

Stratégie de sauvegarde, de restauration et de reconstruction

Modèle de référence — version marque blanche

Publié par Plan R (plan-r.org) sous licence Creative Commons BY-NC-SA 4.0. Version 1.0 — 2026. Ce modèle est un point de départ : il ne dispense ni d'une analyse d'impact propre à l'organisation, ni d'une validation par ses instances.

Fiche de contrôle du document

Caractéristiques

Rubrique	Valeur
Identification	{{CODE_DOCUMENT}} — Stratégie de sauvegarde, de restauration et de reconstruction
Objet	Cadre de gouvernance, d'engagements de service et de maîtrise des activités de sauvegarde, restauration et reconstruction du SI
Version	{{VERSION}}
Classification	{{NIVEAU_DE_DIFFUSION}} (ex. Interne — Diffusion restreinte)
État	☐ Travail ☐ En attente de validation ☐ Validé
Document parent	Politique de Sécurité des Systèmes d'Information (PSSI) de {{ORGANISATION}}
Documents liés	Politique de sauvegarde · Analyse d'impact sur l'activité (BIA) · Stratégie de continuité et de reprise · Plan de Continuité Informatique (PCI) · Plan de Continuité d'Activité (PCA) · Plan de gestion de crise · Conventions de service

Historique des versions

Version	Date	Rédacteur	Modification
{{0.1}}	{{JJ/MM/AAAA}}	{{FONCTION_REDACTEUR}}	Création du document

Validation

	{{FONCTION_VALIDEUR_1}} (ex. RSSI)	{{FONCTION_VALIDEUR_2}} (ex. DSI)
Nom		
Date et signature		

Mode d'emploi du modèle

Ce document est un modèle générique. Il a été conçu pour être adapté à toute organisation disposant d'un système d'information réparti sur un ou plusieurs sites d'hébergement, avec ou sans recours à des prestataires et à des services cloud.

Conventions de personnalisation

Marqueur	Signification	Action attendue
{{ORGANISATION}}	Nom de l'organisation	Remplacer partout

Marqueur	Signification	Action attendue
{{SITE_A}}, {{SITE_B}}...	Sites d'hébergement (centres de données, salles, hébergeur)	Remplacer ; ajouter ou supprimer selon l'architecture retenue au §8.1
{{PRESTATAIRE_COFFRE}}	Prestataire du coffre de sauvegardes isolé	Remplacer ou supprimer si le coffre est interne
{{OUTIL_ITSM}}	Outil de gestion des tickets et incidents	Remplacer
{{INSTANCE_...}}	Comité ou instance de gouvernance	Faire correspondre à la comitologie existante
[À VALIDER]	Valeur proposée par défaut, cohérente avec les pratiques du marché	Confirmer ou ajuster avec les métiers
[À COMPLÉTER]	Élément propre à l'organisation, non déductible du modèle	Produire le contenu

Ordre d'adaptation recommandé

1. Partir de l'analyse d'impact sur l'activité (BIA) : activités prioritaires, dépendances, durées d'interruption tolérables (§5.2, §9.1). Si elle n'existe pas, la conduire d'abord : sans elle, les engagements sont fixés à l'aveugle.
2. Cartographier les sites, les environnements et les prestataires (§5.8, §8).
3. Faire valider par les métiers les engagements DMIA / PDMA (§9.1) — c'est le socle de tout le reste.
4. Renseigner l'affectation des rôles (Annexe B) et raccorder la comitologie aux instances existantes (§7.3), y compris la cellule de crise (§8.4).
5. Produire le plan de sauvegarde détaillé (§9.3) à partir de l'existant, puis mesurer l'écart.
6. Construire la table de correspondance avec la PSSI et les référentiels (§4.3).

Synthèse exécutive

Axe	Ce que la stratégie impose
Finalité	Réduire et borner l'indisponibilité des données et applications métier en cas d'incident, de cyberattaque ou de sinistre.
Socle commun	Une Offre Générale de Sauvegarde (OGS) s'applique par défaut à toutes les données du SI. Les Offres Spécifiques (OSS) ne peuvent que la renforcer, jamais la réduire.
Engagements	DMIA et PDMA, engagements de la DSI dérivés de l'analyse d'impact, fixés par scénario d'indisponibilité, par contexte (PROD / Hors PROD) et, le cas échéant, par classe de criticité — voir §9.1.
Scénarios couverts	Fonctionnement nominal dégradé, Indisponibilité Logique Partielle (ILP), Indisponibilité Physique Partielle (IPP), Indisponibilité Logique Globale (ILG — dont rançongiciel), Indisponibilité Physique Globale (IPG). Le sinistre total est hors périmètre.
Résilience cyber	Au moins une copie immuable et isolée des sauvegardes (règle 3-2-1-1-0), plan d'administration des sauvegardes séparé, capacité de reconstruction des socles techniques (annuaire, DNS, sauvegarde elle-même).
Preuve d'efficacité	Restaurations « témoin » quotidiennes, exercices annuels validés par les métiers, contrôle mensuel par échantillonnage, audit annuel.
Gouvernance	10 rôles dont les propriétaires métier, RACI par activité, comitologie à trois niveaux (stratégique, tactique, opérationnel) raccordée à la cellule de crise, indicateurs IGO / IGT / IGS.
Risques majeurs de mise en œuvre	Retard de validation, défaut de suivi des incidents de sauvegarde, sécurisation pilotée par la technique plutôt que par le besoin métier (criticité 9/9 — voir §11.1).

Décisions attendues de la direction lors de l'adoption

#	Décision	Impact	Urgence
1	Valider les engagements DMIA / PDMA de l'OGS	Dimensionne l'infrastructure et le budget	Haute
2	Désigner le propriétaire de la stratégie (rôle RPCI)	Conditionne l'animation de toute la gouvernance	Haute
3	Arbitrer le niveau d'isolation des sauvegardes (coffre interne ou prestataire)	Conditionne la survie au scénario ILG	Haute
4	Accepter formellement le risque résiduel exclu du périmètre (sinistre total, §6.3.1)	Engage la direction sur ce que la stratégie ne couvre pas	Haute
5	Fixer l'échéance d'application	Cadence le plan d'action	Moyenne

Table des matières

1. Conventions
2. La stratégie en huit actions
3. Préambule
4. Introduction
5. Définitions, concepts et notions
6. Périmètres et limites
7. Gouvernance
8. Modélisation des indisponibilités
9. Offre Générale de Sauvegarde
10. Offres Spécifiques de Sauvegarde
11. Maîtrise des activités de sécurisation
12. Annexes

1. Conventions

Conventions typographiques

Mise en forme	Usage
<i>Texte en italique</i>	Exemple illustrant une définition ou enrichissant une explication
Texte en gras	Notion essentielle du paragraphe
> Bloc de citation	Règle ou principe à retenir
⚠ Point d'attention	Risque ou limite à connaître

Conventions terminologiques

Terme	Signification dans ce document
Sauvegarde	Sauf précision contraire : sauvegardes, restaurations et reconstruction
PROD	Environnements de production, de formation et d'infrastructure
Hors PROD	Tous les autres environnements
Métiers	Directions utilisatrices, propriétaires des données
DMIA / PDMA	Durée Maximale d'Interruption Admissible (RTO) / Perte de Données Maximale Admissible (RPO)

2. La stratégie en huit actions

La stratégie de sauvegarde a pour objectif de soutenir l'activité en réduisant et en limitant les indisponibilités des données et des applications métier en cas d'incident ou de sinistre. Elle se compose de huit actions :

#	Action	Chapitre
1	Partager des définitions, concepts et notions communs	\$5
2	Déterminer la gouvernance des activités de sécurisation	\$7
3	Modéliser les scénarios d'indisponibilité, en généralisant les dispositifs de haute disponibilité	\$8
4	Structurer une Offre Générale de Sauvegarde (OGS) , applicable par défaut à toutes les données du SI	\$9
5	Élaborer des Offres Spécifiques de Sauvegarde (OSS), complémentaires de l'OGS	\$10
6	Mettre en œuvre les moyens de restauration et de reconstruction induits par les sauvegardes	\$9.3, \$9.4
7	Éprouver régulièrement les dispositifs de sécurisation	\$9.2
8	Veiller à la maîtrise des activités de sécurisation	\$11

- **La gouvernance** précise les rôles et les responsabilités afin de les implanter dans l'organisation et de définir la comitologie.
- **L'OGS** est un ensemble de méthodes et de procédures appliqué à tout le SI, s'appuyant sur une infrastructure type, qui garantit un niveau de sécurisation standard, homogène et cohérent.
- **Les OSS** prennent la forme d'annexes aux conventions de service. Elles ne peuvent ni réduire le niveau de l'OGS, ni la rendre incohérente. La convention de service type est hors du périmètre de la présente version.
- **La maîtrise** repose sur un reporting alimenté par le suivi et le contrôle d'indicateurs, indispensable pour apprécier les risques et les réduire.

3. Préambule

Ce document s'intitule « Stratégie de sauvegarde, de restauration et de reconstruction » parce qu'il couvre :

- les besoins de sauvegarde de **{{ORGANISATION}}** ;
- les moyens de restauration et de reconstruction à mobiliser en cas de besoin.

Cette stratégie a vocation à être **appliquée** à l'ensemble du système d'information de **{{ORGANISATION}}** **au plus tard le** **{{ÉCHÉANCE}}**.

Elle a pour objectifs :

- de cadrer la gouvernance et les méthodes à installer au sein de **{{ORGANISATION}}**, sous la responsabilité de **{{FONCTION_PROPRIETAIRE}}** **[À COMPLÉTER]** ;
- de fournir les cibles des solutions opérationnelles aux entités opérationnelles et aux partenaires ;
- de s'aligner avec la stratégie de continuité et de reprise de **{{ORGANISATION}}** (et du groupe, le cas échéant).

Elle répond aux exigences de continuité métier sur la base de la synthèse des risques à couvrir, et notamment des causes d'**Indisponibilité Logique** suivantes :

Cause	Origine	Description
Erreur de manipulation	Humaine	Certaines commandes ont des effets irréversibles sur la validité des données, applicatives ou système.
Malveillance interne	Humaine	Certaines commandes peuvent altérer les données de façon immédiate et irréversible. Les motifs sont multiples : ressentiment, détresse, départ contraint, corruption, menace.
Infection et chiffrement malveillant	Humaine (externe)	Un logiciel malveillant, notamment un rançongiciel, se propage sur le réseau des serveurs et détruit ou chiffre les données. Selon l'attaque, la reconstruction complète d'un grand nombre de serveurs peut devenir nécessaire, y compris celle de l'infrastructure de sauvegarde elle-même.
Accident	Technique	Un défaut de microcode ou un incident de réplication peut propager une corruption et créer un désastre logique.

Elle prend également en compte les conséquences de la **destruction physique** des supports de stockage, dans les cas définis par la politique de sauvegarde.

4. Introduction

4.1 Une stratégie, pour quoi faire ?

La stratégie de sauvegarde décline le volet « sauvegarde » de la **PSSI**. Elle construit un objectif cohérent en appliquant des **méthodes** homogènes, elles-mêmes déclinées en **procédures d'exploitation de sécurité** rationnelles.

La **démarche** consiste à **identifier les besoins** métiers, pour **définir les engagements** à tenir et les **procédures d'exploitation de sécurité** à mettre en œuvre.



Sa formalisation doit permettre :

- d'identifier les procédures d'exploitation de sécurité nécessaires et suffisantes ;
- d'identifier et d'adapter celles déjà en place ;
- de supprimer celles devenues obsolètes.

4.2 Ce que la stratégie ne traite pas

La stratégie ne spécifie ni les procédures opérationnelles, ni les outils d'orchestration. Ces deux points relèvent des structures opérationnelles, sur la base d'un plan d'action construit en comparant la sécurisation existante aux règles de la présente stratégie (analyse d'écart).

4.3 Correspondance avec la PSSI et les référentiels

[À COMPLÉTER] — La colonne « Règle PSSI » est à renseigner avec les identifiants de la PSSI de **{{ORGANISATION}}**. Les colonnes « référentiels » sont fournies à titre indicatif et doivent être vérifiées contre la version en vigueur de chaque texte.

