

Annexe 6 – Plan de reprise en cas de désastre

Commented [AES1]: Pour en savoir plus sur les Plans de reprise en cas de désastre, consultez cet article :

Disaster recovery vs Business continuity
<https://advisera.com/27001academy/blog/2010/11/04/disaster-recovery-vs-business-continuity/>

Historique des modifications

Date	Version	Créé par	Description de la modification
	0.1	Advisera	Structure documentaire de base

Table des matières

- 1. BUT, DOMAINE D'APPLICATION ET UTILISATEURS.....2
- 2. DOCUMENTS REFERENCES2
- 3. HYPOTHESES / RESTRICTIONS.....2
- 4. INFORMATIONS GENERALES.....2
- 5. FONCTIONS ET COORDONNEES.....3
- 6. AUTORISATIONS EN SITUATION DE CRISE4
- 7. RESSOURCES NECESSAIRES.....5
- 8. ETAPES DE REPRISE RELATIVE AUX INFRASTRUCTURES ET SERVICES INFORMATIQUES.....6
- 9. GESTION DES ENREGISTREMENTS CONSERVES SUR LA BASE DE CE DOCUMENT6
- 10. VALIDITE ET GESTION DOCUMENTAIRE.....7
- 11. DOCUMENTS COMPLEMENTAIRES7

1. But, domaine d'application et utilisateurs

Le Plan de reprise en cas de désastre a pour but de définir précisément la manière dont [nom de l'organisation] récupérera ses infrastructures et service informatiques, dans les délais fixés, en cas de désastre ou de tout autre incident perturbateur. L'objectif de ce Plan est de finaliser le rétablissement des infrastructures et services informatiques dans le cadre de l'objectif de temps de reprise (RTO) définis.

Ce Plan comprend toutes les ressources et processus nécessaires à la reprise,

Les utilisateurs de ce document sont les membres de l'Equipe de gestion de crise et les employés nécessaires à la reprise de cette activité.

Commented [AES2]: Ce Plan est rédigé pour les organisations où le rétablissement des infrastructures et systèmes informatiques peut être insérée dans un plan unique.

Pour les organisations disposant d'infrastructures informatiques complexes, ou de RTO et RPO différents pour différents systèmes, il serait préférable de développer des Plans de reprise en cas de désastre distincts pour différents systèmes informatiques.

2. Documents référencés

- Norme ISO/IEC 27001, clauses 7.4, A.5.29, A.5.30 et A.8.14
- Norme ISO 22301, clause 8.4.5
- Liste des exigences légales, réglementaires, contractuelles et autres
- [Procédure de gestion des incidents]
- [Procédure d'audit interne]

Commented [AES3]: Si vous ne disposez pas de cette Liste, alors énumérez dans ces crochets toutes les obligations légales et contractuelles relatives au contrôle d'accès.

Commented [AES4]: Vous pouvez consulter un modèle pour ce document dans le dossier "12_Audit_interne" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

3. Hypothèses / restrictions

Pour que ce Plan fonctionne, les conditions suivantes doivent être remplies :

- Tous les équipements, logiciels et toutes les données sont disponibles comme prévu dans la Stratégie de continuité des activités.

Commented [AES5]: Vous pouvez également ajouter d'autres conditions.

Ce Plan ne couvre pas les types d'incidents suivants :

- []

Commented [AES6]: Vous pouvez indiquer ici certains incidents.

Commented [AES8]: Copiez de la Stratégie de continuité des activités.

Commented [AES7]: Pour en savoir plus sur ce sujet, consultez cet article :

Commented [AES9]: Copiez de la Stratégie de continuité des activités.

