO (international)	AICPA (american)
Périmètre	SMSI global	5 Trust Services Criteria
Audit	Organisme accrédité COFRAC/IAF	CPA indépendant
Durée	Certification 3 ans + suivi annuel	Rapport annuel (Type I / II)

11 Bénéfices et ROI de la certification

La certification ISO 27001 est un investissement stratégique dont le retour sur investissement est mesurable et multidimensionnel.

Réduction des incidents 70% de réduction des incidents de sécurité significatifs chez les organisations certifiées.	**Avantage concurrentiel** La certification rassure les clients et partenaires. Différenciateur clé sur des marchés réglementés.	**Conformité réglementaire** Contribue directement à la conformité RGPD, NIS2, DORA. Réduire le risque de sanctions.
Réduction des coûts 4,45 M$ de coût moyen d'une violation de données. La prévention est significativement moins chère.	**Amélioration des processus** La démarche SMSI structure et optimise les processus IT, sécurité et gouvernance.	**Acces aux marches** Condition d'entrée sur certains marchés (défense, santé, finance). Facilite les partenariats.

Estimation du ROI : Une étude Forrester Research indique que les entreprises certifiées ISO 27001 obtiennent un ROI moyen de 220% sur 3 ans. Le coût moyen d'une certification pour une PME (50-200 personnes) se situe entre 50 000 et 150 000 euros (conseil + mise en œuvre + certification).

12 FAQ — Questions fréquentes

? Combien de temps dure un projet de certification ISO 27001 ?

En moyenne 12 à 18 mois pour une première certification. Ce délai peut être ramené à 9-12 mois avec un accompagnement expérimenté et un fort engagement de la direction. Le renouvellement triennal nécessite généralement 2-3 mois de préparation.

? Quel est le coût d'une certification ISO 27001 ?

Pour une PME (50-200 personnes) : conseil et accompagnement (30-80 k euros) + audit de certification (5-15 k euros) + outillage (5-20 k euros). Les grandes entreprises peuvent investir plusieurs centaines de milliers d'euros.

? L'ISO 27001 est-elle obligatoire ?

Non, la certification est volontaire. Cependant, elle peut être requise contractuellement par des clients stratégiques, des donneurs d'ordre publics, ou imposée de facto par des régulations sectorielles (défense, santé, finance)

? Quelle est la différence entre ISO 27001 et ISO 27002 ?

L'ISO 27001 est la norme de certification : elle définit les exigences du SMSI. L'ISO 27002 est le guide de bonnes pratiques qui détaille comment implémenter les contrôles de l'Annexe A. On ne peut pas être certifié ISO 27002.

? Peut-on certifier uniquement une partie de l'entreprise ?

Oui. Le périmètre de certification peut être limité à un département, un site, un produit ou un service spécifique. Le périmètre doit toutefois être cohérent et les interfaces avec le reste de l'organisation correctement gérées.

? Comment choisir un organisme certificateur ?

En France, les principaux organismes accrédités COFRAC sont : Bureau Veritas, BSI, LRQA, SGS, DNV. Il est recommandé de comparer plusieurs offres sur la méthodologie d'audit, l'expérience sectorielle, le rapport qualité/prix et la notoriété internationale.

? Quels sont les principaux pièges à éviter ?

Sous-estimer l'engagement de la direction, sur-dimensionner le périmètre initial, négliger la sensibilisation des utilisateurs, produire de la documentation sans la mettre en pratique, et traiter le projet ISO 27001 comme un projet IT plutôt qu'un projet organisationnel.

? Que se passe-t-il après la certification ?

La certification est valable 3 ans. Des audits de suivi annuels vérifient le maintien de la conformité. Au bout de 3 ans, un audit de renouvellement complet est réalisé. Le SMSI doit être maintenu et amélioré en continu.

13 Conclusion et perspectives

L'ISO/IEC 27001:2022 représente bien plus qu'un simple label de conformité. C'est un véritable système de management qui ancre la sécurité de l'information au cœur de la stratégie et de la culture d'entreprise.

Les tendances à surveiller dans les années à venir incluent l'intégration croissante de l'intelligence artificielle dans les contrôles de sécurité, l'évolution des menaces liées à l'informatique quantique (post-quantum cryptography), et le renforcement des exigences de sécurité dans les chaînes d'approvisionnement numériques.

Prêt à vous lancer dans votre projet de certification ISO 27001 ?

Transmute Consulting accompagne les organisations de toutes tailles dans leur démarche de certification ISO 27001 : audit de conformité initial, élaboration du SMSI, gestion des risques, sensibilisation, préparation à l'audit. Nos experts certifiés Lead Implementer et Lead Auditor ISO 27001 sont à votre disposition.

References normatives et bibliographiques

- ISO/IEC 27001:2022 - Sécurité de l'information, cybersécurité et protection de la vie privée — SMSI
- ISO/IEC 27002:2022 - Contrôles de sécurité de l'information
- ISO/IEC 27005:2022 - Lignes directrices pour la gestion des risques
- ISO/IEC 27701:2019 - Extension ISO 27001/27002 pour la protection des données personnelles
- ISO/IEC 27017:2015 - Sécurité cloud (contrôles supplémentaires)
- EBIOS Risk Manager - ANSSI, version 2018
- IBM Cost of a Data Breach Report 2023
- CESIN - Baromètre annuel de la cybersécurité des entreprises 2023