Exigence	Règle PSSI	Chapitre de la stratégie	ISO 22301:2019	ISO/IEC 27001:2022 (Annexe A)	NIST CSF 2.0	Textes réglementaires (si applicables)
Analyse d'impact et objectifs de reprise	{{...}}	\$5.2, \$9.1	8.2	5.30	ID.RA, RC.RP	DORA art. 11 · NIS 2 art. 21 §2 c)
Sauvegarde des informations	{{...}}	\$5.10 à \$5.14, \$9.3	8.3	8.13	PR.DS-11	NIS 2 art. 21 §2 c) · DORA art. 12
Préparation des TIC à la continuité	{{...}}	\$8, \$9.1, \$9.4	8.3, 8.4	5.30	RC.RP	NIS 2 art. 21 §2 c) · DORA art. 11
Tests de restauration et exercices	{{...}}	\$9.2	8.5	8.13, 5.30	PR.DS-11, RC.RP	DORA art. 11 et 12
Rôles et responsabilités	{{...}}	\$7.1, \$7.2	5.3	5.2	GV.RR	—
Gestion des incidents et de crise	{{...}}	\$7.4, \$8.4, \$9.5	8.4	5.24 à 5.27	RS.MA	NIS 2 art. 23 · DORA art. 17 à 19
Relations avec les fournisseurs	{{...}}	\$8.8	8.3, 8.6	5.19 à 5.22	GV.SC	DORA art. 28 à 30
Protection des sauvegardes (confidentialité)	{{...}}	\$5.6, \$9.3	—	8.24, 8.13	PR.DS-01	—

Exigence	Règle PSSI	Chapitre de la stratégie	ISO 22301:2019	ISO/IEC 27001:2022 (Annexe A)	NIST CSF 2.0	Textes réglementaires (si applicables)
Conservation et suppression	{{...}}	§5.13, §6.2.4	—	5.33, 8.10	—	RGPD art. 5 §1 e)
Disponibilité de la documentation	{{...}}	§7.6	7.5	5.37	—	—
Surveillance, audit et revue de direction	{{...}}	§7.5, §11	9.1 à 9.3	5.35, 5.36	GV.OV, ID.IM	—

⚠ Les numéros de clauses d'ISO 22301 renvoient à l'édition 2019, en cours de révision : à vérifier contre l'édition en vigueur lors de l'adaptation. La colonne ISO 22301 est utile même sans système de management de la continuité certifié ; elle montre où la stratégie s'insère dans la démarche de continuité.

5. Définitions, concepts et notions

L'ensemble des définitions, concepts et notions exposés ci-dessous **est nécessaire** à l'établissement de la stratégie et requiert **une acceptation commune** de tous les intervenants participant à **sa mise en œuvre**.

5.1 Classification des types de données

Cette classification :

- est cohérente avec la cinématique de sauvegarde / restauration décrite en Annexe A ;
- ne doit pas être confondue avec la classification DICP des données (§5.3) ;
- sert à ajuster le niveau de sécurisation à appliquer aux données.

Elle s'appuie sur trois axes :

Axe	Valeur	Définition
Niveau de support	Primaire	Support où réside la donnée elle-même, et non une copie. Généralement des disques, parfois des bandes.
	Secondaire	Support portant une copie ou une image de la donnée à un instant <i>t</i> . Tout type de support est possible (disque, bande, stockage objet...).
Accessibilité	En ligne	La donnée est lisible ou modifiable sans intervention sur le support.
	Hors ligne	Une intervention est nécessaire pour lire la donnée (récupération de cartouches, montage de disques...).
Évolutivité	Évolutive	La donnée peut être modifiée après sa création.
	Stable	La donnée est figée.

Ces axes permettent de distinguer deux grandes familles.

Données vivantes — stockées sur des supports primaires :

- **Actives** : leur valeur évolue ou peut évoluer. Leur sécurisation exige des sauvegardes régulières dont la fréquence répond au besoin métier.
- **Historiques** : leur valeur n'évolue plus. Elles peuvent représenter une part importante du stockage primaire. Une sauvegarde unique suffit à les sécuriser ; les identifier permet de **réduire fortement le volume à sauvegarder régulièrement**.
- **Archivées** : extraites des supports primaires pour des raisons légales, fiscales ou juridiques. Leur stockage est distinct et isolé des autres données vivantes. Leur inaltérabilité et leur lisibilité doivent être garanties pendant toute la durée de conservation. Les supports d'archive sont consultables, non réinscriptibles. **La PDMA de ces données est égale à 0**. Elles ne figurent plus sur les supports primaires d'origine.
 -  Une donnée stockée parmi des données actives ou historiques accessibles depuis une application **n'est pas archivée**, en raison du risque d'effacement ou de modification.
 - L'accès à une donnée archivée passe par une demande contrôlée de « mise à disposition » et par une procédure de gestion de son obsolescence encadrant sa suppression.

Données mortes — sauvegardes des données vivantes, stockées sur des supports secondaires :

- **Synchrones** : images évoluant en phase avec les données vivantes. Elles permettent une remise à disposition en cas de perte du support primaire.  Elles répliquent aussi les corruptions et les chiffréments malveillants : elles ne protègent pas contre une indisponibilité logique.

- **Asynchrones** : copies figées à un instant *t*. Elles permettent de revenir à un état antérieur pour annuler les effets d'un incident technique ou d'un dysfonctionnement applicatif.
- **Isolées** : copies de sauvegardes (« sauvegarde de la sauvegarde ») et sauvegardes des archives, **logiquement et/ou physiquement isolées et non modifiables**. Elles constituent le dernier recours en cas de perte majeure des données et de leurs sauvegardes primaires, et garantissent la PDMA des archives.

Type	Support	Accessibilité	Évolutivité	Durée de vie	Usage	Exemples
Actives	Primaire	Oui	Oui	Courte	Activité métier quotidienne	Bases applicatives, bureautique, systèmes d'exploitation, flux entrants et sortants
Historiques	Primaire	Oui	Non	Moyenne	Activité métier quotidienne	Bilans de projet, enregistrements au sens ISO 27001, journaux
Archivées	Primaire	Sous contrôle	Non	Longue	Obligation légale, juridique, fiscale	Contrats clos, bilans comptables
Mortes synchrones	Secondaire	Oui	Oui	Courte	Incidents immédiatement détectés (perte matérielle)	Réplicas des données actives et historiques
Mortes asynchrones	Secondaire	Oui	Non	Moyenne	Incidents et dysfonctionnements applicatifs	Sauvegardes des données actives et historiques
Mortes isolées	Secondaire	Sous contrôle	Non	Longue	Dernier recours	Copies externalisées et immuables, sauvegardes des archives

Règles de cardinalité

- Une donnée active ou historique peut générer une ou plusieurs données mortes.
- Une donnée morte est associée à une seule donnée active ou historique.

Sauvegarde ≠ archivage. La sauvegarde produit des copies temporaires destinées à la restauration ; l'archivage déplace la donnée vers un support dédié pour répondre à une obligation de conservation.

5.2 DMIA et PDMA

Sens retenu dans ce document. La DMIA et la PDMA sont ici des **engagements de la DSI** : l'équivalent du RTO et du RPO informatiques. Elles se déduisent des besoins exprimés dans l'analyse d'impact sur l'activité (BIA), selon la chaîne suivante :

Délai	Fixé par	Définition	Relation
Durée d'interruption maximale tolérable (MTPD)	Métier, par la BIA	Délai au-delà duquel les conséquences de l'interruption deviennent inacceptables pour {{ORGANISATION}}	Borne supérieure
Objectif de reprise de l'activité (RTO métier)	Métier	Délai visé pour reprendre l'activité, au moins à son niveau minimal (MBCO)	≤ MTPD
DMIA (engagement de restauration informatique)	DSI, dans la présente stratégie	Délai de retour des données et applications	≤ RTO métier – délai de reprise métier (ressaisie, contrôles, rattrapage)
Perte de données tolérable	Métier, par la BIA	Volume ou ancienneté des données dont la perte reste acceptable	Borne supérieure
PDMA (engagement de point de restauration)	DSI, dans la présente stratégie	Ancienneté maximale des données restituées	≤ perte tolérable

⚠ En France, le sigle DMIA est aussi employé au sens de durée *tolérable* (c'est le cas du lexique du Club de la continuité d'activité). Toute organisation qui adopte ce modèle doit vérifier le sens donné au sigle par ses métiers et par sa BIA, et l'écrire : un même sigle recouvrant deux délais différents produit des engagements intenables.

La DMIA (Durée Maximale d'Interruption Admissible) — engagement de la DSI, équivalent du RTO, *Recovery Time Objective* informatique :

- temps maximal pendant lequel les données peuvent rester inaccessibles suite à l'indisponibilité d'une ressource du SI (serveur, réseau, poste, application) ;
- définie à l'avance, à partir de l'analyse d'impact et des besoins de production de **{{ORGANISATION}}**.

Pour la tenir, il faut :

- détecter l'incident grave le plus tôt possible ;
- décider rapidement du déclenchement du plan de secours ;
- disposer de sauvegardes permettant un redémarrage rapide.

La PDMA (Perte de Données Maximale Admissible) — engagement de la DSI, équivalent du RPO, *Recovery Point Objective* informatique :

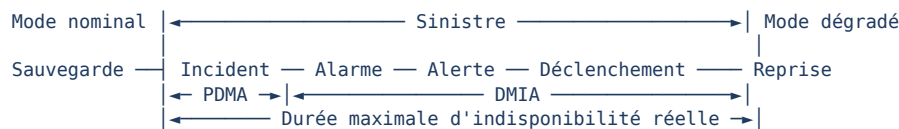
- fixe les objectifs de sauvegarde, qui dépendent de la volumétrie et des fenêtres de sauvegarde.

Pour la tenir, il faut :

- disposer des sauvegardes les plus récentes possibles ;
- pouvoir recharger ces données dans un délai compatible avec la DMIA.

Durée maximale d'indisponibilité réelle d'une donnée. Après un sinistre, elle s'apprécie en combinant DMIA et PDMA. Elle correspond au cumul de six phases :

#	Phase	Borne de début	Borne de fin	Rattachement
1	Âge de la sauvegarde	Dernière sauvegarde valide	Incident	PDMA
2	Détection	Incident	Alarme	DMIA
3	Diagnostic	Alarme	Alerte	DMIA
4	Décision	Alerte	Déclenchement du secours	DMIA (voir règle ci-dessous)
5	Restauration	Déclenchement	Fin de restauration	DMIA
6	Validation et relance	Fin de restauration	Reprise	DMIA



Lorsque la phase de **décision** relève des métiers, la DMIA garantie par la DSI **exclut** la durée de cette phase.

⚠ Point d'expertise — Dans un scénario de cyberattaque, la phase 1 doit intégrer le **délai de latence de l'attaquant** : la dernière sauvegarde *saine* peut être bien plus ancienne que la dernière sauvegarde *réussie*. La PDMA effective en ILG dépend donc de la profondeur de rétention (§5.13) et de la capacité à dater la compromission.

5.3 Classification DICP des données

Classification utilisée pour l'analyse des risques du SI, sur quatre critères :

- **Disponibilité** : garantir aux utilisateurs la continuité des services et des données ;
- **Intégrité** : mettre à disposition des données exactes, dans les délais et les espaces prévus ;
- **Confidentialité** : réserver l'accès aux données sensibles aux seules personnes autorisées ;
- **Preuve** : garantir une traçabilité suffisante pour le contrôle et l'administration de la preuve.

Leur prise en compte suppose des processus, règles, normes, méthodes et procédures.

5.4 Disponibilité au sens DICP

La stratégie est concernée par la nécessité :

- de garantir la récupération des données en cas d'incident ;
- de définir un nombre de copies de secours suffisant ;
- de tenir compte des performances des procédures de restauration.

En cas de sinistre, la disponibilité est qualifiée par la DMIA et la PDMA (§5.2).

5.5 Intégrité au sens DICP

La stratégie est concernée par la nécessité :

- de définir les sauvegardes en fonction des scénarios de perte d'intégrité ;
- de préserver l'intégrité des sauvegardes réalisées (contrôles d'intégrité, empreintes, immutabilité) ;
- de préserver l'intégrité des données pendant l'exécution des sauvegardes (cohérence applicative, §5.15).

5.6 Confidentialité au sens DICP

La stratégie est concernée par la nécessité :

- d'appliquer aux données mortes un niveau de protection **au moins équivalent** à celui des données vivantes associées ;
- de chiffrer les sauvegardes externalisées ou isolées, avec des **clés gérées hors de l'infrastructure de sauvegarde** et elles-mêmes sauvegardées (séquestre) — sans quoi la perte du système de sauvegarde rend les copies illisibles.

5.7 Preuve au sens DICP

La stratégie est concernée par la nécessité :

- de tracer exhaustivement les opérations de sauvegarde, pour identifier les écarts dus à des sauvegardes manquantes ou erronées ;
- de tracer exhaustivement les opérations de restauration, pour identifier les modifications apportées aux données vivantes ;
- de tracer les opérations d'administration sur l'infrastructure de sauvegarde (suppressions, modifications de rétention, changements de politique), qui sont des cibles privilégiées des attaquants.

5.8 Environnement fonctionnel et environnement de sauvegarde

Toute donnée appartient à un environnement fonctionnel. Le SI de **{{ORGANISATION}}** comprend **{{N}}** environnements fonctionnels **[À COMPLÉTER]**, chacun doté d'un niveau de criticité propre au regard des activités. L'environnement d'appartenance contribue donc à déterminer le niveau de sécurisation applicable.

Pour simplifier l'administration de la sauvegarde, les environnements fonctionnels sont regroupés en **trois contextes** :

Contexte de sauvegarde	Environnements fonctionnels inclus
Production	Production, Infrastructure, Formation
Pré-production	Qualification, Pré-production
Hors production	Tous les autres (développement, recette, tests...)

