CONSUP ON
les conseils d'experts

CHECKLIST SÉCURITÉ · ÉDITION 2026

# Questionnaire sécurité : 40 questions pour choisir un prestataire NOC.

Le modèle prêt à l'emploi pour évaluer un prestataire de supervision ou d'administration réseau, et comparer les réponses sur des bases identiques.

Pour les **RSSI**, **DSI** et **acheteurs IT** des MSP, ESN et infogéreurs

consupon.com

MODE D'EMPLOI

# Comment utiliser ce questionnaire

Confier vos réseaux et ceux de vos clients à un prestataire, c'est lui ouvrir vos accès les plus sensibles. Ce questionnaire vous aide à vérifier, par écrit, les garanties qu'il apporte avant de signer.

ÉTAPE 1

**Envoyez-le**

Adressez les 40 questions à chaque prestataire consulté, avec une date de retour.

ÉTAPE 2

**Exigez des preuves**

Pour chaque réponse « oui », demandez la pièce justificative indiquée dans la colonne de droite.

ÉTAPE 3

**Notez et comparez**

Utilisez la grille de notation de la page 7 pour classer les prestataires.

## Les 8 thèmes couverts


01 Gouvernance et certification p. 3

02 Personnel et confidentialité p. 3

03 Gestion des accès et des identités p. 4

04 Traçabilité et journalisation p. 4

05 Gestion des incidents de sécurité p. 5

06 Protection des données p. 5

07 Continuité, réversibilité et sous-traitance p. 6

08 Conformité réglementaire p. 6


**Bon à savoir :** un prestataire sérieux répond à ce type de questionnaire sans difficulté, et fournit les justificatifs sous accord de confidentialité si nécessaire. Une réponse évasive est déjà une réponse.

# Les questions à poser

## 01 · GOUVERNANCE ET CERTIFICATION

| N° | Question | Réponse | Justificatif à demander |
|---|---|---|---|
| 01 | Êtes-vous certifié ISO/IEC 27001 ? Selon quelle version de la norme ? | Oui Non Partiel | Certificat en cours de validité |
| 02 | Le périmètre du certificat couvre-t-il les services que nous achetons ? | Oui Non Partiel | Mention du périmètre sur le certificat |
| 03 | Quel organisme a délivré le certificat, et jusqu'à quelle date est-il valide ? | Oui Non Partiel | Lien de vérification auprès de l'organisme |
| 04 | Qui est responsable de la sécurité de l'information chez vous ? | Oui Non Partiel | Organigramme, fiche de poste |
| 05 | Disposez-vous d'une politique de sécurité formalisée et revue chaque année ? | Oui Non Partiel | Sommaire de la politique, date de revue |

## 02 · PERSONNEL ET CONFIDENTIALITÉ

| N° | Question | Réponse | Justificatif à demander |
|---|---|---|---|
| 06 | Chaque intervenant signe-t-il un engagement de confidentialité ? | Oui Non Partiel | Modèle d'engagement |
| 07 | Les intervenants sont-ils dédiés à notre compte ou partagés entre clients ? | Oui Non Partiel | Description de l'organisation |
| 08 | Quelles vérifications réalisez-vous au recrutement ? | Oui Non Partiel | Procédure de recrutement |
| 09 | Vos équipes suivent-elles une sensibilisation régulière à la sécurité ? | Oui Non Partiel | Programme et fréquence |
| 10 | Que se passe-t-il quand un intervenant quitte notre compte ou votre société ? | Oui Non Partiel | Procédure de départ, délai de retrait des accès |

## 03 · GESTION DES ACCÈS ET DES IDENTITÉS

| N° | Question | Réponse | Justificatif à demander |
|---|---|---|---|
| 11 | Vos équipes passent-elles exclusivement par nos accès (VPN, bastion) ? | Oui Non Partiel | Schéma d'accès |
| 12 | Les comptes sont-ils nominatifs, jamais partagés ? | Oui Non Partiel | Liste des comptes demandés |
| 13 | L'authentification multifacteur est-elle utilisée sur tous les accès ? | Oui Non Partiel | Description de la méthode |
| 14 | Les droits sont-ils limités au strict périmètre de la mission ? | Oui Non Partiel | Matrice des droits |
| 15 | Pouvons-nous révoquer un accès à tout moment, sans préavis ? | Oui Non Partiel | Clause contractuelle |
| 16 | Les postes de travail de vos intervenants sont-ils gérés et sécurisés ? | Oui Non Partiel | Politique postes : chiffrement, antivirus, mises à jour |

## 04 · TRAÇABILITÉ ET JOURNALISATION

| N° | Question | Réponse | Justificatif à demander |
|---|---|---|---|
| 17 | Toutes les interventions sont-elles tracées dans notre outil de tickets ? | Oui Non Partiel | Exemple de ticket anonymisé |
| 18 | Les changements suivent-ils notre processus de validation ? | Oui Non Partiel | Procédure de gestion des changements |
| 19 | Conservez-vous un journal des connexions de vos intervenants ? | Oui Non Partiel | Durée de conservation |
| 20 | La documentation technique est-elle tenue à jour, et à qui appartient-elle ? | Oui Non Partiel | Clause de propriété de la documentation |

