

Checklist arbitrage cyber pour la direction

10 questions pour préparer une décision cyber exploitable : contexte, preuve disponible, propriétaire, échéance et prochaine vérification.

Mode d'emploi

1. Réunir DSI/RSSI, métier et direction.
2. Cocher uniquement ce qui est démontrable.
3. Consigner les déclarations comme non vérifiées.
4. Choisir trois décisions maximum pour les 30 prochains jours.

Règle de preuve

Observé = constaté directement.
Déclaré non vérifié = affirmé sans preuve examinée.
Absent = élément attendu non fourni.
Non applicable = justification documentée.

Avant la réunion

- ☐ Nommer le décideur final et la décision attendue.
- ☐ Fixer le périmètre : organisation, actifs, sites et échéance.
- ☐ Interdire l'envoi de secrets, mots de passe ou données inutiles.
- ☐ Limiter la collecte initiale à dix documents et cinq entretiens.
- ☐ Définir ce qui ferait arrêter ou élargir la revue.

Questions de décision

01 — Quels services métiers provoqueraient l'impact le plus fort en cas d'indisponibilité ?

Statut : ☐ Observé ☐ Déclaré non vérifié ☐ Absent ☐ Non applicable

Décision : _____ Responsable : _____

Échéance : _____ Preuve attendue : _____

02 — Qui possède la décision de risque pour chacun de ces services ?

Statut : ☐ Observé ☐ Déclaré non vérifié ☐ Absent ☐ Non applicable

Décision : _____ Responsable : _____

Échéance : _____ Preuve attendue : _____

03 — Quels comptes ou identités conditionnent l'accès aux services critiques ?

Statut : ☐ Observé ☐ Déclaré non vérifié ☐ Absent ☐ Non applicable

Décision : _____ Responsable : _____

Échéance : _____ Preuve attendue : _____

04 — La récupération de ces comptes a-t-elle été testée et datée ?

Statut : ☐ Observé ☐ Déclaré non vérifié ☐ Absent ☐ Non applicable

Décision : _____ Responsable : _____

Échéance : _____ Preuve attendue : _____

05 — Quelles sauvegardes ont fait l'objet d'une restauration réellement observée ?

Statut : ☐ Observé ☐ Déclaré non vérifié ☐ Absent ☐ Non applicable

Décision : _____ Responsable : _____

Échéance : _____ Preuve attendue : _____

06 — Quels fournisseurs ou accès tiers peuvent interrompre l'activité ?

Statut : ☐ Observé ☐ Déclaré non vérifié ☐ Absent ☐ Non applicable

Décision : _____ Responsable : _____

Échéance : _____ Preuve attendue : _____

07 — Quels accès à privilèges sont revus, par qui et à quel rythme ?

Statut : ☐ Observé ☐ Déclaré non vérifié ☐ Absent ☐ Non applicable

Décision : _____ Responsable : _____

Échéance : _____ Preuve attendue : _____

08 — Quel incident récent a modifié une priorité ou un contrôle ?

Statut : ☐ Observé ☐ Déclaré non vérifié ☐ Absent ☐ Non applicable

Décision : _____ Responsable : _____

Échéance : _____ Preuve attendue : _____

09 — Quelles obligations ou exigences clients nécessitent une qualification séparée ?

Statut : ☐ Observé ☐ Déclaré non vérifié ☐ Absent ☐ Non applicable

Décision : _____ Responsable : _____

Échéance : _____ Preuve attendue : _____

10 — Quels trois risques exigent un arbitrage dans les 30 jours ?

Statut : ☐ Observé ☐ Déclaré non vérifié ☐ Absent ☐ Non applicable

Décision : _____ Responsable : _____

Échéance : _____ Preuve attendue : _____

Contrat de décision

Décision prioritaire	Responsable	Échéance	Preuve attendue

Plan 30 / 60 / 90 jours

30 jours : propriétaires, périmètres critiques, tests minimaux autorisés et décisions urgentes.

60 jours : traitements retenus, responsables, dépendances, échéances et preuves attendues.

90 jours : revue direction, risques résiduels, écarts non traités et prochain cycle.

Limites

Cette checklist aide à préparer un arbitrage. Elle ne réalise aucun scan, pentest, audit de certification, investigation forensique, conseil juridique ou notification réglementaire. Toute observation technique nécessite un périmètre et une autorisation explicites.