Dans la suite du document, **PROD** désigne les environnements du contexte « Production » ; **Hors PROD** désigne tous les autres.

5.9 Flux entrants et flux sortants

- **Flux entrants** : données reçues de SI externes à **{{ORGANISATION}}**.
- **Flux sortants** : données émises vers des SI externes.

Pour se prémunir en cas de litige avec un partenaire ou un client émetteur ou destinataire, il est indispensable de sauvegarder :

- les données reçues, **dès réception et avant toute utilisation** dans le SI ;
- les données émises, **juste avant leur envoi**.

Ces sauvegardes sont restaurées :

- en cas de litige ;
- en cas de sinistre, pour reconstituer les données perdues (§5.20).

5.10 Sauvegarde des données

La sauvegarde (prise d'image des données), associée à la restauration (restitution non altérante), est un procédé de sécurisation visant à supprimer ou réduire les conséquences d'un incident technique ou d'un dysfonctionnement applicatif, volontaire ou non, détecté immédiatement ou non.

Le choix du type de sauvegarde dépend de trois critères :

1. **Le type d'incident à couvrir** : erreur humaine ou malveillance ; sinistre matériel ou immatériel ; incident diffus ou local ; corruption de données ; infection par un logiciel malveillant.

2. **Les objectifs de disponibilité** : DMIA, PDMA, critères D et I au sens DICP.
3. **La performance de l'infrastructure disponible** : technologies et supports de stockage (disques, baies, bandes, librairies, stockage objet, fichiers séquentiels, bases de données...).

La combinaison de ces critères conduit généralement à mettre en œuvre **plusieurs sauvegardes pour une même donnée**.

5.11 Types de sauvegarde

Principaux types : complète (*full*), différentielle, incrémentale, par journalisation (*logging*), par réplication, par clonage, par instantané (*snapshot*). Leurs caractéristiques sont détaillées en Annexe C.

5.12 Dispositifs actif-actif et actif-passif

Dispositifs de haute disponibilité des équipements (serveurs, stockage) fondés sur le basculement d'un équipement défaillant vers un autre. Ils garantissent une PDMA nulle **face à une panne physique** — pas face à une corruption logique, qui est répliquée.

Mode	Principe	Basculement	Effet sur la DMIA
Actif-actif	Répartition de charge	Sans intervention humaine	Temps de bascule considéré comme nul
Actif-passif	Équipement secondaire en veille tant que le primaire fonctionne	Automatisé avec approbation humaine	Inférieur à une restauration ou une reconstruction classique

5.13 Caractéristiques des sauvegardes

Toute sauvegarde est caractérisée a minima par :

- **Sa fréquence** : délai prévu entre deux sauvegardes consécutives d'un même ensemble de données.
 - Fréquence périodique : sauvegarde quotidienne, hebdomadaire, mensuelle, annuelle.
 - Sauvegarde à la demande : pour sécuriser un événement (migration, changement d'environnement, image post-correction d'incident).
 - Fréquence liée au changement d'état de la donnée : sauvegarde dite synchrone, équivalente à une redondance.
- **Son nombre de versions** : nombre d'images distinctes disponibles en fonctionnement nominal.
 -  Après résolution d'un incident, l'image doit être prise par une **procédure spécifique** et non par une procédure périodique, afin de ne pas réduire l'âge maximal des images ni le nombre de versions disponibles.
- **Sa durée de rétention**.

La durée de rétention est la durée de conservation maximale d'une donnée morte, égale au produit de la fréquence par le nombre de versions. La destruction de la donnée d'origine n'entraîne pas la destruction de ses sauvegardes, qui sont détruites à l'expiration de leur rétention.

Exemple de schéma de rétention (valeurs d'illustration [À VALIDER])

Exemple construit sur celui que donne le guide de l'ANSSI « Sauvegarde des systèmes d'information — les fondamentaux » (15 jours de quotidiennes, 1 an de mensuelles, 5 ans d'annuelles), complété d'un niveau hebdomadaire :

Sauvegarde	Fréquence (jours)	Versions	Rétention maximale (jours)
Quotidienne	1	15	15

Sauvegarde	Fréquence (jours)	Versions	Rétention maximale (jours)
Hebdomadaire	7	5	35
Mensuelle	31	12	372
Annuelle	365	5	1 825
Total		37	≈ 5 ans

Ce schéma garantit l'existence d'une sauvegarde sur cinq ans avec 37 versions réparties de façon dégressive : dense sur les derniers jours, espacée au-delà. Les versions anciennes **ne sont pas des archives**.

Au-delà de sa période de rétention, une donnée morte est considérée comme perdue et **doit être détruite** pour garantir la confidentialité des données.

La **profondeur** (âge maximal de conservation) d'une donnée correspond à la rétention maximale de l'ensemble de ses sauvegardes.

 **Point d'expertise** — La conservation de données personnelles dans les sauvegardes doit rester compatible avec les durées de conservation déclarées au titre du RGPD. Une rétention pluriannuelle doit être justifiée dans le registre des traitements, et le traitement des demandes d'effacement vis-à-vis des sauvegardes doit être documenté [**À VALIDER avec le DPO**].

5.14 Sanctuarisation des sauvegardes

La sanctuarisation est un dispositif d'isolation garantissant la **non-altérabilité** des sauvegardes jusqu'à une date ou un événement déterminé. Il combine mesures organisationnelles et techniques. Son objectif est de garantir l'existence de sauvegardes exploitables pour sortir d'un sinistre, y compris lorsque l'attaquant a obtenu des droits d'administration sur le SI.

Exigences minimales de l'OGS [**À VALIDER**] :

Exigence	Contenu
Règle 3-2-1-1-0	3 copies des données, sur 2 supports ou technologies différents, dont 1 hors site, dont 1 hors ligne ou immuable, avec 0 erreur constatée lors des vérifications de restauration.  L'ANSSI formule le socle 3-2-1 ainsi : la production et deux sauvegardes, sur des supports différents, dont une hors ligne — une copie hors site mais joignable par le réseau ne suffit pas
Immutabilité	Verrouillage de la rétention (type WORM / <i>object lock</i> en mode conformité, ou bandes hors ligne) : aucune suppression ni modification possible avant échéance, y compris par un administrateur
Séparation des privilèges	Plan d'administration de la sauvegarde distinct de l'annuaire de production, authentification forte, comptes nominatifs, principe du double contrôle pour toute suppression ou réduction de rétention
Isolation réseau	Flux vers le coffre limités, unidirectionnels lorsque c'est possible, fenêtres d'ouverture contrôlées
Surveillance	Alerte sur les comportements anormaux : suppressions massives, variations brutales de volumétrie ou de taux de déduplication (indice de chiffrement)

Dispositif retenu par **{{ORGANISATION}}** : **{{NOM_DU_DISPOSITIF}}**, opéré par **{{PRESTATAIRE_COFFRE}}** ou en interne [**À COMPLÉTER**].

5.15 Unité de temps et intégrité référentielle

La sécurisation cohérente d'un ensemble de données exige généralement plusieurs sauvegardes unitaires. Celles-ci doivent être réalisées **dans une même unité de temps** (point de cohérence) pour préserver l'intégrité référentielle en cas de restauration du groupe.

⚠ Sans unité de temps, la restauration produit des incohérences entre données. Il faut alors en reconstituer la cohérence par des correctifs appliqués directement sur les données (§5.20).

5.16 Réparation des données

La réparation corrige des données corrompues. Si des sauvegardes exploitables existent, elle s'effectue par **restauration** (§5.17) ; sinon, par **reconstitution** (§5.20).

5.17 Restauration des données

La restauration transfère sur un système existant des données issues d'un support de sauvegarde, pour retrouver les données vivantes dans leur état à un instant *t*. Réalisée directement sur des données vivantes, elle les remplace par leur image à la date de la sauvegarde utilisée.

La capacité de restauration décroît avec le temps (au-delà de la rétention) et avec les événements (sauvegardes échouées ou corrompues).

5.18 Espace de validation et environnement de restauration sain

Lors d'un incident touchant un volume important ou des données critiques, il faut disposer d'un **espace de stockage similaire mais distinct** de celui des données impactées. Il permet de restaurer sans écraser les données en incident, puis de comparer les deux pour mesurer l'impact.

Extension cyber [À VALIDER] — Dans un scénario ILG, cet espace prend la forme d'un **environnement de restauration sain** (*clean room*) : isolé du SI compromis, il permet d'analyser les sauvegardes (recherche de marqueurs de compromission, détection de logiciels malveillants), d'identifier le dernier point de restauration sain, puis de reconstruire les socles avant réintégration.

5.19 Reconstruction

La reconstruction réinstalle, sur les systèmes impactés, un système non corrompu. Elle ne se limite pas aux données métier : une caractéristique de la menace cyber est de devoir **reconstruire les environnements techniques** (systèmes, annuaire, DNS, PKI, outils d'administration, infrastructure de sauvegarde).

Conséquence directe : **les éléments nécessaires à la reconstruction doivent eux-mêmes être sauvegardés et isolés** — images de référence, configurations, code d'infrastructure, secrets et clés, documentation d'exploitation, procédures de reconstruction.

5.20 Reconstitution des données

Activité complémentaire de la restauration et de la reconstruction. Elle minimise la perte de données, lorsqu'aucune sauvegarde n'est disponible, en jouant d'anciens flux métier (§5.9), puis remet les données dans un état cohérent garantissant leur intégrité référentielle.

▮ Le recours à la reconstitution doit rester exceptionnel et limité aux sinistres majeurs.

6. Périmètres et limites

6.1 Sur les rôles

6.1.1 Propriété

Les données métier appartiennent aux métiers ; les supports de stockage appartiennent à **{{ORGANISATION}}**.

La DSI apporte aux supports de stockage le niveau de sécurité permettant de répondre aux exigences exprimées par les métiers. À défaut d'expression de besoin, l'**Offre Générale de Sauvegarde** (§9) s'applique à l'ensemble des données.

6.1.2 Responsabilité

La responsabilité de la sécurisation des données du SI relève de **{{ORGANISATION}}** et **ne peut être déléguée** à un tiers.

Seules la conception, la mise en œuvre ou l'exploitation de la sécurisation peuvent être sous-traitées. **{{ORGANISATION}}** conserve le contrôle de la sécurisation et de son efficacité.

Sont hors de la responsabilité de la DSI les données concernant **{{ORGANISATION}}** :

- qui ne sont pas intégrées au SI géré par la DSI ;
- pour lesquelles une direction a contracté directement avec un partenaire ou un prestataire, sans passer par la DSI. ⚠ Ces situations doivent être recensées : elles constituent des angles morts de la continuité.

6.2 Sur les données

6.2.1 Environnements fonctionnels (données structurées)

Toutes les données du SI exploitées par la DSI, quel que soit leur environnement, sont sécurisées selon le niveau de disponibilité défini par leur classification DICP.

Exemple : les sources et les exécutables relèvent aussi des méthodes et procédures découlant de la présente stratégie.

6.2.2 Données bureautiques et données locales (données non structurées)

La sécurisation des données bureautiques est assurée par la mise à disposition d'espaces de stockage partagés (partagés réseau, espaces collaboratifs), eux-mêmes sauvegardés.

En conséquence, **aucune donnée bureautique ne doit être stockée sur les disques locaux des postes de travail.**

⚠ La sécurisation des données locales des postes est **exclue** de la stratégie. La perte massive de postes (sinistre d'un site utilisateur, attaque destructrice) relève d'un scénario spécifique — *Indisponibilité Massive des Postes de Travail* — couvert par le Plan de Reprise Utilisateurs [À COMPLÉTER : nom local du scénario et du plan].

6.2.3 Données nomades

Les données nomades sont stockées localement sur les équipements mobiles et synchronisées avec les espaces serveur à chaque connexion. En mode déconnecté, elles ne sont pas sauvegardées : seules les données présentes côté serveur le sont.

 La perte d'un équipement nomade entraîne la perte définitive des données non synchronisées. Des connexions régulières sont fortement recommandées.

6.2.4 Archives et supports d'archive

L'archivage est une mesure fonctionnelle, destinée à répondre à une obligation juridique, fiscale ou légale portée par les métiers. Ce n'est pas une mesure de sécurisation à l'initiative de la DSI.

 La constitution fonctionnelle des archives est **hors du périmètre** de la stratégie.

Les données archivées ont une PDMA nulle, une DMIA et une durée de conservation potentiellement très longues. L'inaltérabilité, l'accessibilité et la lisibilité des supports primaires d'archive doivent être garanties jusqu'à la date de péremption des données.

 La **sécurisation des supports d'archive** fait partie de la stratégie, au même titre que celle des autres supports.

6.2.5 Conservation longue

Une donnée nécessitant une conservation de plusieurs années est sécurisée par une sauvegarde isolée (§5.1, données mortes isolées), afin de prévenir l'illisibilité ou la perte liées à la durée. Une vérification périodique de relecture et un plan de migration des formats et des supports sont à prévoir.

