

Comment se déroule une certification

Le parcours complet, de votre demande à votre renouvellement

Une certification ISO/IEC 27001 se déroule en huit étapes, puis se maintient pendant trois ans. Voici le parcours et les délais sur lesquels nous nous engageons.

1	Votre demande Vous remplissez le formulaire joint au kit (pièce 8) et vous nous le retournez signé.	Réponse sous 5 jours ouvrés
2	Notre revue de votre demande Nous vérifions quatre points : vos informations sont suffisantes, il n'y a pas de malentendu sur votre périmètre, nous avons les compétences et la disponibilité nécessaires, et rien ne menace notre neutralité. Nous acceptons ou nous refusons par écrit, avec un motif.	Acceptation ou refus motivé
3	Contrat et calcul de la durée d'audit La durée est calculée selon une méthode écrite, à partir de l'effectif concerné par votre système, du nombre de sites et de la complexité de vos systèmes d'information. Elle est justifiée par écrit et ne se négocie pas.	Devis et contrat
4	Audit étape 1 Nous vérifions que votre système est prêt à être audité : périmètre, documentation, appréciation des risques, déclaration d'applicabilité, audits internes et revue de direction déjà réalisés. Vous recevez un compte rendu écrit.	1 à 3 mois après la signature
5	Audit étape 2 Sur site. Nous vérifions que votre système fonctionne réellement et produit les résultats attendus. Réunion d'ouverture, entretiens, examen des preuves, réunion de clôture où les constats vous sont présentés.	1 à 3 mois après l'étape 1
6	Rapport et traitement des écarts Vous recevez le rapport d'audit. S'il y a des non-conformités, vous nous transmettez un plan de correction, puis les preuves que les actions ont été menées.	Rapport sous 15 jours ouvrés
7	Relecture et décision Votre dossier est relu, puis la décision est prise par une personne qui n'a pas participé à votre audit. Aucune non-conformité majeure ouverte ne permet une décision favorable.	Décision sous 60 jours après l'étape 2, dont 30 jours au plus une fois votre dossier complet
8	Votre certificat Il précise votre périmètre exact, la version de la norme, vos sites, la référence de votre déclaration d'applicabilité et sa date d'expiration.	Émis sous 10 jours ouvrés après la décision — valable 3 ans

Puis, pendant les trois ans

Quand	Ce qui se passe
Au plus tard 12 mois après la décision	Premier audit de surveillance. Plus court qu'un audit initial : nous vérifions que votre système continue de fonctionner et que vos engagements sont tenus.
24 mois après la décision (± 3 mois)	Deuxième audit de surveillance.
Avant la fin des 3 ans	Audit de renouvellement, à mener suffisamment tôt pour que la décision intervienne avant l'expiration de votre certificat. Prévoyez environ trois mois de marge.
À tout moment	Audit d'extension si votre périmètre s'élargit, ou audit à préavis court en cas d'incident ou de plainte. Le préavis minimal est de cinq jours ouvrés, sauf urgence.

Les délais que vous devez tenir de votre côté

Situation	Votre délai
Non-conformité majeure	Plan de correction sous 30 jours, actions menées et prouvées sous 90 jours
Non-conformité mineure	Plan de correction sous 60 jours, actions vérifiées lors de l'audit suivant
Récusation d'un auditeur	5 jours ouvrés après réception de la composition de l'équipe

Changement significatif chez vous

Nous en informer sans délai (voir la pièce 6)

Vous nous avez aussi interrogés sur le HDS

Nous ne délivrons pas de certificat d'hébergeur de données de santé aujourd'hui. Le parcours décrit ci-dessus concerne l'ISO/IEC 27001. La pièce 4 vous explique pourquoi, et ce que nous pourrions proposer ensuite.