CHECKLIST IT DE SÉCURITÉ

pour cabinets d'expertise comptable

20 points à vérifier avant la prochaine période fiscale

Sauvegardes | Sécurité & accès | RGPD | Logiciels métier

Pour chaque point, cochez **OUI** si votre cabinet est conforme, **NON** sinon. Additionnez les points obtenus. Un score inférieur à **14/20** indique des vulnérabilités significatives à corriger avant la prochaine liasse fiscale.

■ 1. Sauvegardes & Continuité

1. Vos données sont sauvegardées quotidiennement Sauvegarde automatique nocturne recommandée	OUI	NON	+3
2. Vous testez la restauration au moins une fois par trimestre Un backup non testé n'est pas un backup fiable	OUI	NON	+3
3. Une copie hors-site ou cloud existe (règle 3-2-1) 3 copies, 2 supports différents, 1 hors site	OUI	NON	+3
4. Votre plan de reprise d'activité (PRA) est documenté Que se passe-t-il si votre serveur tombe le 15 avril ?	OUI	NON	+2
5. Le délai de reprise (RTO) est inférieur à 4 heures Standard pour cabinets en période fiscale	OUI	NON	+2

■ 2. Sécurité & Accès

6. L'authentification à deux facteurs (2FA) est activée Applicable à tous les comptes critiques (email, ERP, cloud)	OUI	NON	+3
7. Les accès collaborateurs sont révoqués à leur départ Un ancien employé ne doit jamais rester en base	OUI	NON	+3
8. Vos postes de travail sont à jour (OS + antivirus) Windows Update + EDR ou antivirus professionnel actif	OUI	NON	+2
9. Votre réseau Wi-Fi invité est séparé du réseau interne Un client sur votre Wi-Fi ne doit pas voir vos serveurs	OUI	NON	+2
10. Un audit de sécurité a été réalisé dans les 12 derniers mois Pentest ou scan de vulnérabilités externe	OUI	NON	+2

■ 3. Conformité RGPD

11. Votre registre des traitements est à jour Obligation RGPD Article 30 — tous les traitements de données clients	OUI	NON	+3
12. Vos sous-traitants ont signé un DPA (Data Processing Agreement) Logiciels SaaS, hébergeurs, prestataires IT inclus	OUI	NON	+3

13. Vous avez un processus de notification en cas de fuite de données
72h pour notifier la CNIL après un incident (Article 33)

OUI	NON	
		+2

14. Les données clients sont chiffrées au repos et en transit
HTTPS obligatoire + chiffrement disque recommandé

OUI	NON	
		+2

15. Vos collaborateurs ont reçu une formation RGPD de base
Le phishing est la première cause de fuite de données

OUI	NON	
		+2

■■ 4. Performance Logiciels Métier

16. Votre version de Cegid / Sage / ACD est à jour
Les mises à jour intègrent correctifs de sécurité et conformité fiscale

OUI	NON	
		+3

17. Votre infrastructure supporte la charge en période de liasse
Pic de charge janvier-avril — avez-vous testé sous stress ?

OUI	NON	
		+3

18. Vous disposez d'une assistance technique dédiée (SLA contractuel)
Un ticket "low priority" pendant la liasse peut coûter des milliers d'euros

OUI	NON	
		+2

19. Vos licences logicielles sont toutes régularisées
Un audit éditeur en période chargée est un risque réel

OUI	NON	
		+2

20. Vos accès distants (VPN, RDP) sont sécurisés et auditables
Télétravail et accès depuis l'extérieur = surface d'attaque à protéger

OUI	NON	
		+2

Interprétation de votre score

18-20 ■ Excellent	Votre cabinet est bien protégé. Maintenez ce niveau.	**14-17 ■■ Bon niveau**	Quelques points à renforcer avant la prochaine période.
10-13 ■ Risque modéré	Des vulnérabilités importantes — agissez rapidement.	**< 10 ■ Risque élevé**	Votre cabinet est exposé. Un audit urgent s'impose.

Votre score est inférieur à 14 ?

Réservez votre **audit IT gratuit de 30 minutes** avec un expert Ochyro.
Nous identifions vos vulnérabilités prioritaires avant la période fiscale.

■ ochyro.net — section Diagnostic