## 05 · GESTION DES INCIDENTS DE SÉCURITÉ

| N° | Question | Réponse | Justificatif à demander |
|---|---|---|---|
| 21 | Avez-vous une procédure de gestion des incidents de sécurité ? | Oui Non Partiel | Procédure documentée |
| 22 | Sous quel délai sommes-nous informés d'un incident nous concernant ? | Oui Non Partiel | Engagement contractuel |
| 23 | Qui est notre interlocuteur en cas d'incident, de jour comme de nuit ? | Oui Non Partiel | Contacts d'escalade |
| 24 | Réalisez-vous une analyse après chaque incident significatif ? | Oui Non Partiel | Modèle de rapport d'incident |

## 06 · PROTECTION DES DONNÉES

| N° | Question | Réponse | Justificatif à demander |
|---|---|---|---|
| 25 | Nos données et celles de nos clients restent-elles dans nos systèmes ? | Oui Non Partiel | Description des flux de données |
| 26 | Depuis quel pays vos équipes interviennent-elles ? | Oui Non Partiel | Adresse des sites d'intervention |
| 27 | Quelles mesures encadrent un éventuel transfert de données hors de l'UE ? | Oui Non Partiel | Clauses contractuelles, garanties |
| 28 | Utilisez-vous vos propres outils pour stocker des données nous concernant ? | Oui Non Partiel | Liste des outils |
| 29 | Signez-vous un accord de traitement des données (DPA) ? | Oui Non Partiel | Modèle de DPA |

## 07 · CONTINUITÉ, RÉVERSIBILITÉ ET SOUS-TRAITANCE

| N° | Question | Réponse | Justificatif à demander |
|---|---|---|---|
| 30 | Comment assurez-vous la continuité du service pendant les congés et absences ? | Oui Non Partiel | Organisation des remplacements |
| 31 | Sous quel délai remplacez-vous un intervenant qui quitte notre compte ? | Oui Non Partiel | Engagement contractuel |
| 32 | Disposez-vous d'un plan de continuité d'activité pour vos sites ? | Oui Non Partiel | Synthèse du plan |
| 33 | Comment se déroule la réversibilité en fin de contrat ? | Oui Non Partiel | Plan de réversibilité |
| 34 | Faites-vous appel à des sous-traitants ? Lesquels, et pour quoi ? | Oui Non Partiel | Liste des sous-traitants |
| 35 | Vos sous-traitants sont-ils soumis aux mêmes exigences de sécurité ? | Oui Non Partiel | Clauses imposées aux sous-traitants |

## 08 · CONFORMITÉ RÉGLEMENTAIRE

| N° | Question | Réponse | Justificatif à demander |
|---|---|---|---|
| 36 | Comment prenez-vous en compte le RGPD pour nos clients européens ? | Oui Non Partiel | Description des mesures |
| 37 | Pouvez-vous répondre aux exigences NIS2 que nos clients nous imposent ? | Oui Non Partiel | Exemple de réponse à une exigence |
| 38 | Pour la Suisse ou le Québec, fournissez-vous les éléments utiles à la nLPD ou à la Loi 25 ? | Oui Non Partiel | Informations transmises |
| 39 | Acceptez-vous un audit de sécurité de notre part ou de nos clients ? | Oui Non Partiel | Clause d'audit |
| 40 | Répondez-vous aux questionnaires sécurité de nos propres clients ? | Oui Non Partiel | Exemple de questionnaire traité |

NOTATION

# La grille de notation

Attribuez 2 points pour un « oui » justifié, 1 point pour un « partiel » ou un « oui » sans justificatif, et 0 point pour un « non ». Le total est sur 80 points.

| Thème | Questions | Points max | Prestataire A | Prestataire B |
|---|---|---|---|---|
| 01 · Gouvernance et certification | 5 | 10 | | |
| 02 · Personnel et confidentialité | 5 | 10 | | |
| 03 · Gestion des accès et des identités | 6 | 12 | | |
| 04 · Traçabilité et journalisation | 4 | 8 | | |
| 05 · Gestion des incidents de sécurité | 4 | 8 | | |
| 06 · Protection des données | 5 | 10 | | |
| 07 · Continuité, réversibilité et sous-traitance | 6 | 12 | | |
| 08 · Conformité réglementaire | 5 | 10 | | |
| **Total** | **40** | **80** | | |

### Plus de 64 points

Prestataire mature : vous pouvez avancer, en reprenant ses engagements dans le contrat.

### De 48 à 64 points

Des points à clarifier : demandez un plan d'action daté avant de signer.

### Moins de 48 points

Risque élevé : le prestataire n'apporte pas les garanties nécessaires pour accéder à vos réseaux.

### Questions éliminatoires

Un « non » aux questions 01, 06, 11, 12 ou 27 devrait suffire à écarter un prestataire.

À PROPOS

# Testez-nous avec ce questionnaire.

Consup ON met à disposition des administrateurs réseaux dédiés, basés à La Marsa (Tunis), pour les MSP, ESN et infogéreurs francophones. Nos services NOC sont certifiés ISO/IEC 27001:2022, et nos équipes interviennent exclusivement via vos accès, dans vos outils.

**27001**

services NOC certifiés ISO/IEC 27001:2022 (CERT-000658, MSECB)

**1 mois**

pour remplacer un administrateur qui quitte votre compte

**24/7**

couverture possible sur demande

## Envoyez-nous votre questionnaire

Nous vous retournons nos réponses et les justificatifs disponibles.

Yacine Ouerghemi · yacine.ouerghemi@consupon.com · +33 6 52 51 39 01

consupon.com/securite-conformite