6.2.6 Données hébergées en SaaS ou en cloud public (ajout)

Les services SaaS et cloud reposent sur un **modèle de responsabilité partagée** : le fournisseur garantit généralement la disponibilité de son service, rarement la restauration des données du client après suppression, corruption ou chiffrement initié depuis un compte légitime.

 Toute donnée métier hébergée en SaaS ou en cloud public entre dans le périmètre de l'OGS. Pour chaque service, la couverture contractuelle du fournisseur est analysée ; l'écart est comblé par une sauvegarde tierce ou par une OSS.

[À COMPLÉTER] — Inventaire des services concernés (messagerie et suite collaborative, CRM, plateformes PaaS...) et solution retenue pour chacun.

6.3 Sur les dysfonctionnements

6.3.1 Sinistre total

 Le sinistre total — perte simultanée des données vivantes et de leurs sauvegardes sur l'ensemble des sites d'hébergement **et** dans le coffre isolé (**{{PRESTATAIRE_COFFRE}}**) — est **hors périmètre** de la stratégie.

 Cette exclusion constitue une **acceptation de risque**. Elle est formellement validée par la direction générale, ou par l'instance qui porte l'appétence au risque de **{{ORGANISATION}}**, et revue chaque année [À COMPLÉTER : instance et date de validation].

6.3.2 Corruption des données

 La corruption de données équivaut à une indisponibilité et déclenche l'application des principes de la présente stratégie.

La DSI garantit l'efficacité des procédures de sauvegarde et de restauration pour en assurer l'utilisabilité en cas d'incident ou de sinistre.

La validation de l'intégrité des procédures de sauvegarde et de restauration (§9.2.1) fait partie intégrante de la stratégie.

La corruption n'étant pas toujours détectée immédiatement, **le délai probable entre corruption et détection** doit être pris en compte pour dimensionner la profondeur des sauvegardes.

7. Gouvernance

Avant toute mise en œuvre opérationnelle ou technique, la stratégie s'assure qu'une gouvernance adaptée est en place, garantissant le maintien en condition opérationnelle et une démarche d'amélioration continue.

7.1 Rôles

L'affectation nominative des rôles figure en Annexe B.

Rôle	Missions principales
Propriétaires métier (MÉT) — responsables des activités prioritaires identifiées par la BIA	Exprimer les besoins de disponibilité et de perte de données tolérables · Valider les engagements DMIA / PDMA de l'OGS · Demander et financer les Offres Spécifiques · Décider, pour leur périmètre, du déclenchement du secours (phase 4 du §5.2) · Valider les résultats des exercices · Recevoir le reporting sur le respect des engagements
Directeur des Systèmes d'Information (DSI)	Mandater le DIO sur le respect de la politique de sauvegarde · Informer le DIO et le RPCI des évolutions planifiées · Aligner la gouvernance et les moyens physiques, logistiques et humains sur les besoins
Responsable de la Sécurité des SI (RSSI)	Communiquer la PSSI · Aligner les programmes de sécurisation · S'assurer du respect de la PSSI
Directeur des Infrastructures et des Opérations (DIO)	Organiser, sous l'impulsion du DSI, la conception et la mise en œuvre d'une stratégie de sauvegarde pérenne, alignée sur la PSSI · Prendre en compte les remontées du RPCI · Transmettre au DSI les besoins d'évolution (gouvernance, moyens) · Produire le reporting stratégique à destination du DSI
Responsable du Plan de Continuité Informatique (RPCI)	Établir et faire évoluer la stratégie · Définir le PCI · Sensibiliser les intervenants · Veiller à l'application opérationnelle de la stratégie · Organiser son suivi · Piloter opérationnellement les exercices · Suivre les écarts d'application · Piloter les solutions de secours en cas de sinistre · Produire le reporting tactique à destination du RSSI et du DIO
Responsable de Production (RPROD)	Intégrer les principes et règles de la stratégie · Les traduire en méthodes et procédures opérationnelles · Sensibiliser ses équipes, les AdMP et les AdSv · Veiller au respect des méthodes et règles · Suivre les incidents de sauvegarde et de restauration · Produire le reporting opérationnel à destination du DSI, du DIO et du RPCI
Responsable du Plan de Continuité d'Activité (RPCA)	Établir les critères de sécurité applicables aux services métier · Décrire à haut niveau les scénarios de secours informatique · Organiser les exercices de validation · Animer les comités de continuité
Directeur de l'Architecture (DARCH)	Prendre en compte les besoins de disponibilité et de continuité des métiers · Concevoir les évolutions de l'infrastructure et des services pour y répondre
Administrateur des moyens de production (AdMP)	Mettre en œuvre les méthodes conformément à la stratégie · Instruire les incidents affectant le plan de sauvegarde · Fournir les éléments du reporting opérationnel · Établir le plan de capacité des moyens de sauvegarde et de restauration

Rôle	Missions principales
Administrateur de sauvegardes (AdSv)	Établir les procédures opérationnelles du plan de sauvegarde · Garantir l'opérabilité des moyens de sauvegarde et de restauration · Instruire les incidents de sauvegarde et de restauration · Réaliser les restaurations demandées par les métiers · Contribuer au plan de capacité

7.2 Responsabilités (RACI)

Les responsabilités sont présentées selon une **matrice RACI au format français** :

- **R — Responsable** : rend compte de l'activité auprès des instances et garantit la cohérence de son organisation ;
- **A — Acteur** : exécute ou fait exécuter l'activité conformément à la stratégie ;
- **C — Consulté** : avant ou pendant l'exécution ;
- **I — Informé** : reçoit les informations utiles.

La colonne **MÉT** désigne les propriétaires métier des activités concernées. Leur présence est délibérée : ce sont eux qui fixent les seuils, financent les offres spécifiques et valident les exercices.

 Dans le format anglo-saxon, **A** signifie *Accountable* (redevable) et **R** *Responsible* (exécutant) : les lettres sont inversées. À préciser lors de toute diffusion à des interlocuteurs internationaux.

Activité	MÉT	DSI	RSSI	DIO	RPCI	RPR OD	RPC A	DAR CH	AdM P	AdSv
Politique										
Communiquer la politique de sauvegarde	I	C	AR	I	I	I	I	I	I	I
Mettre en place l'organisation et les moyens permettant le respect de la politique	I	AR	C	C	C	C	C	C	I	I
Mandater le DIO sur le respect de la politique	-	AR	C	C	I	I	I	I	I	I
Aligner la gouvernance et les moyens sur les besoins	C	R	I	A	C	C	C	C	-	-
S'assurer du respect de la politique	-	A	AR	C	C	C	C	I	-	-
Stratégie										
Organiser la conception et la mise en œuvre d'une stratégie pérenne alignée sur la PSSI	I	C	C	R	A	I	I	I	-	-
Établir la stratégie de sauvegarde	C	C	C	C	AR	C	C	C	C	C
Définir le Plan de Continuité Informatique	C	I	I	R	A	C	C	C	I	I
Organiser le suivi de la stratégie	-	-	-	I	AR	C	C	C	I	I
Veiller à l'application opérationnelle de la stratégie	-	I	I	A	AR	C	C	C	-	-
Établir les critères de disponibilité des données applicables aux services métier	A	C	R	A	C	C	A	C	-	-
Valider les engagements DMIA / PDMA de l'OGS (ajout)	AR	C	I	C	C	C	C	C	-	-
Demander et financer une Offre Spécifique (ajout)	AR	I	-	C	C	I	C	A	-	-
Programme										
Aligner les programmes de sécurisation	-	C	AR	C	C	C	C	C	-	-
Informar le DIO et le RPCI des évolutions planifiées	-	AR	I	I	I	I	I	I	-	-
Intégrer les besoins de disponibilité et de continuité dans le programme d'architecture	C	C	I	C	C	A	I	R	I	I
Concevoir les évolutions de l'infrastructure pour répondre à ces besoins	-	-	I	I	C	C	I	AR	-	-
Opérations										
Intégrer les principes et règles de la stratégie	-	C	I	C	C	AR	-	-	I	I

Activité	MÉT	DSI	RSSI	DIO	RPCI	RPR OD	RPC A	DAR CH	AdM P	AdSv
Traduire la stratégie en méthodes et procédures opérationnelles	-	-	-	I	I	R	I	C	A	A
Veiller au respect des méthodes et règles	-	-	-	-	I	AR	-	-	I	I
Mettre en œuvre les méthodes conformément à la stratégie	-	-	-	-	C	C	-	-	AR	C
Établir les procédures opérationnelles du plan de sauvegarde	-	-	-	-	I	C	-	-	A	AR
Réaliser les restaurations à la demande des métiers	C	-	-	-	I	C	I	-	A	AR
Garantir l'opérabilité des moyens de sauvegarde et de restauration	-	-	-	-	I	C	-	-	A	AR
Validation										
Décrire à haut niveau les scénarios de continuité informatique	C	-	-	I	C	C	AR	C	-	-
Organiser les exercices de validation (volet organisationnel)	C	I	I	I	A	C	R	C	I	I
Piloter les exercices de validation (volet opérationnel)	C	I	I	I	AR	C	C	C	C	C
Piloter les solutions de continuité et de reprise en cas de sinistre	C	C	C	C	AR	C	C	I	I	I
Décider du déclenchement du secours ou de la restauration (cellule de crise en ILG / IPG) <i>(ajout)</i>	AR	C	C	C	A	C	C	I	I	I
Valider les résultats des exercices <i>(ajout)</i>	AR	I	I	I	C	I	C	I	-	-
Sensibilisation										
Sensibiliser les intervenants	I	I	I	C	AR	I	I	I	I	I
Sensibiliser ses collaborateurs	-	-	-	-	I	AR	-	-	I	I
Reporting										
Animer les comités de continuité d'activité	C	I	I	I	C	C	AR	C	-	-
Transmettre au DSI les besoins d'évolution (gouvernance, moyens)	-	C	I	AR	C	C	I	C	-	-
Prendre en compte les remontées du RPCI	-	-	I	AR	C	-	-	C	-	-
Reporting stratégique à destination du DSI	-	I	-	AR	C	-	-	-	-	-
Reporting tactique à destination du DIO et du RSSI	I	-	I	C	AR	C	C	C	C	C
Reporting opérationnel à destination du DSI, du DIO et du RPCI	-	I	-	I	C	AR	-	-	C	C
Produire les éléments du reporting opérationnel	-	-	-	-	-	I	-	-	AR	C
Incidents										
Suivre les écarts d'application de la stratégie	I	I	-	I	AR	C	I	I	-	-
Suivre les incidents de sauvegarde et de restauration	-	I	-	I	C	AR	-	I	C	C
Instruire les incidents affectant le plan de sauvegarde	-	-	-	I	I	C	-	I	AR	C
Instruire les incidents de sauvegarde et de restauration	-	-	-	I	I	C	-	I	A	AR
Plan de capacité										
Établir le plan de capacité des moyens de sauvegarde et de restauration	-	-	-	-	I	C	-	I	AR	C
Contribuer au plan de capacité	-	-	-	-	I	C	-	-	A	AR

La mise en œuvre et sa déclinaison en procédures opérationnelles couvrent :

- les périmètres techniques de sauvegarde ;
- les modalités d'exécution ;
- les supports utilisés ;
- le planning des opérations ;

- le planning et la fréquence des tests de restauration et de reconstruction.

La sauvegarde couvre **tout le périmètre de la PSSI**, quel que soit l'environnement de stockage des données.

7.3 Comitologie

[À COMPLÉTER] — Faire correspondre chaque instance ci-dessous à une instance existante de

{{ORGANISATION}} plutôt que d'en créer de nouvelles.

Niveau	Instance	Fréquence	Pilote	Livrables
Stratégique	Comité de pilotage de la continuité ({{INSTANCE_STRATEGIQUE}})	Trimestrielle	RPCA	Validation du périmètre et des plans de test
Tactique	Comité de suivi des objectifs	Semestrielle	RPCI	Évolutions de la stratégie, du PCI, de la gouvernance
Opérationnel	Comité de gestion des incidents	Selon rituel ITSM	Gestionnaire des incidents	Remontée des incidents de sauvegarde au RPCI
Opérationnel	Comité de gestion des changements	Selon rituel ITSM	Gestionnaire des changements	Remontée des changements impactant la sauvegarde
Opérationnel	Réunion de préparation d'exercice	J-2 mois	RPCI	Plan d'actions préventif, relevé de décisions
Opérationnel	Réunion de bilan d'exercice	J+8 jours	RPCI	Relevé de décisions, incidents ouverts
Opérationnel	Comité de suivi des exercices	Bimestrielle [À VALIDER]	RPCI	Plan d'actions des bilans à jour

7.3.1 Comité stratégique — pilotage de la continuité

Lors des comités trimestriels :

- le **RPCI** présente les évolutions de la stratégie et du PCI, le bilan des exercices et l'analyse causale des incidents (une déplanification ou un changement de périmètre est considéré comme un incident) ;
- le **RPCA** présente l'évolution de la stratégie de PCA au regard du PCI, pour {{ORGANISATION}} et ses entités, ainsi que les objectifs de continuité pour les années suivantes, notamment ceux des exercices ;
- le **comité** valide le périmètre prévisionnel et les plans de test associés.

