Luxgap

DATA PRIVACY PARTNER

LUXGAP

CONTINUITÉ D'ACTIVITÉ

BCMS / BCP as-a-Service

Un système de management de la continuité d'activité **conforme ISO 22301**, aligné **NIS2** et **DORA**, maintenu en continu et accessible en toutes circonstances.

Julien Winkin – Julien.winkin@luxgap.com +352 621 583 116

CHAPITRE 1 ENJEUX & CADRE RÉGLEMENTAIRE

Pourquoi un BCMS/BCP "always-on" ?

Continuité d'activité = exigence réglementaire + résilience opérationnelle

Un BCP « statique » — un document rangé dans un dossier partagé et rarement mis à jour — est rarement utilisable le jour où la crise survient. Les organisations qui subissent une interruption majeure découvrent souvent trop tard que leurs plans sont obsolètes, que les contacts ont changé, que les dépendances IT ont évolué ou que les procédures ne correspondent plus à la réalité opérationnelle. L'offre **Luxgap** répond à ce constat en mettant en place et en maintenant un **système de management de la continuité d'activité (BCMS)** conforme à la norme **ISO 22301**, testé au minimum une fois par an, et accessible même en cas d'indisponibilité totale de votre infrastructure.

NIS2 (Dir. UE 2022/2555)

- Mesures de gestion des risques cyber imposées aux entités « essentielles » et « importantes »
- Inclut explicitement la continuité d'activité : gestion de crise, sauvegardes, reprise après sinistre
- Approche « state of the art » et alignement sur des standards reconnus (ISO 22301 / ISO 27001)

DORA (Règl. UE 2022/2554)

- Obligation directe pour le secteur financier : plans ICT de continuité, réponse et rétablissement
- BIA exigée + tests périodiques des plans, y compris ceux impliquant des fournisseurs ICT tiers
- Traçabilité et preuve d'efficacité : audits, rapports d'exercices, actions correctives documentées

Résultat attendu

Décisions rapides

Rôles prédéfinis, critères d'escalade clairs, priorités établies à l'avance pour agir sans hésitation dans les premières minutes critiques d'un incident.

RTO/RPO tenables

Objectifs de rétablissement définis et validés pour chaque processus, système IT et prestataire critique, garantissant des délais de reprise réalistes et mesurables.

Communication maîtrisée

Plans de communication pré-validés pour les clients, autorités de supervision, partenaires et médias, réduisant le risque réputationnel et les obligations de notification.

Dossier d'audit prêt

Ensemble complet de preuves auditables aligné ISO 22301, NIS2 et DORA : politiques, rapports d'exercices, CAPA, revues de direction et registres de changements.

CHAPITRE 2 PORTAIL DE CONTINUITÉ

BCP accessible en toutes circonstances

Site web indépendant de votre infrastructure — option d'accès « break-glass » garantissant la disponibilité même en cas de sinistre total

L'un des principaux écueils des plans de continuité traditionnels est leur inaccessibilité au moment où ils sont le plus nécessaires. Si vos plans sont stockés sur un serveur interne, un SharePoint ou un intranet, une cyberattaque de type ransomware ou une panne d'infrastructure les rend justement indisponibles au moment critique. Le portail Luxgap résout ce paradoxe en hébergeant l'intégralité de votre BCMS sur une infrastructure dédiée, totalement indépendante de votre SI.

Structure du portail de continuité

- **Page « crash total »** : que faire dans les 0–60 premières minutes — checklists d'activation immédiate, décisions critiques à prendre, contacts prioritaires
- **Arbre d'escalade** : seuils de déclenchement, niveaux de priorité, critères d'activation formelle du BCMS
- **Comité de crise** : rôles, responsabilités, remplaçants désignés, coordonnées multi-canaux
- **Plans opérationnels** : ITDR/DRP, continuité métiers, communications de crise, gestion fournisseurs
- **Annexes pratiques** : inventaires d'actifs, procédures manuelles de contournement, modèles de messages pré-validés
- **Exports offline** : PDF téléchargeables + sauvegarde chiffrée de l'ensemble des contenus

Garanties opérationnelles

Accès 24/7

Disponibilité permanente même si l'ensemble de vos serveurs internes est indisponible. Infrastructure hébergée de façon indépendante avec redondance géographique.

Contrôle d'accès & journalisation

Authentification sécurisée et journaux d'accès horodatés constituant des preuves d'utilisation exploitables lors d'audits ou d'investigations post-incident.

