

# Contacts et communication

Fiche 1 sur 4. Complétez ces champs avec la direction, l'informatique et les équipes opérationnelles. Conservez une copie à jour dans un lieu hors ligne convenu.

Organisation / site : \_\_\_\_\_ Responsable : \_\_\_\_\_  
Version / prochaine revue : \_\_\_\_\_ Validation : \_\_\_\_\_

## Qui assume les responsabilités

| Rôle                         | Nom et suppléant | Contact vérifié et solution de secours |
|------------------------------|------------------|----------------------------------------|
| Coordination / pilotage      | _____<br>_____   | _____<br>_____                         |
| Informatique / prestataire   | _____<br>_____   | _____<br>_____                         |
| Opérations / continuité      | _____<br>_____   | _____<br>_____                         |
| Services généraux / sécurité | _____<br>_____   | _____<br>_____                         |

## Si la messagerie ou le téléphone ne fonctionne plus

Canal de secours autorisé : \_\_\_\_\_  
Si ce canal échoue aussi, lieu de rencontre convenu : \_\_\_\_\_  
Emplacement hors ligne du dossier et personnes habilitées : \_\_\_\_\_  
Dernier test de contact / résultat : \_\_\_\_\_

## Signaler et coordonner

En cas de danger immédiat, suivez les consignes de sécurité et d'évacuation du site et contactez les secours locaux si nécessaire. Sinon, signalez vos observations, l'heure, le lieu et l'activité touchée. Obtenez un accusé de réception ; sans réponse, contactez le suppléant convenu. N'improvisez aucune intervention sur les installations électriques ou les systèmes critiques pour la sécurité.

N'inscrivez ni mots de passe ni clés de récupération. Limitez la diffusion des coordonnées personnelles. Ne publiez pas les fiches remplies.

# Activités critiques et continuité

Fiche 2 sur 4. Dupliquez cette fiche pour chaque activité importante. Les durées estimées sont des hypothèses de planification à convenir et vérifier avec les responsables.

| Question de planification                                            | Décision de votre organisation |
|----------------------------------------------------------------------|--------------------------------|
| Activité et responsable                                              | <div></div> <div></div>        |
| Effets sur les clients, les personnes et les opérations              | <div></div> <div></div>        |
| Quand l'interruption devient-elle inacceptable et pourquoi           | <div></div> <div></div>        |
| Personnel, informatique, données, locaux et prestataires nécessaires | <div></div> <div></div>        |
| Service minimum et procédure de secours autorisée                    | <div></div> <div></div>        |
| Qui active le mode dégradé et qui y met fin                          | <div></div> <div></div>        |
| Objectif de reprise et conditions d'autorisation                     | <div></div> <div></div>        |

## À convenir avant le retour à la normale

Qui confirme la sécurité et la disponibilité ? Comment tester le service ? Comment rapprocher les dossiers papier et le retard accumulé sans doublons ni transactions manquantes ?

Disposer d'une sauvegarde ne garantit pas la reprise. L'informatique et les opérations doivent vérifier séparément les besoins en données, les dépendances et les possibilités de reprise testées.

# Un exercice d'équipe de 30 minutes

Fiche 3 sur 4. Exercice de discussion avec des informations fictives. N'arrêtez aucun système, ne déclenchez aucune alerte réelle et n'utilisez aucune donnée client. Un incident réel met fin à l'exercice.

Date : \_\_\_\_\_ Animation : \_\_\_\_\_ Prise de notes : \_\_\_\_\_

Participants / rôles : \_\_\_\_\_

| Temps     | Situation et questions                                                                                                                                                                                                                      |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0-5 min   | Convenir de l'objectif : tester les contacts et une activité critique. Attribuer les rôles et confirmer les règles de l'exercice.                                                                                                           |
| 5-15 min  | 09 h 10 : panne électrique sur le site. Le progiciel de gestion et les téléphones fixes sont indisponibles. La cause est inconnue. Qui vérifie la sécurité ? Qui coordonne ? Comment joindre le suppléant sans courriel ?                   |
| 15-25 min | 09 h 30 : aucun délai de rétablissement fiable ; le réseau mobile est instable. Une commande client importante est attendue. Quelle procédure de secours est autorisée ? Qu'est-ce qui est suspendu ? Qui communique avec qui, et comment ? |
| 25-30 min | Noter les trois lacunes principales. Attribuer à chacune un responsable, une échéance et une preuve de réalisation observable.                                                                                                              |

## Consigner les observations

| Question / décision | Observation ou lacune non résolue |
|---------------------|-----------------------------------|
| _____               | _____<br>_____                    |
| _____               | _____<br>_____                    |

Pour explorer des scénarios cyber, utilisez le générateur d'exercices sur table CyberDecisionLab. Choisissez un scénario adapté ; les questions et notes de cette fiche ne sont pas transférées automatiquement.

[Générateur d'exercices sur table](#)

# Actions et prochaine revue

Fiche 4 sur 4. Terminez l'exercice en consignant les résultats et en attribuant les prochaines étapes. Vérifiez ensuite la mise en œuvre des actions.

| Lacune et action                             | Responsable / échéance            | Preuve / statut                   |
|----------------------------------------------|-----------------------------------|-----------------------------------|
| <div><div></div><div></div><div></div></div> | <div><div></div><div></div></div> | <div><div></div><div></div></div> |
| <div><div></div><div></div><div></div></div> | <div><div></div><div></div></div> | <div><div></div><div></div></div> |
| <div><div></div><div></div><div></div></div> | <div><div></div><div></div></div> | <div><div></div><div></div></div> |

Date de suivi des actions :   
Personne vérifiant la réalisation :   
Prochain exercice et thème :

## Tenir le dossier à jour

Après un changement ou un incident, vérifiez les contacts, les canaux de secours et les activités. Convenez d'une date de revue interne régulière. Remplacez les copies hors ligne périmées. Ne clôturez une action qu'avec une preuve, par exemple un test de contact consigné.

## Utilisation et sources

Ces modèles originaux de Paragamix GmbH peuvent être utilisés en interne, adaptés et partagés gratuitement avec les clients. Un lien vers la source est apprécié, sans être obligatoire. Les ressources externes conservent leurs propres conditions.

[BSI sur l'organisation face aux incidents \(allemand\)](#) | [CISA sur les exercices sur table \(anglais\)](#)

### Version actuelle et sources

Point de départ pour la préparation organisationnelle. Ni plan de continuité complet, ni autorisation technique, ni certificat de conformité. Créé avec l'aide de l'IA ; aucune validation indépendante par un expert n'est revendiquée. Faites examiner et approuver ce kit par les responsables avant toute utilisation opérationnelle.