7.3.2 Comité tactique — suivi des objectifs

Chaque semestre, le RPCI réunit le DIO et le Responsable de Production pour arrêter :

- les évolutions de la stratégie, de la gestion des infrastructures, des méthodes et des procédures ;
- les adaptations de gouvernance, de suivi et de reporting ;
- les évolutions du PCI pour l'année suivante.

Le DIO s'appuie sur le compte rendu pour transmettre au DSI les besoins d'évolution (§7.2, Reporting).

7.3.3 Comités opérationnels

Comité de gestion des incidents. Le gestionnaire des incidents :

- informe le RPCI de tout incident dont l'origine concerne le dispositif de sauvegarde, de restauration ou de reconstruction ;

- lui transmet tous les éléments d'identification et d'analyse.

Comité de gestion des changements. Le gestionnaire des changements signale au RPCI les changements non répercutés dans la CMDB, afin qu'il en tienne compte pour les exercices à venir.

La gestion des changements intègre un indicateur « nouvelle technologie », qui permet d'extraire les risques technologiques et les applications métier associées. Une technologie validée lors d'un exercice PCI n'est plus considérée comme nouvelle.

Réunion de préparation d'exercice — organisée par le RPCI deux mois avant chaque exercice, pour :

- revoir les objectifs de l'exercice ;
- identifier les participants et valider leur disponibilité ;
- faire le point sur les modifications du SI depuis le dernier exercice ;
- intégrer le plan d'actions des bilans précédents ;
- identifier et planifier les actions préventives.

Les managers invités désignent les responsables des actions préventives ; en cas d'absence, ils se font représenter par un collaborateur habilité à décider. Livrables : plan d'actions préventif et relevé de décisions.

Réunion de bilan d'exercice — organisée par le RPCI dans les huit jours suivant chaque exercice. Elle recense tous les incidents et dysfonctionnements (opérationnels, fonctionnels, organisationnels) constatés et désigne pour chacun un responsable d'action disposant du niveau de responsabilité suffisant pour élaborer, piloter et rendre compte du plan correctif. Livrables : relevé de décisions, mise à jour du plan d'actions des bilans, ouverture des incidents.

Comité de suivi des exercices — organisé par le RPCI tous les deux mois [À VALIDER]. Il suit les plans d'actions correctifs issus des bilans. Chaque responsable d'action y est invité ou se fait représenter. Livrable : plan d'actions des bilans à jour.

7.4 Suivi des incidents

7.4.1 Suivi opérationnel

- L'AdSv ouvre un ticket dans {{OUTIL_ITSM}} pour chaque incident ou dysfonctionnement d'un traitement ou d'une procédure de sauvegarde ou de restauration. **Un traitement prévu et non exécuté est un incident.**
- L'AdMP ouvre un ticket pour chaque incident touchant une ressource matérielle ou logique participant à la sauvegarde ou à la restauration.
- Des incidents de même type survenus le même jour peuvent être regroupés en un seul ticket, qui précise le nombre d'occurrences.
- Un incident récurrent sur plusieurs jours donne lieu à un ticket par jour ; cette récurrence déclenche l'ouverture d'un **problème** pour en éradiquer la cause.

7.4.2 Suivi tactique

Le Responsable de Production établit chaque mois un **rapport de synthèse des incidents de sauvegarde** : situation mensuelle en volume et en nature, tendance annuelle. Il est présenté à {{INSTANCE_TACTIQUE}} [À COMPLÉTER], en présence du RPCI, avec une proposition de priorisation des plans d'actions selon les besoins métier.

7.4.3 Suivi stratégique

Le RPCI émet chaque trimestre un **rapport de respect de la stratégie**, fondé sur les rapports mensuels : synthèse des manquements, état des lieux et évolution du niveau de risque. Destinataires : DSI, DIO, RPCA, DARCH, RPROD, RSSI.

7.5 Révision de la stratégie

Le RPCI engage une révision :

- après toute nouvelle version de la politique de sauvegarde ;
- avant toute évolution majeure du SI ;
- annuellement, pour intégrer les évolutions mineures ;
- **après tout incident majeur ou exercice** ayant révélé une insuffisance de la stratégie (*ajout*).

Une **évolution majeure** est un changement (ou un ensemble de changements liés) rendant les méthodes et solutions de la stratégie inefficaces au regard du besoin de continuité.

Toute révision suit le cycle de validation suivant :

Activité	Fonction
Rédaction	RPCI
Relecture	AdSv, AdMP, RPCA
Validation	DIO, Responsable de Production, RSSI
Validation des engagements (§9.1)	Propriétaires métier, en comité stratégique de continuité
Approbation	DSI
Acceptation des risques résiduels (§6.3.1)	Direction générale ou instance d'appétence au risque

Les résultats de la stratégie (indicateurs, exercices, incidents majeurs) alimentent la **revue de direction** du système de management de la continuité ou de la sécurité, lorsqu'il existe (*ajout*).

7.6 Disponibilité de la documentation en situation de sinistre (*ajout*)

La stratégie, le plan de sauvegarde, les procédures de restauration et de reconstruction, l'ordre de priorité et les coordonnées des intervenants doivent rester **accessibles sans le système d'information**.

Exigences minimales [À VALIDER] :

- une copie à jour dans le coffre isolé, avec les sauvegardes (§5.14, §5.19) ;
- une copie hors ligne (support chiffré ou papier) des procédures critiques et de l'annuaire de crise, détenue par le RPCI et son suppléant ;
- une vérification de la présence et de la lisibilité de ces copies à chaque exercice ;
- une mise à jour à chaque révision de la stratégie (§7.5).

8. Modélisation des indisponibilités

La stratégie applicable aux données hébergées dans les sites de **{{ORGANISATION}}** (§8.1 à §8.7) repose sur cinq hypothèses d'indisponibilité :

Code	Scénario	Nature	Étendue
IPG	Indisponibilité Physique Globale	Physique	Tous les sites
IPP	Indisponibilité Physique Partielle	Physique	Un site ou une ressource vitale d'un site
ILG	Indisponibilité Logique Globale	Logique	Données primaires de tous les sites
ILP	Indisponibilité Logique Partielle	Logique	Sous-ensemble de données
ND	Fonctionnement Nominal Dégradé	Physique ou logique	Sans impact métier

Les données hébergées hors site sont traitées au §8.8. Le sinistre total est hors périmètre (§6.3.1).

8.1 Architecture de référence et influence sur la stratégie

[À COMPLÉTER] — Insérer le schéma d'architecture de **{{ORGANISATION}}** et décrire le rôle de chaque site. L'architecture conditionne directement la couverture des scénarios physiques ; le tableau ci-dessous aide à situer l'organisation parmi les configurations courantes.

Configuration	Couverture de l'IPP	Point d'attention pour la stratégie
Mono-site , secours externalisé (contrat de secours, cloud, hébergeur)	Par restauration sur l'infrastructure de secours : DMIA longue	Les copies externalisées sont la seule protection contre la perte du site ; la DMIA dépend du délai de mise à disposition du secours
Bi-site actif-passif ou actif-actif	Par bascule : DMIA courte	Le site secondaire réplique aussi les altérations logiques ; une copie isolée hors des deux sites reste nécessaire
Multi-site , rôles spécialisés (production, reprise, administration)	Par bascule et répartition des applications	La spécialisation n'apporte de résilience que si les domaines d'administration sont séparés
Hybride sur site et cloud	Selon le service	Modèle de responsabilité partagée (§6.2.6) ; réversibilité et localisation des copies à contractualiser

Principes structurants, quelle que soit la configuration :

- la **répartition des applications** entre sites et la **généralisation de la haute disponibilité** transforment la majorité des incidents physiques en incidents de niveau « nominal dégradé » ;
- le **coffre des sauvegardes et le plan d'administration de la sauvegarde ne partagent pas les privilèges d'administration de la production** : c'est ce qui leur permet de survivre à une compromission de l'annuaire de production ;
- les flux de réplication, de pilotage et de reprise entre sites sont documentés ; ceux vers le coffre sont restreints (§5.14).

8.2 Indisponibilité Physique Globale (IPG)

Définition — Situation de « choc extrême » correspondant :

- soit à l'indisponibilité simultanée et totale de tous les sites d'hébergement de **{{ORGANISATION}}** ;
- soit à l'indisponibilité simultanée et totale d'au moins un type de ressource vitale (calcul, stockage, réseau) sur tous les sites, même si ceux-ci restent accessibles.

Stratégie de sauvegarde associée [À VALIDER]

Phase	Dispositions
Pendant le sinistre	Activation de la cellule de crise · Recensement des sauvegardes disponibles dans le coffre isolé · Mise à disposition d'une capacité d'hébergement de repli (contrat de secours, cloud, site tiers) [À COMPLÉTER] · Reconstruction des socles dans l'ordre de priorité du §9.4.4
Retour au mode nominal	Restauration des données à partir des copies isolées · Contrôle d'intégrité et validation métier · Reconstitution des données manquantes par rejeu des flux (§5.20) · Reconstitution des sauvegardes perdues
Éprouver le dispositif	Test annuel de restauration d'un périmètre représentatif depuis le coffre uniquement , sur une infrastructure vierge · Vérification de la lisibilité des supports et de la disponibilité des clés de chiffrement

8.3 Indisponibilité Physique Partielle (IPP)

Définition — « Sinistre physique local » correspondant :

- soit à l'indisponibilité totale d'un des sites (toutes salles confondues) ;
- soit à l'indisponibilité globale d'une ressource vitale (serveurs ou stockage) d'un des sites.

Stratégie de sauvegarde associée [À VALIDER]

Phase	Dispositions
Pendant le sinistre	Basculement des applications sur les dispositifs de haute disponibilité (réplication synchrone ou asynchrone) · Pour les applications non couvertes : restauration sur le site survivant à partir des sauvegardes asynchrones qui y sont répliquées · Poursuite des sauvegardes depuis le site survivant, avec une copie hors site maintenue
Retour au mode nominal	Reconstruction du site sinistré · Resynchronisation des données · Bascule retour planifiée · Reconstitution des sauvegardes perdues avec le site (§8.6.2)
Éprouver le dispositif	Exercice annuel de bascule, en alternant le site sinistré (voir §9.2.2)

8.4 Indisponibilité Logique Globale (ILG)

Définition — Altération globale des données primaires stockées sur tous les sites : propagation d'une corruption, destruction ou **chiffrement malveillant (rançongiciel)**, erreur d'administration à grande échelle.

 C'est le scénario le plus probable parmi les scénarios globaux dans le contexte de menace actuel. La haute disponibilité n'offre **aucune protection** : elle réplique l'altération.

Stratégie de sauvegarde associée [À VALIDER]

Phase	Dispositions
Pendant le sinistre	Activation de la cellule de crise : la décision de restaurer lui revient, sur avis de l'équipe de réponse à incident ; la restauration n'est pas engagée par l'équipe de sauvegarde seule · Information de l'assureur selon les conditions du contrat de cyberassurance, le cas échéant · Notifications réglementaires déclenchées par le plan de gestion de crise (hors périmètre du présent document) · Suspension de l'ensemble des services PROD et Hors PROD jusqu'au diagnostic · Préservation des preuves (images et journaux) avant toute restauration · Sauvegarde « à la demande » généralisée de la PROD, conservée à part (analyse forensique, récupération de données récentes non compromises) · Vérification de l'intégrité de l'infrastructure de sauvegarde et de son plan d'administration · Identification du dernier point de restauration sain en environnement isolé (§5.18)

Phase	Dispositions
Retour au mode nominal	Reconstruction des socles puis restauration selon l'ordre de priorité du §9.4.3 · Application d'un même point de restauration à l'ensemble des données, pour une PDMA homogène et la préservation de l'intégrité référentielle · Renouvellement des secrets et des comptes à privilèges avant réouverture · Reconstitution des données par rejeu des flux · Si les sauvegardes principales sont compromises : restauration depuis le coffre isolé (DMIA dégradée — §9.1)
Éprouver le dispositif	Exercice annuel de type « cyber-reconstruction » : reconstruction de l'annuaire et d'une application critique à partir des seules copies isolées · Test de détection d'une sauvegarde compromise

8.5 Indisponibilité Logique Partielle (ILP)

Définition — Ensemble des incidents affectant les données, du mode dégradé jusqu'aux incidents graves interrompant des services métier :

- soit l'indisponibilité simultanée et partielle des données primaires de tous les sites (volumes, fichiers, serveurs, bases de données) ;
- soit l'indisponibilité partielle des données primaires d'un site, combinée à l'indisponibilité totale des données primaires des autres sites.