4. Informations générales

Emplacement du site alternatif / Stratégie de reprise :	[]
Objectif de temps de	[]

reprise :	
Personne responsable de l'activation de Plan de reprise en cas de désastre / Personne d'urgence :	[Redacted]
Personne qui valide les copies de l'activation de Plan de reprise / Personne d'urgence :	[Redacted]
Personne responsable de la distribution de Plan de reprise en cas de désastre / Personne d'urgence / Personne :	[Redacted]
Tâches clés / obligations / SLA qui doivent être respectés et délais respectifs :	
Capacité minimum nécessaire immédiatement après le désastre (OMCA – objectifs minimaux de continuité des activités) :	
Délai après lequel le niveau opérationnel normal doit reprendre :	

Commented [AES11]: Personne définie dans la partie principale

Commented [AES10]: Pour en savoir plus sur ce sujet, consultez cet article :

Commented [AES12]: Habituellement tous les employés du

Commented [AES13]: Habituellement le chef de service des

Commented [AES14]: Habituellement le chef de service des

Commented [AES15]: Le critère habituel consiste à déterminer

Commented [AES16]: Copiez de la stratégie du département informatique.

Commented [AES18]: Par ex. 20 % des utilisateurs doivent

Commented [AES17]: Copiez du Questionnaire du Bilan d'impact sur les activités.

Commented [AES19]: Copiez du Questionnaire du Bilan d'impact sur les activités.

5. Fonctions et coordonnées

Pour le service des technologies de l'information :

N.	Fonction dans la reprise	Nom	Adresse du domicile	N. du substitut
1.	Récupération de la base de données	Paul Martin	Rue ABC, n° 123, code postal 5678	2
2.	Récupération	Jeanne	Rue XYZ, n°	

Commented [AES20]: Pour en savoir plus sur ce sujet, consultez cet article :

Commented [AES21]: Si vous n'utilisez pas de téléphones

Commented [AES22]: Désigner la personne qui agira en tant

Commented [AES23]: Il ne s'agit que d'exemples ; modifiez ces

[nom de l'organisation]

[niveau de confidentialité]

	tion des applicati ons	Dupon					789, code postal 1432
3.							
4.							
5.							

Autres activités au sein de l'organisation :

N.	Nom	Titre du poste / unité organisationnelle				N. du substitut
11.						
12.						
13.						
14.						
15.						

Commented [AES24]: C'est-à-dire les services commerciaux de l'organisation.

Contacts externes :

N.	Nom de l'organisation	Nom				E-mail	N. du substitut
21.							
22.							
23.							
24.							
25.							

Commented [AES25]: Assurez-vous d'indiquer les informations concernant :

- les opérateurs de télécommunications
- les fournisseurs de matériels

Indiquer également tous les autres fournisseurs, partenaires d'externalisation, agences gouvernementales, clients, etc. nécessaires.

6. Autorisations en situation de crise

Fonction dans la reprise / titre du poste	Autorisations
Chef du service des technologies de l'information	Autorisé à prendre toutes les mesures indiquées dans le Plan de continuité des activités et dans le Plan de reprise en cas de désastre afin de rétablir les infrastructures / services informatiques
...	

Commented [AES26]: Pour remplir ce tableau, copiez les

Commented [AES27]: Par ex. Responsable des achats

Commented [AES28]: Ex : PDG, Responsable mercatique

Commented [AES29]: Par ex. Responsable continuité d'activité,

Commented [AES30]: Par ex. administrateur du système

Commented [AES31]: Enumérez toutes les autres autorisations

Remarque : Seul [titre du poste] est autorisé à communiquer avec le public à travers les médias publics.

Commented [AES32]: Habituellement quelqu'un de l'Equipe de gestion de crise.

7. Ressources nécessaires

Les ressources suivantes seront utilisées pour la reprise de cette activité :

Nom de la ressource	Description	Quantité	A quel moment la ressource est nécessaire	Personne chargée d'obtenir la ressource
<i>Personnes :</i>				
<i>Applications / bases de données :</i>				
<i>Données sous forme électronique :</i>				
<i>Données sous forme papier :</i>				
<i>Equipements informatiques et de communication :</i>				
<i>Canaux de communication :</i>				
<i>Autres équipements :</i>				

Commented [AES33]: Pour remplir ce tableau, copiez les

Commented [AES34]: Décrire où sont situées les ressources,

Commented [AES35]: Indiquer dans cette colonne la personne

Commented [AES36]: Enumérez notamment toutes les

Installations et infrastructures :				
Services externes :				

8. Etapes de reprise relative aux infrastructures et services informatiques

Les informations dans cette section définissent les actions visant à la mise en œuvre de solutions pour la reprise de l'infrastructure / des services informatiques.

