

Nos compétences

Ce que nous certifions, et ce que nous exigeons de nos auditeurs

Un audit ne vaut que ce que vaut l'auditeur qui le conduit. Ce document décrit ce que nous couvrons et les règles que nous appliquons pour choisir, qualifier et surveiller les personnes qui interviennent chez vous.

Les référentiels que nous couvrons

- ISO/IEC 27001:2022 — système de management de la sécurité de l'information. C'est notre activité de certification.
- Référentiel HDS (hébergeur de données de santé) — nos procédures sont écrites, mais nous ne proposons pas cette certification aujourd'hui. La délivrance d'un certificat HDS suppose une accréditation que nous n'avons pas encore. Voir la pièce 4 du kit.

Nos audits sont conduits sur site, à distance ou en formule mixte, en français.

Les domaines techniques que nous couvrons

Cryptographie, infrastructures et services cloud, systèmes industriels et d'automatisme, services financiers, télécommunications, administration publique, secteur de la santé.

Ce que nous exigeons d'un auditeur

- Un diplôme de niveau bac+3 minimum en informatique, sécurité, management ou ingénierie, ou une expérience équivalente reconnue.
- Une certification de responsable d'audit ISO/IEC 27001 en cours de validité, obtenue à l'issue d'une formation d'au moins 40 heures.
- La maîtrise de la famille de normes ISO 27000, d'une méthode d'appréciation des risques (ISO 27005 ou EBIOS Risk Manager) et des règles de conduite d'un audit (ISO 19011).
- Au moins quinze jours d'audit réalisés au cours des cinq dernières années.
- Seize heures de formation continue par an, dont une part obligatoire sur l'évolution des normes, sur la cybersécurité et sur l'impartialité.
- Un engagement d'indépendance et un engagement de confidentialité signés.

Nos autres rôles

Rôle	Ce que nous exigeons
Expert technique	Expertise pointue dans une technologie ou un secteur, au moins cinq ans d'expérience récente, et la compréhension du déroulement d'un audit. Il n'audite pas seul : il assiste l'équipe.
Relecteur du dossier	Certification de responsable d'audit ISO/IEC 27001 valide, plus une formation attestée aux règles applicables aux organismes de certification.
Décideur	Mêmes exigences, plus un cadre de décision documenté et vingt heures de formation continue par an.
Décideur externe de secours	Mêmes exigences, plus l'indépendance vis-à-vis de notre direction. Il intervient sous dix jours ouvrés lorsqu'il est sollicité.

Comment nous sélectionnons nos auditeurs

Six étapes, dans cet ordre :

- Dossier de candidature complet : CV, diplômes, certifications, attestations d'audits réalisés avec leurs référents, déclaration d'intérêts, engagement de confidentialité.
- Vérification des pièces et contrôle d'au moins deux références professionnelles, sous quinze jours ouvrés.
- Entretien technique de quatre-vingt-dix minutes, avec étude d'un cas pratique.
- Évaluation des aptitudes personnelles pendant soixante minutes, avec mise en situation.
- Décision écrite et motivée : autorisation, autorisation sous condition, ou refus.
- Contrat signé et inscription au registre des personnes qualifiées.

Comment nous vérifions qu'ils restent compétents

- Une observation sur site lors de la qualification initiale, puis des observations périodiques tout au long de la collaboration.

- La relecture systématique de tous les rapports d'audit qu'ils produisent.
- Une enquête de satisfaction auprès du client après chaque audit.
- Le suivi de toute plainte les concernant.
- Une revue individuelle de compétence, une fois par an.
- Un plan de formation annuel et une sensibilisation obligatoire à l'impartialité.

Notre vivier d'auditeurs

Nous tenons un vivier d'auditeurs qualifiés, mis à jour par notre direction des opérations. Chaque auditeur y est suivi par les rôles qu'il est autorisé à tenir, les référentiels qu'il maîtrise, la date de sa dernière évaluation de compétence et la validité de sa déclaration d'intérêts. Un auditeur dont l'un de ces éléments est périmé ne peut pas être affecté à une mission.