Mise à jour continue

Chaque changement organisationnel ou IT déclenche une mise à jour du BCMS. Le portail reflète en permanence la réalité opérationnelle de votre organisation.

Traçabilité complète

Versioning intégral de tous les documents et registre des changements horodaté, garantissant une piste d'audit continue et la conformité réglementaire.

CHAPITRE 3 NOTRE OFFRE

Offre « BCMS as-a-Service » (tout inclus)

Mise en place + maintien + preuves d'audit + exercices annuels (minimum) — le tout dans un **abonnement mensuel** aligné **ISO 22301 / NIS2 / DORA** avec une **gestion continue des risques**.

Notre offre « tout compris » couvre l'intégralité du cycle de vie du BCMS, de l'implémentation initiale au maintien opérationnel en passant par les exercices et la production de preuves auditables. Cette approche « as-a-Service » élimine la charge de gestion interne tout en garantissant un niveau de maturité constant et démontrable.

Implémentation initiale

- Cadrage : périmètre, parties intéressées, exigences réglementaires applicables
- BIA + Risk Assessment (scénarios de disruption) + cartographie complète des dépendances
- Définition RTO/RPO/MTPD par processus et services critiques
- Stratégies & solutions : people / premises / technology / suppliers / data
- Rédaction des plans et procédures : crise, communication, continuité, ITDR

Run & maintien continu

- Cycle PDCA : objectifs, KPI/KRI, revues périodiques, actions correctives
- Gestion des changements (IT, prestataires, organisation) avec mise à jour immédiate
- Mise à jour continue du portail BC + contrôle strict de versions
- Sensibilisation et formation : managers, équipes opérationnelles, astreintes
- Veille réglementaire : évolutions NIS2/DORA + standards « state of the art »

Exercices & preuves

- Exercice annuel de simulation (tabletop + communication de crise)
- Test(s) technique(s) ciblé(s) si ITDR inclus (restauration, bascule)
- Rapport d'exercice + REX structuré + plan d'actions (CAPA)
- Audit interne ISO 22301 + revue de direction annuelle
- Dossier d'audit prêt pour certification (si souhaitée)

CHAPITRE 4 ISO 22301 EN DÉTAIL

ISO 22301:2019 — Exigences (clauses 4 à 10)

Le BCMS est un **système de management** (structure Annex SL) : **PDCA + preuves.** Il ne s'agit pas d'un simple document, mais d'un dispositif vivant de planification, d'exécution, de vérification et d'amélioration continue.

PLAN
Clauses 4–7 : Contexte, Leadership, Planification, Support

DO
Clause 8 : BIA/Risques, Stratégies, Plans, Exercices

ACT
Clause 10 : CAPA, Amélioration continue

CHECK
Clause 9 : KPI/KRI, Audit interne, Revue de direction

Ce que « conforme ISO 22301 » implique (sans compromis)

01

Périmètre, politiques, rôles et responsabilités formalisés

Le BCMS doit reposer sur un cadre documenté, validé par la direction, avec des autorités clairement attribuées à chaque niveau de l'organisation.

02

Processus BIA + évaluation des risques de disruption

Analyse d'impact et identification des scénarios de menace, revues périodiquement pour refléter l'évolution de l'environnement opérationnel et technologique.

03

Stratégies et solutions validées

Couverture complète des ressources critiques : personnes, sites, IT, données et prestataires, avec des solutions testées et documentées.

04

Plans et procédures exécutables + communication

Documents opérationnels prêts à l'emploi, incluant la communication interne et externe de crise avec des modèles pré-validés.

05

Programme d'exercices/tests + amélioration continue

Validation régulière de l'efficacité des dispositifs avec boucle de retour d'expérience structurée et actions correctives tracées.

06

Contrôle documentaire et enregistrements auditables

Maîtrise documentaire rigoureuse : versioning, approbations, diffusion contrôlée et conservation des preuves pour chaque exigence.

Tout est maintenu dans le temps — un BCMS n'est pas un document figé mais un système vivant qui évolue avec votre organisation, vos technologies et votre environnement réglementaire.

ISO 22301 — Clauses 4 à 6 (cadrage & gouvernance)

Fondations du BCMS : contexte de l'organisation, engagement de la direction, planification des objectifs et des actions.

