

# Checklist d'audit de certification ISO 27001 — Cloud & Data Centers

Un outil d'auto-évaluation, clause par clause, pour préparer votre audit de certification ISO 27001 en tenant compte des risques propres au cloud et aux data centers : sécurité physique, isolation multi-tenant et engagements de disponibilité.

## COMMENT UTILISER CETTE CHECKLIST

Pour chaque question, évaluez votre niveau de préparation réel, avec le responsable sécurité de l'information (RSSI) et les équipes IT concernées. Cette auto-évaluation ne remplace pas un audit de certification : elle vous permet d'identifier, en amont, les points forts et les zones qui nécessitent encore un travail de mise en conformité.

### OUI

Vous êtes en mesure de démontrer ce point avec des preuves documentées.

### PARTIELLEMENT

Le point existe mais nécessite d'être renforcé, formalisé ou complété.

### PAS ENCORE

Le point n'est pas encore traité ; un plan d'action est à prévoir.

## CLAUSE 4 — CONTEXTE DE L'ORGANISME

Pour un opérateur de data center ou de cloud, le contexte est marqué par l'hébergement mutualisé de multiples clients et des engagements contractuels de disponibilité stricts.

| VOTRE ENTREPRISE A-T-ELLE DÉTERMINÉ                                                                                      | OUI | PARTIELLEMENT | PAS ENCORE |
|--------------------------------------------------------------------------------------------------------------------------|-----|---------------|------------|
| les enjeux externes propres au secteur : exigences de disponibilité (SLA), réglementation sur l'hébergement de données ? |     |               |            |
| les enjeux internes : criticité de l'infrastructure physique, isolation entre clients hébergés ?                         |     |               |            |
| les parties intéressées pertinentes (clients hébergés, fournisseurs d'énergie, autorités) et leurs exigences ?           |     |               |            |
| le domaine d'application du SMSI (data centers, infrastructure cloud, sites concernés) ?                                 |     |               |            |

## CLAUSE 5 — LEADERSHIP

La direction doit porter un engagement sur la disponibilité et l'isolation des environnements clients, condition de la confiance en hébergement mutualisé.

| LA DIRECTION GÉNÉRALE                                                                                         | OUI | PARTIELLEMENT | PAS ENCORE |
|---------------------------------------------------------------------------------------------------------------|-----|---------------|------------|
| assume-t-elle la responsabilité de la disponibilité et de l'isolation des environnements clients hébergés ?   |     |               |            |
| a-t-elle établi une politique de sécurité de l'information intégrant les engagements de disponibilité (SLA) ? |     |               |            |
| a-t-elle désigné un responsable sécurité de l'information (RSSI) avec l'autorité nécessaire ?                 |     |               |            |
| s'assure-t-elle que les rôles liés à la sécurité physique et logique sont clairement définis ?                |     |               |            |

## CLAUSE 6 — PLANIFICATION

La planification doit inclure une analyse de risques couvrant la sécurité physique des sites, l'isolation multi-tenant et les risques de continuité de service.

| VOTRE ENTREPRISE A-T-ELLE                                                                                           | OUI | PARTIELLEMENT | PAS ENCORE |
|---------------------------------------------------------------------------------------------------------------------|-----|---------------|------------|
| réalisé une analyse de risques formelle couvrant la sécurité physique et l'isolation entre environnements clients ? |     |               |            |
| établi une déclaration d'applicabilité (SoA) justifiant les contrôles de l'Annexe A retenus ou exclus ?             |     |               |            |
| défini des objectifs de sécurité mesurables (taux de disponibilité, délai de détection d'intrusion physique) ?      |     |               |            |

## CLAUSE 7 — SUPPORT

Le support couvre la sensibilisation des équipes d'exploitation, la formation aux procédures d'urgence, et la maîtrise documentaire des politiques d'accès physique.

| QUESTIONS                                                                                                           | OUI | PARTIELLEMENT | PAS ENCORE |
|---------------------------------------------------------------------------------------------------------------------|-----|---------------|------------|
| l'ensemble du personnel suit-il une formation de sensibilisation à la sécurité de l'information annuellement ?      |     |               |            |
| les équipes d'exploitation sont-elles formées aux procédures de sécurité physique et logique du data center ?       |     |               |            |
| les politiques de sécurité (accès physique, isolation logique, chiffrement) sont-elles documentées et accessibles ? |     |               |            |
| les nouveaux employés accédant aux salles serveurs font-ils l'objet d'une vérification des antécédents ?            |     |               |            |

