Les 12 points de contrôle de votre système d’information

Ce que nous vérifions chez chaque PME et ETI d’Île-de-France avant de parler de budget

Audit gratuit de 30 minutes

Guide de terrain — septembre 2026
Infogérance · Cybersécurité · Cloud privé
01 86 04 83 42 · kelly@2srk.com · 2srk.com

Contrôles 1 à 6 — le socle

1 Inventaire du parc et des logiciels

Lister postes, serveurs, systèmes et versions pour connaître le périmètre réellement supporté, et savoir ce qui n'est plus maintenu.

2 Sauvegardes réellement restaurables

Tester une restauration complète sur un environnement isolé. Une sauvegarde qui s'exécute sans erreur n'est pas une sauvegarde utilisable.

3 Règle 3-2-1 appliquée

Trois copies des données, sur deux supports différents, dont une hors site ou hors ligne. C'est ce qui protège d’un rançongiciel.

4 Comptes à privilèges maîtrisés

Administrateurs nominatifs, aucun compte partagé, revue régulière des droits, retrait immédiat des accès des personnes qui partent.

5 Double facteur sur les accès sensibles

Messagerie, VPN, consoles d’administration et applications métier : la première cause de compromission reste le mot de passe volé.

6 Accès à distance inventoriés et fermés

Bureau à distance, VPN, services exposés sur internet : les recenser, fermer ce qui ne sert pas, journaliser ce qui reste.

Contrôles 7 à 12 — la maîtrise dans le temps

7 Correctifs de sécurité suivis

Systèmes, hyperviseurs, pare-feu et applications : un plan de mise à jour avec une fenêtre de sécurité définie, pas des correctifs « quand on a le temps ».

8 Protection des postes et des mails

Antivirus ou EDR géré, filtrage des pièces jointes et de l’hameçonnage, sensibilisation des équipes : la messagerie est la première porte d’entrée.

9 Plan de reprise testé

RTO et RPO écrits, procédure connue des équipes, exercice de reprise effectué au moins une fois par an et documenté.

10 Énergie et environnement maîtrisés

Onduleurs testés, autonomie connue, température et humidité surveillées dans le local technique : la panne électrique reste la première cause d’arrêt.

11 Journalisation et supervision 24/7

Des alertes hiérarchisées qui remontent à une astreinte humaine, avec seuils définis et historique : pas une boîte mail que personne ne lit.

12 Documentation et plan d'action

Schéma d'architecture à jour, procédures, mots de passe dans un coffre, contacts d'escalade et plan d'action priorisé.

Et maintenant ?

Un seul point manquant suffit à transformer un incident en arrêt d'activité. En 30 minutes, nous passons ces 12 contrôles en revue avec vous et vous remettons les 3 risques à traiter en premier, par écrit et sans engagement.

2SRK Solutions Informatiques
4 rue de la Mare à Vinant — 77127 Lieusaint
01 86 04 83 42 · kelly@2srk.com · https://2srk.com