Stratégie de sauvegarde associée [À VALIDER]

Phase	Dispositions
Pendant le sinistre	Qualification du périmètre et de la date de l'altération · Restauration dans l'espace de validation (§5.18) pour comparaison · Choix du point de restauration avec le métier
Retour au mode nominal	Restauration ciblée (serveur, base, fichiers) · Correction de cohérence ou reconstitution si nécessaire · Sauvegarde post-incident par procédure spécifique (§5.13)
Éprouver le dispositif	Procédures « témoin » quotidiennes (§9.2.1) · Restaurations réelles à la demande des métiers, comptabilisées dans les indicateurs

Cinématique type ILP — voir Annexe A.

8.6 Fonctionnement nominal dégradé

Ce scénario regroupe tous les autres incidents d'indisponibilité de ressources ou de données. Les applications métier ne sont pas impactées.

8.6.1 Incident sur les données vivantes

Incidents touchant les supports primaires d'un site, pour lesquels la haute disponibilité assure la continuité des applications. Ce cas relève de l'IPP (§8.3) sans interruption de service.

8.6.2 Incident sur les données mortes

Incidents ayant altéré ou détruit tout ou partie des sauvegardes. Ils n'interrompent pas les applications mais **dégradent le niveau de sécurité** des données actives associées. La stratégie consiste à reconstituer les sauvegardes concernées.

Destruction localisée sur un seul site — la reconstitution dépend de la récurrence de l'incident, de la criticité des données et de la fréquence de la sauvegarde :

Données	Règle
Critiques	Sauvegardes reconstituées par recopie depuis un autre site
Non critiques — sauvegarde quotidienne	Non reconstituées (renouvellement naturel)

Données	Règle
Non critiques — sauvegarde hebdomadaire ou plus espacée	Reconstituées

Destruction sur tous les sites — reconstitution à partir des copies sanctuarisées dans le coffre isolé, si elles sont disponibles. À défaut, les sauvegardes sont définitivement perdues, le niveau de sécurité est dégradé et l'incident est référencé.

⚠ Une destruction simultanée des sauvegardes sur plusieurs sites doit être traitée comme un **indicateur de compromission** jusqu'à preuve du contraire (préparation typique d'une attaque par rançongiciel).

8.6.3 Incident sur les ressources d'infrastructure de sauvegarde

Incidents touchant le réseau, les disques de clonage ou les lecteurs de bandes, sans altération ni destruction de données. Les actions relèvent de la gestion des incidents, pas de la présente stratégie. Leur durée doit cependant être suivie : une indisponibilité prolongée réduit la couverture PDMA.

8.7 Synthèse des scénarios pour les données hébergées sur site

Conventions — Chaque ressource est notée **disponible**, **indisponible** ou, pour les seules ressources de type « données », **partiellement disponible**.

Pour chaque cas majeur, un scénario type est identifié avec sa gravité, sa probabilité et sa criticité. Un incident est supposé ne concerner qu'un type de ressource ; s'il en concerne plusieurs, le scénario le plus grave s'applique.

8.7.1 Infrastructure actuelle

[À COMPLÉTER] — Gabarit :

#	Cas d'incident	Ressources vitales	Ressources critiques	Données	Scénario	Gravité (1-5)	Fréquence (1 fois tous les x ans)	Probabilité	Criticité
1	Ex. perte d'une baie de stockage sur {{SITE_A}}				IPP				
2	Ex. chiffrement de l'ensemble des serveurs Windows				ILG				
...									

Méthode de calcul proposée :

- **Probabilité** = (durée d'indisponibilité en h/jour × nombre de jours/an) / fréquence (1 fois tous les x ans) ;
- **Criticité** = exp(Gravité) × Probabilité — la fonction exponentielle donne un poids prépondérant aux scénarios graves, même rares ;
- **Ressources vitales** : indispensables au fonctionnement nominal ;

- **Ressources critiques** : indispensables au fonctionnement des sauvegardes.

⚠ Cette formule est une convention interne. Les échelles de gravité et de fréquence doivent être alignées sur la méthode d'analyse de risques de **{{ORGANISATION}}** (par exemple EBIOS RM ou ISO 27005) pour garantir la comparabilité avec le registre des risques.

8.7.2 Infrastructure cible

[À COMPLÉTER] — Même gabarit.

La généralisation de la haute disponibilité dans l'infrastructure cible dispense de restauration en cas d'IPP : ces incidents deviennent des cas de fonctionnement nominal dégradé. Les priorités se recentrent alors sur :

- le sinistre total, qui suppose un site tiers ;
- les sinistres massifs de type ILG et IPG ;
- les incidents de type ILP.

8.8 Indisponibilité des données hors site

Deux hypothèses sont retenues.

8.8.1 Services exploités par la DSI hors des sites principaux

Données stockées sur des infrastructures hébergées hors des sites principaux (agences, sites distants) mais exploitées par la DSI. Celle-ci organise une sécurisation couvrant un sinistre sur le site d'hébergement :

- les sauvegardes (socle technique, paramétrage, données métier) sont stockées sur les sites principaux ;
- la capacité de restauration est compatible avec les besoins exprimés par les métiers.

8.8.2 Prestations sous-traitées par la DSI

Certaines données du SI sont hébergées hors site et exploitées par un prestataire sous la responsabilité de la DSI. Le scénario dépend du type de prestataire.

Prestataires intra-groupe [À COMPLÉTER : cas concrets le cas échéant]

Chaque activité d'un prestataire intra-groupe participant à la sécurisation du SI reste sous la responsabilité de la DSI. Elle est encadrée par une ou plusieurs conventions de service précisant le cadre de réalisation, les responsabilités et les engagements réciproques.

Le prestataire maintient dans le temps les niveaux d'opérabilité et de sécurisation contractualisés, y compris en cas de modification d'architecture, d'infrastructure, de méthodes ou de procédures. Tout incident est déclaré au centre de services via **{{OUTIL_ITSM}}** et fait l'objet d'un suivi.

Prestataires externes

Les prestations encadrées par un Plan d'Assurance Sécurité (PAS) intègrent les exigences de la présente stratégie. La liste des prestations concernées figure en annexe **[À COMPLÉTER]**.

Étape	Exigences
Contractualisation	Offre de sécurité du prestataire validée par le DSI ou, par délégation, le RSSI · Clauses DMIA, PDMA et disponibilité spécifiées et compatibles avec l'OGS · Scénarios d'indisponibilité couverts explicités · Niveau de tests et d'exercices défini, avec droit de participation ou d'audit · Obligation de déclaration des incidents · Conditions de réversibilité et de restitution des données · Éléments de suivi attendus (métriques, rapports, bilans) · Désignation d'un responsable de compte côté DSI · Localisation et isolation des sauvegardes du prestataire
Suivi de la prestation	Revue opérationnelle mensuelle avec le prestataire (responsable de compte) · Reporting tactique trimestriel au RPCI · Comité stratégique annuel entre les achats et la direction du prestataire
Sinistre ou incident	Le prestataire déclare l'incident au centre de services, applique ses dispositifs contractuels pour restaurer les données et informe du rétablissement · La DSI anime la cellule de coordination et informe les métiers concernés

9. Offre Générale de Sauvegarde (OGS)

L'OGS est l'élément central de la stratégie. Elle découle des scénarios, définitions et notions présentés précédemment et porte sur cinq aspects :

1. les engagements de service de continuité ;
2. la validation de ces engagements ;
3. la sécurisation des données ;
4. la couverture de l'ensemble des scénarios d'indisponibilité ;
5. les modalités préétablies de gestion des incidents.

9.1 Engagements de service de continuité

Les engagements varient selon le type d'incident ou de sinistre. La continuité est caractérisée par la PDMA et la DMIA.

Valeurs par défaut [À VALIDER par les métiers]

Scénario	PROD — PDMA	PROD — DMIA	Hors PROD — PDMA	Hors PROD — DMIA
Nominal dégradé	N/A	0	N/A	0
ILP	≤ 24 h	≤ 12 h	≤ 24 h	≤ 12 h
IPP	0	≤ 1 h	0	≤ 24 h
ILG — corruption technique, sauvegardes saines	≤ 24 h (**)	≤ 12 h	≤ 24 h (**)	≤ 48 h
ILG — cyberattaque avec reconstruction	≤ 24 h (**) (***)	{{...}} [À VALIDER]	Best effort	Best effort
ILG — sauvegardes principales compromises	Selon disponibilité des copies isolées	≤ 7 jours	Best effort	Best effort
IPG	Selon disponibilité des copies isolées	{{...}} (*) [À COMPLÉTER]	Best effort	Best effort

(*) À compter de la mise à disposition des infrastructures matérielles de repli. (**) Sous réserve que l'incident ou le sinistre ait été détecté dans les 24 heures. (***) Mesurée à partir du dernier point de restauration **sain**, et non de la dernière sauvegarde réussie.

⚠ Point d'expertise — Une DMIA de 12 heures en ILG n'est réaliste que si les sauvegardes et le socle d'infrastructure sont intacts. Face à un rançongiciel ayant compromis l'annuaire, la reconstruction (socles, identités, analyse des sauvegardes) se compte généralement en jours. Distinguer les deux cas évite de prendre un engagement intenable ; la valeur retenue doit être étayée par un exercice.

Classes de criticité issues de la BIA (facultatif) [À COMPLÉTER] — Dans les scénarios massifs (ILG, IPG), tout ne peut pas revenir en même temps. Les engagements ci-dessus sont alors déclinés par classe, dans l'ordre de restauration du §9.4.3. L'OGS reste le plancher : aucune classe ne dispose d'un engagement inférieur à celui du contexte auquel elle appartient.

Classe	Critère (issu de la BIA)	Exemples	Vague de restauration (§9.4.3)	DMIA en ILG	PDMA
1 — Vitale	Durée d'interruption tolérable ≤ {{...}}	Services d'infrastructure, applications cœur de métier	Étapes 0 à 2, puis première vague métier	{{...}}	{{...}}
2 — Critique	≤ {{...}}		Deuxième vague	{{...}}	{{...}}

Classe	Critère (issu de la BIA)	Exemples	Vague de restauration (§9.4.3)	DMIA en ILG	PDMA
3 — Importante	$\leq \{\{\dots\}\}$		Troisième vague	$\{\{\dots\}\}$	$\{\{\dots\}\}$
4 — Différable	$> \{\{\dots\}\}$		Après retour à la normale	Best effort	$\{\{\dots\}\}$

Contexte de pré-production — Les données sont reconstruites à partir de celles de la PROD et ne sont pas sauvegardées au titre de l'OGS. Les engagements sont ceux du contexte Hors PROD. Un engagement plus contraignant relève d'une Offre Spécifique (§10).

9.2 Validation des engagements de service

9.2.1 Opérabilité des procédures de sauvegarde et de restauration

L'opérabilité des outils utilisés pour la sauvegarde et la restauration est vérifiée **quotidiennement** par des procédures « témoin », exécutées avant l'ouverture et après la fermeture du service :

- sauvegarde d'objets « témoin » représentatifs de tous les types de données du SI ;
- restauration dans un espace de validation (§5.18) ;
- comparaison : les objets restaurés doivent être identiques aux objets témoin.

En cas d'écart, l'efficacité des procédures est suspecte. Il faut alors vérifier l'opérabilité des outils **et** la validité de toutes les sauvegardes réalisées depuis la dernière exécution témoin valide.

Compléments recommandés [À VALIDER]

Contrôle	Fréquence	Périmètre
Restauration témoin automatisée	Quotidienne	Échantillon de tous les types de données
Restauration applicative complète avec validation fonctionnelle	Au moins annuelle	100 % des applications critiques, par rotation
Vérification de lisibilité des copies isolées	Trimestrielle	Échantillon du coffre
Vérification de restauration des clés et secrets	Semestrielle	Séquestre des clés de chiffrement

9.2.2 Opérabilité des scénarios d'indisponibilité

Validation par des **exercices annuels** organisés par le RPCI et budgétés l'année précédente.

Seuls les **métiers** sont habilités à valider les résultats des exercices éprouvant l'efficacité de la stratégie.

Ces exercices répondent, le cas échéant, aux obligations réglementaires ou sectorielles de $\{\{\text{ORGANISATION}\}\}$ en matière de test annuel du plan de continuité [À COMPLÉTER : textes applicables]. Ils sont planifiés sur trois mois pour limiter leur impact sur le SI. **Principe d'alternance** : d'une année sur l'autre, le sinistre simulé porte alternativement sur le site nominal et sur le site de secours, afin d'éprouver les deux sens de bascule.