Les clauses 4 à 6 constituent le socle sur lequel repose l'ensemble du système de management. Elles définissent le « pourquoi » et le « comment » du BCMS avant même la production des plans opérationnels. Sans ces fondations solides, les plans de continuité manquent d'ancrage stratégique et de légitimité organisationnelle.

1

Clause 4 — Contexte

- Analyse du contexte interne et externe + identification des parties intéressées et de leurs attentes
- Définition du périmètre BCMS (services, sites, entités) avec justification des exclusions éventuelles
- Cartographie des processus et des dépendances critiques : personnes, IT, données, fournisseurs
- Registre des exigences applicables : NIS2, DORA, obligations contractuelles, exigences sectorielles

2

Clause 5 — Leadership

- Politique de continuité validée par la direction + définition d'objectifs BC mesurables
- Attribution des rôles et autorités : sponsor direction, BC manager, owners métiers, ITDR, communications
- Constitution du comité de crise : suppléance assurée, règles de décision formalisées, call-tree opérationnel
- Intégration du BCMS dans les processus existants : gestion des risques, conformité, achats, IT

3

Clause 6 — Planification

- Identification des risques et opportunités liés au BCMS + plan d'actions priorisé
- Objectifs mesurables : RTO/RPO cibles, délais d'activation, taux de réussite des tests
- Planification des changements anticipés : migration cloud, M&A, changements de prestataires
- Critères de déclenchement, niveaux d'escalade et conditions de retour à la normale

ISO 22301 CLAUSE 7 — SUPPORT

ISO 22301 — Clause 7 (Support)

Compétences, sensibilisation, communication, maîtrise documentaire — les ressources indispensables au fonctionnement du BCMS

La clause 7 garantit que les personnes disposent des compétences nécessaires, que les canaux de communication sont définis et testés, et que l'ensemble de la documentation est maîtrisée. Ces éléments de « support » sont souvent sous-estimés mais constituent la colonne vertébrale opérationnelle du système.

Livrables « Support » inclus dans l'abonnement

Compétences & awareness

- Plan de compétences détaillé : qui doit savoir faire quoi, et à quel moment
- Matrice de formation couvrant les crisis leaders, équipes ITDR, métiers, accueil et communications
- Sensibilisation continue : rappels périodiques, intégration onboarding, participation aux exercices
- Registre des habilitations « break-glass » et des suppléances formalisées

Communication maîtrisée

- Plan de communication de crise (interne et externe) avec modèles de messages pré-validés
- Annuaire de contacts priorisés : clients clés, autorités de supervision, prestataires critiques
- Canaux alternatifs définis : téléphone/SMS, messagerie hors SI, site web BC dédié
- Gestion des médias et cohérence des messages pour réduire le risque réputationnel

Documents & preuves

- Maîtrise documentaire complète : versioning, approbation, diffusion contrôlée
- Traçabilité : preuves d'exercices, comptes rendus de crise, CAPA documentés
- Registre des changements et des écarts (non-conformités identifiées)
- Conservation structurée des enregistrements (evidence pack audit)

ISO 22301 | CLAUSE 8.2 — BIA & RISQUES

ISO 22301 — Clause 8.2 (BIA + évaluation des risques)

Base factuelle : impact, priorités, objectifs de rétablissement — le socle analytique de toute stratégie de continuité

BIA (Business Impact Analysis)

L'analyse d'impact sur les activités constitue le fondement du BCMS. Elle établit de manière objective quelles activités sont critiques, dans quels délais elles doivent être rétablies, et quelles ressources sont indispensables à leur fonctionnement.

1 Inventaire des activités et processus

Classification par niveau de criticité : « critique / important / support ». Chaque processus est évalué en fonction de son rôle dans la chaîne de valeur et de son impact en cas d'interruption.

2 Analyse des impacts par horizon temporel

Évaluation multi-dimensionnelle : financier, légal/réglementaire, clients, sécurité des personnes, réputation. Les impacts sont projetés sur différents horizons (1h, 4h, 24h, 72h, 1 semaine…).

3 MTPD / MTPoD + RTO et RPO

Définition de la durée maximale tolérable d'interruption (MTPD) et des objectifs de temps de reprise (RTO) et de point de reprise (RPO) pour chaque processus et service critique.

4 Cartographie des dépendances

Identification exhaustive des ressources nécessaires : applications, bases de données, personnes clés, sites physiques, fournisseurs et prestataires tiers.