## CLAUSE 8 — OPÉRATION

C'est la clause la plus dense : sécurité physique des sites, isolation logique entre clients, redondance des infrastructures et gestion des incidents de disponibilité.

| VOTRE ENTREPRISE A-T-ELLE MIS EN PLACE                                                                            | OUI | PARTIELLEMENT | PAS ENCORE |
|-------------------------------------------------------------------------------------------------------------------|-----|---------------|------------|
| des contrôles d'accès physique multicouches aux salles serveurs (badges, biométrie, vidéosurveillance) ?          |     |               |            |
| une isolation logique stricte entre les environnements des différents clients hébergés ?                          |     |               |            |
| une redondance des infrastructures critiques (alimentation électrique, refroidissement, connectivité réseau) ?    |     |               |            |
| un chiffrement des données clients au repos et en transit, avec gestion sécurisée des clés ?                      |     |               |            |
| une politique de gestion des vulnérabilités incluant des tests d'intrusion réguliers sur l'infrastructure ?       |     |               |            |
| une procédure de gestion des incidents de sécurité, incluant les atteintes à la disponibilité (SLA) ?             |     |               |            |
| un plan de continuité d'activité et de reprise après sinistre testé périodiquement, incluant un site de secours ? |     |               |            |
| une évaluation de sécurité des fournisseurs critiques (énergie, connectivité, maintenance) ?                      |     |               |            |

## CLAUSE 9 — ÉVALUATION DES PERFORMANCES

L'évaluation des performances doit démontrer la disponibilité constante des infrastructures et l'efficacité de l'isolation multi-tenant.

| QUESTIONS                                                                                                        | OUI | PARTIELLEMENT | PAS ENCORE |
|------------------------------------------------------------------------------------------------------------------|-----|---------------|------------|
| l'infrastructure est-elle surveillée en continu (NOC/SOC) pour détecter les anomalies physiques et logiques ?    |     |               |            |
| des audits internes du SMSI couvrant la sécurité physique et logique sont-ils conduits à intervalles planifiés ? |     |               |            |
| les indicateurs de sécurité (disponibilité, incidents, temps de réponse) sont-ils suivis et analysés ?           |     |               |            |
| la revue de direction intègre-t-elle un bilan des incidents et du respect des engagements de disponibilité ?     |     |               |            |

## CLAUSE 10 — AMÉLIORATION

L'amélioration continue dans le cloud et les data centers se mesure à la réduction durable des incidents de disponibilité et de sécurité.

| QUESTIONS                                                                                                  | OUI | PARTIELLEMENT | PAS ENCORE |
|------------------------------------------------------------------------------------------------------------|-----|---------------|------------|
| chaque incident de sécurité ou de disponibilité fait-il l'objet d'une action corrective documentée ?       |     |               |            |
| les enseignements des incidents sont-ils intégrés à l'architecture de redondance et d'isolation ?          |     |               |            |
| l'entreprise recherche-t-elle activement des opportunités d'amélioration de sa résilience infrastructure ? |     |               |            |

### VOTRE PROCHAINE ÉTAPE

Le résultat de cette auto-évaluation vous oriente vers l'une des situations suivantes.

#### Majorité de OUI

Votre système est globalement prêt. Un audit à blanc ciblé permettra de sécuriser les derniers points avant la certification.

#### Majorité de PARTIELLEMENT

Les fondations existent mais doivent être structurées et documentées. Un accompagnement resserré permet de combler ces écarts rapidement.

#### Majorité de PAS ENCORE

Une mise à niveau complète du système est nécessaire avant d'envisager un audit de certification. Un diagnostic initial est recommandé.

## Besoin d'un accompagnement ISO 27001 pour votre entreprise de cloud ou de data center ?

Agilion Quality accompagne les entreprises marocaines dans la mise en place de leur système de management de la sécurité de l'information, du diagnostic initial jusqu'à l'obtention du certificat, avec un engagement de résultat et une mobilisation possible des subventions étatiques (OFPPT, GIAC, Maroc PME).

**W.** agilionquality.com **E.** contact@agilionquality.com **T.** +212 (0) 620 55 97 20

4ème Étage – Bureau N°12, Bd 11 Janvier, 2 Rue Essanaoubar, Casablanca 20130

### À PROPOS D'AGILION QUALITY

Agilion Quality SARL AU est un cabinet de conseil basé à Casablanca, spécialisé dans l'accompagnement à la certification ISO, la mise en place de systèmes de management intégrés (SMI), les accréditations réglementaires et sectorielles et la mobilisation de subventions publiques pour le financement des démarches qualité.