Rétroplanning

Échéance	Objectif
J-3 mois	Définition du périmètre fonctionnel, validé par le RPCA
J-2 mois	Réunion de préparation d'exercice (§7.3.3)
J-1 mois	Préparation et validation de la disponibilité des ressources et de la date
J-2 semaines	Publication du planning prévisionnel des opérations
J-1 semaine	Réunion de coordination avec tous les participants

Échéance	Objectif
J+1 semaine	Réunion de bilan d'exercice

Phases d'un exercice

Phase	Objectif
Préparation	Réduire le risque opérationnel lié à l'exercice
Bascule « aller »	Transférer les activités du site à secourir vers le site de secours, dans le respect de la DMIA cible
Mode secours	Exécuter l'ensemble des activités sur le site de secours
Bascule « retour »	Redémarrer les activités de production en mode nominal
Finalisation	Rétablir le fonctionnement nominal de tous les environnements

Deux niveaux d'épreuve [À VALIDER]

Niveau	Contenu	Fréquence
Tests techniques par scénario	Les épreuves décrites à la ligne « Éprouver le dispositif » de chaque scénario (§8.2 à §8.5) : bascule, restauration depuis le coffre, reconstruction de l'annuaire et d'une application critique	Annuelle pour chaque scénario
Exercice majeur avec les métiers	Un scénario par an, en rotation : bascule de site (IPP), restauration massive (ILP massive), cyber-reconstruction depuis les copies isolées (ILG), exercice de crise sur table (IPG)	Annuel, scénario ILG au moins une année sur deux

Exigences applicables à chaque exercice (ajout, d'après ISO 22301 § 8.5) :

- objectifs et critères de réussite fixés et validés **avant** l'exercice (DMIA et PDMA cibles, périmètre, conditions d'arrêt) ;
- rapport formalisé après l'exercice : résultats mesurés, écarts, actions correctives (§7.3.3, réunion de bilan) ;
- exercice complémentaire après tout changement significatif du SI ou de l'organisation (§7.5).

9.3 Sécurisation des données

L'ensemble des données de **{{ORGANISATION}}** est sécurisé selon le plan de sauvegarde décrit par deux tableaux et deux schémas **[À COMPLÉTER]**.

Tableau 1 — Couverture par type de données. Pour chaque type de données, selon son lieu d'hébergement (sur site ou externalisé) et son contexte (PROD, Hors PROD) : origine, sauvegardes, type de donnée morte produite, utilité.

Type de données	Hébergement	Contexte	Sauvegardes appliquées	Données mortes produites	Utilité (scénario couvert)
Ex. base de données transactionnelle	Sur site	PROD	Réplication synchrone · journalisation · incrémentale quotidienne · copie isolée hebdomadaire	Synchrones · asynchrones · isolées	IPP · ILP · ILG
Ex. serveur de fichiers	Sur site	PROD			
Ex. messagerie SaaS	Externalisé	PROD			
...					

Schéma 1 — Cinématique des sauvegardes du contexte PROD. **Schéma 2** — Cinématique des sauvegardes du contexte Hors PROD.

Tableau 2 — Caractéristiques de chaque sauvegarde.

Sauvegarde	Fréquence	Règle de planification	Versions	Rétention maximale	Localisation	Immuable / isolée
Ex. quotidienne incrémentale	1 j	Fenêtre nocturne, {{HEURE}}	15	15 j	{{SITE_A}} + copie dans le coffre isolé	Non / Oui
Ex. instantané	12 h	Deux fois par jour, {{HEURES}}	2	24 h	Baie primaire	Non
...						

9.4 Couverture des scénarios d'indisponibilité

Principes directeurs de restauration pour un retour au mode nominal global.

9.4.1 ILP ou nominal dégradé

- Les données actives ou historiques (§5.1) impactées sont restaurées à partir des sauvegardes disponibles.
- Les données mortes impactées sont reconstituées à partir des sauvegardes disponibles sur un autre site ou une autre source.

9.4.2 IPP

- Les dispositifs de haute disponibilité assurent la sécurité des données primaires.
- Les données qui n'en bénéficient pas sont couvertes par les mesures du scénario ILP.

9.4.3 ILG

Dispositions détaillées au §8.4, en particulier :

- suspension de tous les services PROD et Hors PROD jusqu'au diagnostic ;
- sauvegarde « à la demande » généralisée de la PROD ;
- restauration à partir des dispositifs de sauvegarde et de restauration rapides (snapshots, clones), **après vérification de leur intégrité** ;
- application du même point de restauration à toutes les données, pour une PDMA homogène ;
- en cas de corruption des sauvegardes principales, restauration depuis les copies isolées : DMIA de 7 jours, PDMA dépendant de la disponibilité de ces copies.

Le volume impose de **prioriser** les restaurations selon la disponibilité attendue des applications :

Étape	Périmètre
0 (ajout)	Infrastructure de sauvegarde et coffre, poste d'administration sain, gestion des secrets
1	Services d'infrastructure : annuaire, DNS, DHCP, PKI, pare-feu, antivirus / EDR
2	Systèmes d'exploitation et hyperviseurs
3	Services IT transverses : messagerie, ordonnancement, supervision
4	Fonctions support et ressources d'analyse d'impact : centre de services, gestion des incidents, référentiel des sources applicatives, CMDB
5 et suivantes	Données métier, selon les critères de disponibilité de la CMDB et les dépendances entre applications

9.4.4 IPG

La sécurisation repose sur le dispositif d'externalisation et d'isolation des sauvegardes (§5.14). L'ordre de priorité de reconstruction est celui du §9.4.3, sur l'infrastructure de repli.

9.5 Modalités préétablies de gestion des incidents

Un incident sur un traitement de sauvegarde réduit le niveau de sécurité des données associées. La reprise ou l'abandon du traitement dépend de la récurrence de l'incident, de la criticité des données et de la fréquence du traitement.

Données	Traitement	Règle de reprise
Critiques	Tous	Sauvegarde réalisée dans le respect de la PDMA. À défaut, alerte des métiers .
Non critiques	Quotidien	Abandonné une fois (repris au cycle suivant)
	Hebdomadaire	Repris une fois
	Mensuel ou plus espacé	Repris jusqu'à réalisation
	Tous	En cas de non-respect, alerte des métiers

⚠ Deux abandons consécutifs d'un traitement quotidien constituent un incident à part entière (§7.4.1) [À VALIDER].

10. Offres Spécifiques de Sauvegarde (OSS)

Des OSS peuvent être constituées à la demande d'un ou plusieurs métiers. Elles complètent l'OGS sans pouvoir en réduire la portée, et peuvent porter sur tout ou partie de ses aspects.

Elles sont construites en mode projet :

1. le métier exprime son besoin complémentaire de sécurisation ;
2. le DARCH réalise une étude des moyens complémentaires et de leurs conséquences sur le SI et son exploitation ;
3. l'étude chiffrée est présentée au métier pour validation et budgétisation ;
4. en cas de validation, une annexe à la convention de service est établie.

Exemples d'OSS : PDMA quasi nulle par journalisation continue, rétention prolongée, pré-production sauvegardée, sauvegarde renforcée d'un service SaaS.

11. Maîtrise des activités de sécurisation

11.1 Maîtrise des risques liés à la stratégie

Toute activité organisationnelle ou opérationnelle comporte des risques. La matrice ci-dessous recense les principaux risques liés aux activités de la stratégie ; pour chacun, des métriques et un suivi adaptés sont à mettre en place.

Échelle — Criticité = Probabilité × Gravité, chacune notée de 1 (faible) à 3 (forte). Criticité de 1 (très faible) à 9 (certaine).

Activité	Faiblesse	Risque	P	G	C
Politique					
Mettre en place l'organisation et les moyens permettant le respect de la PSSI	Défaut de moyens	Retard de mise en œuvre ; MCO difficile	1	3	3
Aligner la gouvernance et les moyens sur les besoins	Multiplicité des canaux d'expression des besoins	Amélioration continue difficile	2	2	4
Stratégie					
Établir la stratégie	Incompréhension des enjeux ; délais de validation et de mise en œuvre	Retard de mise en œuvre	3	3	9
Organiser le suivi de la stratégie	Manque de sensibilisation ou de disponibilité	Stratégie non appliquée	2	3	6
Veiller à l'application opérationnelle	Défaut de communication sur les activités de sauvegarde et de restauration	MCO difficile	3	3	9
Établir les critères de disponibilité des services métier	Attentes de disponibilité fluctuantes	Surévaluation des besoins	2	2	4
Programme					
Aligner les programmes de sécurisation	Besoins d'évolution mal identifiés ; charge et planning non absorbables	Niveau de sécurisation en retard sur le besoin	1	3	3
Informers le DIO et le RPCI des évolutions planifiées	Stratégie non mise à jour	Sécurisation inadaptée	1	3	3
Intégrer les besoins de continuité dans le programme d'architecture	Planification pluriannuelle	Surdimensionnement des moyens hors haute disponibilité	2	2	4
Concevoir les évolutions de l'infrastructure	Besoins de continuité non pris en compte	Continuité non assurée par la haute disponibilité	2	2	4
Opérations					
Intégrer les principes et règles de la stratégie	Sauvegarde et restauration non alignées sur la stratégie	Sécurisation pilotée par la technique	2	3	6
Traduire la stratégie en méthodes et procédures	Manque de ressources et de moyens	Procédures incomplètes ou non conformes à la stratégie	3	2	6
Veiller au respect des méthodes et règles	Manque de disponibilité	Méconnaissance du niveau réel de sécurisation	2	3	6
Mettre en œuvre les méthodes	Manque de ressources et de moyens	Méconnaissance du niveau de sécurisation ; sécurisation pilotée par la technique	3	2	6
Établir les procédures du plan de sauvegarde	Manque de ressources et de moyens	Non-respect de la PDMA ou de la DMIA	3	2	6

Activité	Faiblesse	Risque	P	G	C
Réaliser les restaurations à la demande	Sauvegardes indisponibles	Non-respect de la PDMA ou de la DMIA	2	3	6
Garantir l'opérabilité des moyens	Difficultés de restauration	Non-respect de la DMIA	1	3	3
Protéger l'infrastructure de sauvegarde (<i>ajout</i>)	Administration partagée avec la production ; absence d'immuabilité	Destruction des sauvegardes lors d'une cyberattaque	2	3	6
Validation					
Décrire les scénarios de continuité	Scénarios non identifiés ; documentation absente, inadaptée ou incomplète	Validation des scénarios difficile	2	3	6
Organiser les exercices (volet organisationnel)	Erreur d'exécution des scénarios	Couverture incomplète ; non-respect d'obligations réglementaires	1	3	3
Piloter les exercices (volet opérationnel)	Manque de disponibilité ; concurrence avec les changements	Impact sur l'activité ; non-respect de la PDMA ou de la DMIA	2	3	6
Piloter les solutions de continuité en cas de sinistre	Niveau de continuité insuffisant	Impact sur l'activité métier	1	3	3
Sensibilisation					
Sensibiliser les intervenants	Manque de disponibilité et de compréhension des enjeux	Mise en œuvre difficile	3	2	6
Sensibiliser ses collaborateurs	Manque de disponibilité	Suivi de la mise en œuvre difficile	3	2	6
Reporting					
Transmettre au DSI les besoins d'évolution	Ressources et moyens inadaptés	Mise en œuvre et MCO difficiles ; perte de données	2	3	6
Prendre en compte les remontées du RPCI	Défaut de communication	Désalignement avec la stratégie	1	3	3
Reporting tactique	Activité non formalisée ; manque de disponibilité	Besoins de sécurité métier insuffisamment pris en compte	3	2	6
Reporting opérationnel	Éléments nécessaires mal identifiés ; manque de disponibilité	Orientation sécurité erronée ; manque de transparence	2	3	6
Produire les éléments du reporting opérationnel	Manque de disponibilité ; activité non formalisée ; éléments mal identifiés	Reporting sans valeur au regard des besoins métier	1	3	3
Incidents					
Suivre les écarts d'application de la stratégie	Activité non formalisée ; manque de visibilité	MCO difficile	3	3	9
Suivre les incidents de sauvegarde et de restauration	Activité non formalisée ; manque de visibilité	MCO difficile	3	3	9
Instruire les incidents affectant le plan de sauvegarde	Qualification sécurité des incidents insuffisante ; manque de visibilité	Amélioration continue inadaptée	3	3	9
Instruire les incidents de sauvegarde et de restauration	Qualification sécurité des incidents insuffisante ; manque de visibilité	Amélioration continue inadaptée	3	3	9
Plan de capacité					
Établir le plan de capacité	Manque de disponibilité	Sur- ou sous-dimensionnement	2	3	6

11.2 Indicateurs

Les indicateurs permettent à toutes les parties prenantes d'évaluer le risque résiduel et de vérifier le respect de la stratégie. Les exemples ci-dessous sont proposés **[À VALIDER]** ; seuils à fixer après une période de mesure initiale.

11.2.1 Indicateurs de gestion opérationnelle (IGO)

Construits et utilisés par les équipes d'exploitation pour le suivi courant. Ils portent sur chaque sauvegarde et restauration, quel que soit son type ou sa périodicité, déclinés par direction ou entité, par application et par environnement.