Évaluation des risques de disruption

- **Scénarios évalués :** cyberattaque/ransomware, panne critique (SI, réseau, cloud), perte ou corruption de données, indisponibilité d'un fournisseur ICT majeur, sinistre physique du site
- **Méthode :** probabilité × gravité × détectabilité ⟶ priorisation des risques et identification des besoins en contrôles
- **Mesures préventives & de résilience :** backup, segmentation réseau, redondance, procédures manuelles de contournement
- **Revues planifiées** + revues « à chaud » après chaque incident significatif ou changement majeur de l'environnement

Sorties BCMS (pilotage)

- RTO/RPO consolidés
- Priorisation de rétablissement
- Liste des ressources critiques
- Exigences contractuelles fournisseurs
- Backlog d'amélioration priorisé

ISO 22301 | CLAUSE 8.3 — STRATÉGIES & SOLUTIONS

ISO 22301 — Clause 8.3 (stratégies & solutions)

Choisir des solutions réalistes pour tenir les RTO/RPO

À partir des exigences issues du BIA et de l'évaluation des risques, nous concevons et validons des stratégies de continuité « de bout en bout » couvrant l'ensemble des ressources critiques : personnes, lieux, technologies, données et chaîne de fournisseurs. L'objectif est de garantir que chaque stratégie est non seulement documentée mais surtout réaliste, testée et maintenue dans le temps.

Axes de solutions

People

Ressources critiques identifiées, suppléance formalisée, astreintes définies, accès « break-glass » aux systèmes essentiels en cas d'indisponibilité des personnes habituelles.

Premises

Télétravail activable, sites alternatifs pré-identifiés, accès physique sécurisé, procédures d'évacuation et de repli documentées.

Technology

Architecture de reprise définie, procédures de restauration et de bascule documentées, runbooks techniques testés et versionnés.

Data

Stratégie de sauvegarde 3-2-1, immutabilité des sauvegardes, restauration régulièrement testée, conformité aux RPO définis.

Suppliers

Clauses BC intégrées aux contrats, exigences RTO/RPO communiquées, plans de remplacement et stratégies d'exit documentés.

Décisions de conception

- **Niveaux de service par criticité** (bronze/argent/or) et par processus, permettant un dimensionnement proportionné des solutions
- **Rétablissement par « wave »** : priorités, dépendances et séquencement documentés pour une reprise ordonnée
- **Critères d'acceptation** : tests, métriques, preuves et contrôles définis pour valider chaque solution
- **Mesures de résilience cyber** : segmentation réseau, MFA, contrôle des accès administrateurs, journalisation
- Alignement ITDR ↔ continuité métier pour éviter les « plans en silo » qui se contredisent le jour J

Livrables

- Stratégie BC consolidée (par scénario et criticité)
- Catalogue des solutions + coûts / efforts / dépendances
- Exigences fournisseurs & clauses contractuelles
- Runbooks ITDR et checklists métiers
- Matrice de priorisation (ré-activation)

ISO 22301 | CLAUSE 8.4 — PLANS & PROCÉDURES

ISO 22301 — Clause 8.4 (plans & procédures)

Des documents exécutables, disponibles et entraînés — des plans que vos équipes peuvent réellement utiliser sous pression

Pack de plans « ready-to-run » inclus

1

Plan de gestion de crise

Activation du dispositif, processus de décision, tenue du journal de crise, critères de fin de crise et de retour au mode normal.

2

Plan de communication

Communication interne et externe coordonnée avec « message map » pré-validée pour chaque audience : collaborateurs, clients, régulateurs, médias.

3

Plan de continuité métier

Workarounds opérationnels, priorités de rétablissement, ressources nécessaires et délégations d'autorité pour maintenir les activités critiques.

4

ITDR / DRP

Restauration, bascule, rebuild des systèmes critiques avec runbooks techniques détaillés et séquencés.

5

Plan fournisseurs critiques

SLA de continuité, procédures d'escalade, alternatives pré-identifiées et exit plan pour chaque fournisseur critique.

6

Plan de retour à la normale

Retour contrôlé aux opérations normales, post-mortem structuré et plan d'actions correctives (CAPA).

Scénarios prêts à l'emploi

Chaque scénario inclut : **actions immédiates (0–60 min)**, **responsables & contacts**, **décisions / critères d'escalade**, **communications pré-rédigées** et **procédure de retour à la normale**.