La reprise de cette activité doit respecter les étapes suivantes :

Procédures de reprise (étapes principales / tâches individuelles)	Personnes responsables de la mise en œuvre		
[nom de l'étape n. 1]			
[tâche n. 1.1]			
[tâche n. 1.2]			
...			
[nom de l'étape n. 2]			
[tâche n. 2.1]			
[tâche n. 2.2]			
...			

9. Gestion des enregistrements conservés sur la base de ce document

Nom de l'enregistrement	Lieu de conservation	Responsable de la conservation	Responsable de la destruction des enregistrements	Temps de rétention
Enregistrement de la mise en œuvre	Archive de [titre]	[nom de l'utilisateur]	[nom de l'utilisateur]	3 ans

Commented [AES37]: Assurez-vous d'énumérer tous les

Commented [AES38]: Pour en savoir plus sur ce sujet, consultez cet article :

Commented [AES39]: La communication est habituellement réalisée par :

- d'autres activités / services
- l'Equipe de gestion de crise

La communication comprend habituellement :

- la notification qu'une étape a été mise en œuvre

Commented [AES40]: Remplir cette colonne uniquement dans

Commented [AES41]: Ces étapes doivent prendre en compte les différentes stratégies que vous avez définies – par ex. les étapes seront différentes si la stratégie consiste à déplacer l'ensemble du centre de données vers un site alternatif ; si la stratégie consiste à rediriger les opérations vers un fournisseur de sauvegarde ; ou si la stratégie consiste à travailler avec une capacité plus faible.

En fonction de votre infrastructure informatique, vous pouvez diviser votre Plan en plusieurs paragraphes qui traiteront par exemple :

- du plan de reprise des ordinateurs

Par exemple, pour le plan de reprise des ordinateurs, vos étapes pourraient être les suivantes (vous devez ajouter plus de tâches détaillées pour chacune de ces étapes) :

- 1) Les utilisateurs doivent avertir [votre coordinateur] concernant les postes de travail nécessaires
- 2) [votre coordinateur] crée une liste de tous les ordinateurs et autres équipements avec la configuration nécessaire

Les étapes de reprise doivent notamment comprendre les points suivants :

- Rassembler l'équipe sur le site alternatif et décider de la manière dont les personnes indisponibles seront remplacées

Commented [AES42]: Modifiez ces enregistrements pour les faire correspondre aux pratiques de votre organisation.

Commented [AES43]: Adaptez la durée dans cette colonne à

[nom de l'organisation]

[niveau de confidentialité]

de l'étape de reprise (enregistrement sous forme papier)	du poste]			
--	-----------	--	--	--

Commented [AES44]: Habituellement le Coordinateur de la

Seul [titre du poste] peut autoriser l'accès aux enregistrements à d'autres employés.

10. Validité et gestion documentaire

Ce document est valide à compter du [date].

Ce document, ainsi que tous les documents complémentaires, sont conservés de la façon suivante :

- la forme papier du document est conservée dans les lieux suivants : Centre de commandement, [énumérez les emplacements]

Commented [AES45]: Ils sont généralement conservés sur le

- le format électronique du document est conservé de la manière suivante: [énumérez les emplacements]

Commented [AES46]: Conserver les documents de façon à ne

La responsabilité de ce document est définie de manière que tout employé de la [organisation] puisse le documenter en vertu de [référence à la politique]

Commented [AES47]: Il ne s'agit que d'une recommandation ;

Lors de l'évaluation de l'efficacité et de la pertinence de ce document, les critères suivants doivent être considérés :

- le nombre d'actions correctives fondées sur des exercices menés
- le nombre d'actions correctives fondées sur la mise en œuvre d'un plan de reprise de site
- la fréquence de mise à jour et la manière dont le contenu de l'annexe est tenu à jour

11. Documents complémentaires

- [documentation technique relative aux systèmes TIC]

Commented [AES48]: Si une telle documentation est

- [énumérez les documents]

Commented [AES49]: Si les consignes de travail existantes, du

[titre du poste]

[nom]

[signature]

Commented [AES50]: Nécessaire uniquement si la Procédure pour le contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.