Indicateur	Formule	Cible indicative
Taux de réussite des sauvegardes	Sauvegardes réussies / sauvegardes planifiées	≥ 98 %
Taux de réussite des restaurations témoin	Témoins conformes / témoins exécutés	100 %
Délai de reprise des sauvegardes échouées	Temps moyen entre échec et réussite	< 24 h
Couverture du périmètre	Actifs sauvegardés / actifs de la CMDB soumis à l'OGS	100 %
Remplissage de la capacité	Capacité utilisée / capacité disponible	< 80 %

11.2.2 Indicateurs de gestion tactique (IGT)

Construits et utilisés par le RPCI, gestionnaire du processus de continuité, pour évaluer la maîtrise des risques, le respect des engagements, le respect de la stratégie par les intervenants et les besoins d'amélioration du processus.

Indicateur	Formule	Cible indicative
Respect de la PDMA	Actifs dont la dernière sauvegarde valide respecte la PDMA / actifs couverts	≥ 99 %
Couverture des tests de restauration	Applications critiques restaurées avec succès sur 12 mois / applications critiques	100 %
Couverture de l'isolation	Données critiques disposant d'une copie immuable ou isolée / données critiques	100 %
Écart DMIA en exercice	DMIA mesurée / DMIA engagée	≤ 1
Actions correctives en retard	Actions échues non soldées / actions ouvertes	< 10 %

11.2.3 Indicateurs de gestion stratégique (IGS)

Constitués par le DIO à partir des informations de ses responsables de service et du RPCI, ils aident au pilotage des directions concernées par la continuité.

Indicateur	Contenu
Niveau de conformité à la stratégie	Synthèse pondérée des IGT
Exposition résiduelle	Scénarios dont l'engagement n'est pas démontré par un exercice
Tendance des incidents majeurs	Nombre et gravité sur 12 mois glissants
Avancement du plan d'action	Réalisé / prévu

11.3 Suivi et contrôle

Les indicateurs font l'objet d'un suivi permettant d'en interpréter l'évolution et d'acter les évolutions, maintenances et corrections à apporter aux activités.

11.3.1 Niveau opérationnel

Suivi assuré par le **Responsable de Production**. Contrôle par le **RPCI**, qui :

- analyse le rapport mensuel de synthèse des incidents de sauvegarde (§7.4.2) ;
- réalise un contrôle mensuel des sauvegardes par échantillonnage aléatoire ;
- fait réaliser au moins un audit annuel des sauvegardes sur un périmètre technique ou fonctionnel complet.

En cas de dysfonctionnement, le RPCI s'assure que l'anomalie est référencée ; la remise en état relève de la gestion des incidents.

11.3.2 Niveau tactique

Suivi assuré par le **RPCI**, pour vérifier l'effectivité et l'efficacité des sauvegardes et identifier le niveau de sécurisation des données et les besoins de remise à niveau.

Contrôle par le **DIO**, qui vérifie le respect de la stratégie par l'ensemble des intervenants, détermine les évolutions de gouvernance nécessaires et identifie le besoin de révision.

11.3.3 Niveau stratégique

Suivi assuré par le **DIO** ; contrôle par le **DSI**, avec information du **RSSI**.

11.4 Reporting

Les activités de suivi et de contrôle alimentent des reportings réguliers et planifiés qui permettent :

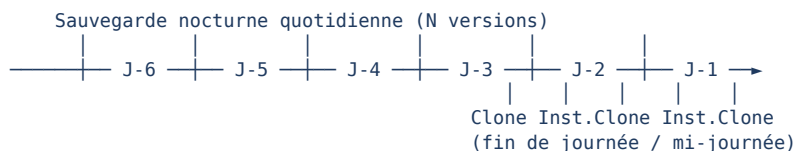
- d'établir une « météo » de la sauvegarde ;
- de consolider l'historique ;
- de s'appuyer sur des indicateurs pertinents, reflétant fidèlement l'activité ;
- de partager l'information avec les parties prenantes.

Rapport	Émetteur	Fréquence	Destinataires
Synthèse des incidents de sauvegarde	RPROD	Mensuelle	RPCI, {{INSTANCE_TACTIQUE}}
Respect de la stratégie	RPCI	Trimestrielle	DSI, DIO, RSSI, RPCA, DARCH, RPROD
Tableau de bord stratégique	DIO	Semestrielle	DSI, comité stratégique
Bilan annuel des exercices	RPCI	Annuelle	Comité stratégique, métiers

12. Annexes

Annexe A — Cinématique de sauvegarde et de restauration selon l'ampleur du sinistre

Exemple de cinématique [À ADAPTER] combinant sauvegardes nocturnes, instantanés et clones. Les horaires sont à fixer selon les fenêtres de **{{ORGANISATION}}**.



Ampleur	Situation	Moyen de restauration	PDMA	DMIA
Locale	Destruction ou corruption limitée à un serveur ou une base de données	Sauvegardes nocturnes : choix du point de restauration parmi les versions disponibles	1 à 35 jours selon la date de l'altération	≤ 12 h
Massive	Destruction ou corruption à grande échelle	Instantané (12 h) ou clone (00 h) le plus récent antérieur à l'incident	12 h (instantané) ou 24 h (clone)	Quelques heures

⚠ Les instantanés et clones résidant sur la même baie ou dans le même domaine d'administration que les données primaires ne protègent pas d'une compromission de ce domaine. En ILG, ils ne sont utilisables qu'après vérification de leur intégrité (§9.4.3).

Annexe B — Affectation des rôles

[À COMPLÉTER] — Renseigner les fonctions plutôt que les noms lorsque le document est largement diffusé ; tenir la liste nominative dans un registre séparé, mis à jour à chaque mouvement.

Rôle	Acronyme	Fonction dans l'organisation	Titulaire	Suppléant
Propriétaires métier (un par activité prioritaire)	MÉT			
Directeur des Systèmes d'Information	DSI			
Responsable de la Sécurité des SI	RSSI			
Directeur des Infrastructures et des Opérations	DIO			
Responsable du Plan de Continuité Informatique	RPCI			
Responsable de Production	RPROD			
Responsable du Plan de Continuité d'Activité	RPCA			
Directeur de l'Architecture	DARCH			
Administrateur des moyens de production	AdMP			
Administrateur de sauvegardes	AdSv			

Annexe C — Types de sauvegarde

Type	Principe	Usage recommandé	Avantages	Limites
Complète (full)	Copie de toutes les données du support d'origine (logique ou physique) sur un support distinct	Données vivantes ; peu recommandée comme usage exclusif en raison de sa durée	Restauration simple, en une seule étape	Longue ; impacte la disponibilité pendant la sauvegarde et la restauration (DMIA, D au sens DICP)
Différentielle	Copie des données modifiées depuis la dernière sauvegarde complète	Historisation sur longue période ; usage en recul au profit de l'incrémentale	Restauration en deux étapes (complète + dernière différentielle)	Volume croissant jusqu'à la complète suivante ; impact sur la disponibilité
Incrémentale	Copie des données modifiées depuis la dernière sauvegarde, quel que soit son type	Données à fort taux de modification ; historisation sur longue période	Rapide et économe ; peut être le seul type utilisé (la première incrémentale équivaut à une complète)	Restauration nécessitant la reconstruction de la chaîne ; mise en œuvre plus complexe
Par journalisation (logging)	Chaque création, modification ou suppression est journalisée sur un support indépendant	Bases de données	Restauration à n'importe quel état (point dans le temps)	Restauration assimilable à une reconstruction depuis le dernier état complet ; exploitation complexe
Par réplication	Duplication synchrone de chaque donnée sur un support distinct	Données vivantes, face au sinistre physique	Mise en œuvre simple ; PDMA nulle face à une panne	Réplique aussi les corruptions et chiffréments ; inapplicable aux archives ; coût équivalent au stockage primaire
Par clonage	Copie intégrale à un instant donné sur un support distinct	Données exigeant une restauration très rapide (le clone peut remplacer le support d'origine)	Restauration quasi instantanée	Une seule version par clone ; coût équivalent au stockage primaire
Par instantané (snapshot)	Image logique reposant sur le support d'origine	Données exigeant une restauration très rapide	Coût limité à la réserve allouée (souvent de l'ordre de 30 % du volume)	Dépend de la disponibilité du support d'origine ; ne protège pas d'une perte de la baie

Note sur les outils actuels — Les solutions de sauvegarde modernes proposent :

- des sauvegardes **incrémentales au niveau bloc**, indépendantes du format logique des données, qui optimisent l'usage des supports et des matériels, augmentent les débits et réduisent l'impact sur les données vivantes ;
- des **restaurations consolidées** au niveau logique : restauration au niveau bloc pour privilégier la vitesse, ou au niveau des structures de données (fichier, base, objet) pour la granularité ;
- des fonctions d'**immutabilité**, de **détection d'anomalies** et d'**analyse des copies** avant restauration, qui répondent spécifiquement au scénario ILG.

Annexe D — Glossaire

Sigle	Signification
AdMP	Administrateur des moyens de production

Sigle	Signification
AdSv	Administrateur de sauvegardes
BIA	<i>Business Impact Analysis</i> — analyse d'impact sur l'activité
CMDB	Base de données de gestion des configurations
DARCH	Directeur de l'Architecture
DICP	Disponibilité, Intégrité, Confidentialité, Preuve
DIO	Directeur des Infrastructures et des Opérations
DMIA	Durée Maximale d'Interruption Admissible — dans ce document, engagement de restauration de la DSI (RTO informatique) ; voir §5.2
DSI	Directeur (ou Direction) des Systèmes d'Information
IGO / IGT / IGS	Indicateurs de gestion opérationnelle / tactique / stratégique
MBCO	<i>Minimum Business Continuity Objective</i> — niveau minimal d'activité à assurer pendant une perturbation
MÉT	Propriétaires métier
MTPD	<i>Maximum Tolerable Period of Disruption</i> — durée d'interruption maximale tolérable
ILG / ILP	Indisponibilité Logique Globale / Partielle
IPG / IPP	Indisponibilité Physique Globale / Partielle
ITSM	Gestion des services informatiques
MCO	Maintien en condition opérationnelle
OGS / OSS	Offre Générale / Spécifique de Sauvegarde
PAS	Plan d'Assurance Sécurité
PCA / PCI	Plan de Continuité d'Activité / Informatique
PDMA	Perte de Données Maximale Admissible — dans ce document, engagement de point de restauration de la DSI (RPO informatique) ; voir §5.2
PRI	Plan (ou site) de Reprise Informatique
PSSI	Politique de Sécurité des Systèmes d'Information
RPCA / RPCI	Responsable du Plan de Continuité d'Activité / Informatique
RPROD	Responsable de Production
RSSI	Responsable de la Sécurité des Systèmes d'Information
RTO / RPO	<i>Recovery Time Objective / Recovery Point Objective</i> — objectifs de délai et de point de reprise
WORM	<i>Write Once, Read Many</i> — support ou mode d'écriture non modifiable

Annexe E — Liste de contrôle d'adaptation

#	Élément à produire ou arbitrer	Section	Porteur suggéré	Fait
1	Nommer le propriétaire de la stratégie et fixer l'échéance d'application	§3	DSI	☐
2	Table de correspondance avec la PSSI	§4.3	RSSI	☐
3	Nombre et liste des environnements fonctionnels	§5.8	RPROD	☐
4	Dispositif de sanctuarisation retenu	§5.14	DIO	☐
5	Durées de rétention compatibles avec le registre des traitements	§5.13	DPO	☐
6	Inventaire SaaS / cloud et solution de sauvegarde associée	§6.2.6	DARCH	☐
7	Rattachement de la comitologie aux instances existantes	§7.3	RPCI	☐
8	Schéma d'architecture et rôle de chaque site	§8.1	DARCH	☐
9	Solution d'hébergement de repli pour l'IPG	§8.2	DIO	☐
10	Tableaux de gravité, probabilité et criticité (actuel et cible)	§8.7	RPCI	☐
11	Liste des prestations sous PAS	§8.8.2	Achats / RSSI	☐
12	Validation métier des engagements DMIA / PDMA, dont ILG cyber et IPG	§9.1	RPCA	☐
13	Textes réglementaires imposant un test annuel	§9.2.2	Conformité	☐
14	Plan de sauvegarde détaillé (tableaux 1 et 2, schémas 1 et 2)	§9.3	AdSv	☐

#	Élément à produire ou arbitrer	Section	Porteur suggéré	Fait
15	Seuils des indicateurs après période de mesure	\$11.2	RPCI	☐
16	Affectation nominative des rôles, dont les propriétaires métier	Annexe B	DSI	☐
17	Analyse d'impact de référence et classes de criticité	\$5.2, \$9.1	RPCA	☐
18	Validation formelle de l'exclusion du sinistre total	\$6.3.1	Direction générale	☐
19	Raccordement à la cellule de crise et à la réponse à incident	\$8.4	RPCA / RSSI	☐
20	Copies hors SI de la documentation critique	\$7.6	RPCI	☐

Fin du document.

Modèle Plan R — plan-r.org — licence Creative Commons Attribution - Pas d'utilisation commerciale - Partage dans les mêmes conditions 4.0 International (CC BY-NC-SA 4.0), <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.fr>. Vous pouvez le copier, l'adapter et le diffuser, à condition de citer la source, sans usage commercial, et de diffuser vos adaptations sous la même licence.