- Cyberattaque / Ransomware
- Panne critique (SI, réseau, cloud)
- Perte / corruption de données
- Indisponibilité fournisseur ICT
- Catastrophe / sinistre site
- Indisponibilité RH (pandémie, grève)

ISO 22301 | CLAUSES 8.5 & 8.6 — EXERCICES & ÉVALUATION

ISO 22301 — Clauses 8.5 & 8.6 (exercices & évaluation)

Tester, mesurer, corriger : au minimum 1 exercice par an + après chaque changement majeur

Le programme d'exercices valide l'efficacité réelle des stratégies et des plans en conditions simulées. Il produit des preuves documentées et exploitables lors d'audits de certification, de contrôles par les autorités de supervision ou de due diligence clients. Un plan non testé n'est qu'une hypothèse.

Typologie d'exercices

Tabletop

Simulation de gestion de crise : décisions, escalade, priorisation, coordination du comité de crise dans un scénario réaliste.

Call-tree / mobilisation

Test des temps de contact et de prise de rôle effective. Vérification de la joignabilité et de la réactivité des équipes.

Exercice communication

Simulation de notification aux clients, régulateur et presse avec utilisation des messages pré-validés.

Test technique ITDR

Restauration, bascule et exécution des runbooks en environnement de test — si le périmètre ITDR est inclus.

Exercice fournisseurs

Coordination avec les prestataires critiques : SLA, points de bascule, procédures d'exit et de remplacement.

Gouvernance du test annuel

- **Scénario défini sur base des risques et du BIA** avec des objectifs mesurables et des critères de réussite clairs
- **Rôles observateurs** désignés + critères de réussite : RTO/RPO atteints, time-to-decision, qualité des communications
- **Journal d'événements** tenu en temps réel et collecte d'évidences structurées pendant l'exercice
- **REX structuré** (analyse des causes racines) + plan d'actions (CAPA) priorisé avec owners et échéances
- **Mise à jour des plans** et revalidation formelle après intégration des corrections identifiées

Sorties auditables

1. Plan d'exercice
2. Rapport d'exercice
3. CAPA & suivi
4. Évaluation formelle
5. Mise à jour portail

ISO 22301 | CLAUSES 9 & 10 — AUDIT & AMÉLIORATION

ISO 22301 — Clauses 9 & 10 (mesure, audit, amélioration)

Prouver la maîtrise et améliorer en continu — le BCMS ne se contente pas d'exister, il doit démontrer son efficacité de manière tangible et continue.

Clause 9 — Évaluation des performances

KPI / KRI

Couverture BIA, taux de mise à jour des plans, réussite des exercices, délais de rétablissement mesurés vs. objectifs.

Audit interne ISO 22301

Programme d'audit structuré, checklists par clause, constats documentés et preuves collectées.

Revue de direction

Évaluation de l'adéquation du BCMS, allocation des ressources, décisions stratégiques et priorisation des actions.

Reporting direction / risques

Tableau de bord mensuel ou trimestriel synthétisant l'état du BCMS, les risques résiduels et les actions en cours.

Clause 10 — Amélioration

Gestion des non-conformités

Identification, documentation et traitement des écarts avec actions correctives formalisées (CAPA) et suivi jusqu'à clôture.

Amélioration post-incident & post-exercice

Retour d'expérience (REX) structuré après chaque incident significatif ou exercice, alimentant le cycle d'amélioration.

Traitement des changements majeurs

Nouveaux services, migrations cloud, outsourcings : chaque changement déclenche une réévaluation du BCMS.

Optimisation des procédures

Simplification, automatisation et renforcement de la robustesse des plans et procédures au fil du temps.

Evidence pack (audit-ready) maintenu en continu

L'ensemble des preuves requises par ISO 22301, NIS2 et DORA est collecté, organisé et maintenu à jour de manière proactive dans le portail de continuité. À tout moment, votre organisation dispose d'un dossier d'audit complet et exploitable, sans effort de préparation de dernière minute.

CHAPITRE 5 ALIGNEMENT RÉGLEMENTAIRE

Alignement ISO 22301 ↔ NIS2 ↔ DORA

ISO 22301 fournit le « système » ; NIS2 et DORA fixent des obligations juridiques.

Notre approche : utiliser ISO 22301 comme colonne vertébrale structurante et produire simultanément les preuves exigées par NIS2 (mesures de gestion des risques pour les entités essentielles et importantes) et DORA (résilience opérationnelle numérique pour le secteur financier). Un seul BCMS, trois cadres de conformité couverts.

ISO 22301 (livrable)	NIS2 — Mesures de gestion des risques	DORA — ICT BCP (réponse & rétablissement)	Bénéfice concret
8.2 BIA + risques	Continuité d'activité, gestion de crise, évaluation des risques imposées par la directive	BIA + scénarios de disruption ICT, base des plans de réponse et de rétablissement	Une seule analyse factuelle servant les trois référentiels
8.3 Stratégies / solutions	Sauvegardes, reprise, résilience, contrôles « state of the art »	Plans ICT, sauvegarde/restauration, solutions pour fonctions critiques	Stratégies validées et dimensionnées de bout en bout
8.4 Plans / procédures	Gestion de crise et continuité opérationnelle (exécution effective)	Réponse & rétablissement, communication, continuité fournisseurs ICT	Plans exécutables et testés, pas seulement documentés
8.5–8.6 Exercices / évaluation	Capacité démontrable (tests/exercices) + amélioration continue	Tests périodiques des plans ICT + preuve d'efficacité mesurable	Preuves d'efficacité exploitables par les superviseurs
9–10 Audit & amélioration	Gouvernance et mesures proportionnées, preuves d'exécution	Traçabilité, contrôle interne, reporting et remédiation	Dossier d'audit complet et toujours à jour

→ **Résultat :** une continuité opérationnelle **prouvable** et **auditable** — et non une simple « documentation » rangée dans un dossier partagé. Votre organisation peut démontrer à tout moment sa conformité aux trois cadres réglementaires avec un seul système de management.

CHAPITRE 6 CERTIFICATION

Certification ISO 22301 (possible)

Préparation incluse : documentation, preuves, audits internes, accompagnement — notre abonnement prépare et maintient un BCMS certifiable en permanence.

La certification ISO 22301 est un puissant levier de confiance auprès de vos clients, partenaires et autorités de supervision. Elle repose sur un audit externe mené par un organisme certificateur accrédité et démontre que votre système de management de la continuité n'est pas seulement documenté mais effectivement opérationnel et amélioré en continu.

Parcours vers la certification

1. Cadrage & périmètre
2. BIA & risques
3. Solutions & plans
4. Exercices & preuves
5. Audit interne
6. Revue direction
7. Audit Stage 1/2
8. Maintien (surveillance)

Répartition des responsabilités

Ce que Luxgap prend en charge

- Rédaction et maintenance de toutes les informations documentées requises par la norme
- Mise à disposition du portail BC avec contrôle de versions et traçabilité complète
- Programme d'exercices et de tests + rapport détaillé et CAPA
- Conduite de l'audit interne + support pendant l'audit de certification externe
- Gestion des actions post-audit : traitement des non-conformités et opportunités d'amélioration

Rôle attendu du client

- Désigner les owners métiers et IT ainsi qu'un sponsor au niveau de la direction
- Valider les objectifs (RTO/RPO) et arbitrer les choix de solutions de continuité
- Participer activement aux exercices avec les décisionnaires clés
- Fournir la visibilité sur les changements : IT, fournisseurs, organisation
- Approuver les messages externes et les politiques (validation direction)

CHAPITRE 7 GOUVERNANCE DU SERVICE

Gouvernance du service (RACI) — tout compris mensuel

Un BCMS vivant : mises à jour continues + test annuel + preuves — votre continuité d'activité gérée comme un service managé avec des responsabilités claires.

Le tableau RACI ci-dessous clarifie la répartition des responsabilités entre Luxgap et vos équipes internes. Cette gouvernance transparente garantit que chaque activité du BCMS dispose d'un responsable identifié et d'un approbateur légitime, tout en maintenant l'implication appropriée de vos fonctions IT et métiers.

RACI (extrait)

Activité	Luxgap	Direction	IT	Métiers
Pilotage BCMS (PDCA)	**R**	**A**	C	C
BIA / RTO-RPO	**R**	**A**	C	C
ITDR / DRP (runbooks)	C	I	**R**	C
Comité de crise & communications	**R**	**A**	C	C
Exercice annuel + rapport	**R**	**A**	C	C
Audit interne & revue de direction	**R**	**A**	C	C

R = Responsible (réalise) | **A** = Accountable (approuve) | **C** = Consulted (contribue) | **I** = Informed (informé)

24/7	1+/an	100%	3
Accès portail	Exercice de simulation	Preuves maintenues	Cadres couverts
Disponibilité permanente du BCP	Test complet du dispositif	Evidence pack toujours à jour	ISO 22301, NIS2, DORA