LIVRE BLANC STRATÉGIQUE

SoReady™

La couche de continuité des grands événements

Positionnement complémentaire, architecture modulaire, sécurité, universalité et valeur pour les événements d'ampleur.

THÈSE

SoReady relie exigences, données, dépendances, ressources, risques, preuves et décisions. Il préserve les systèmes spécialistes et comble l'espace entre planification fragmentée et readiness démontrable.

Know more. Decide earlier. Be ready.

Analyse LSE - édition publique - sans divulgation des mécanismes propriétaires

Septembre 2026

Le trou n'est pas un manque d'outils

Les grands événements disposent déjà de solutions performantes. La rupture se situe entre elles : versions divergentes, dépendances invisibles, arbitrages tardifs et preuves dispersées.

TROU 1

Fragmentation

Chaque fonction optimise son périmètre, sans continuité transverse suffisante.

TROU 2

Décision tardive

Les impacts croisés apparaissent lorsque le coût de correction devient élevé.

TROU 3

Preuve diffuse

Une déclaration de readiness reste difficile à expliquer, sourcer et auditer.

RÉPONSE

Continuité gouvernée

SoReady relie les objets utiles sans remplacer leurs systèmes d'autorité.

NIVEAU 2 | COMPRENDRE

Les fonctions d'un grand événement sont généralement bien équipées : finance, planning, accréditation, sport, sécurité, logistique ou documentation. Pourtant, aucune ne porte seule la question décisive : l'ensemble peut-il fonctionner, à la date prévue, avec les moyens confirmés et les preuves requises ? SoReady traite cette discontinuité horizontale. Il rend visibles les dépendances entre domaines, les informations contradictoires et les décisions restées sans propriétaire.

NIVEAU 3 | APPROFONDIR

La valeur ne vient pas d'une nouvelle saisie centrale, mais d'un lien gouverné entre sources d'autorité. Mesurer la réduction des réconciliations manuelles et le délai d'arbitrage.

Complémentaire par construction

SoReady se positionne au-dessus des systèmes transactionnels et spécialistes, au-dessous de la décision exécutive : une couche de gouvernance, de readiness et de corrélation.

SoReady ne prétend pas refaire la finance, le planning, le CAD, le BIM ou l'accréditation. Il rend leurs contributions cohérentes, explicables et actionnables.

NIVEAU 2 | COMPRENDRE

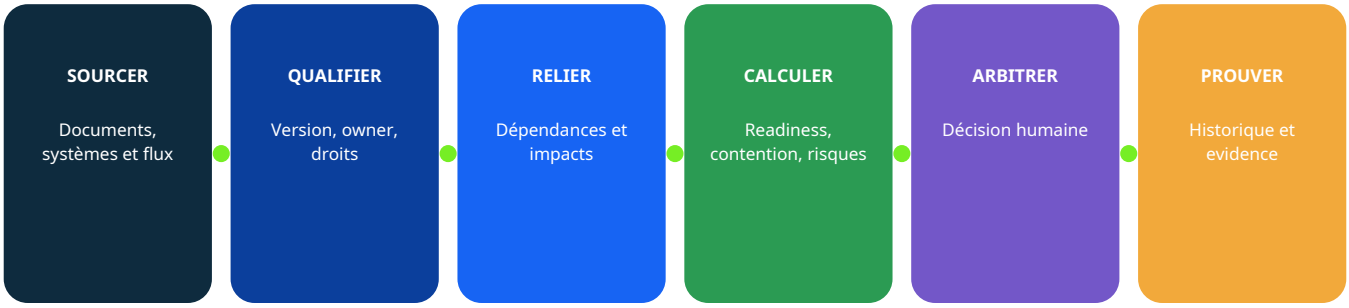
Le positionnement de SoReady repose sur une discipline : ne pas reproduire la profondeur des outils spécialistes. Le système financier demeure autoritaire pour les engagements ; le planning pour les dates ; la GED pour les documents ; les solutions sportives pour leurs objets. SoReady assemble la lecture nécessaire au management : obligations, états, impacts, réserves, preuves et décisions. Cette complémentarité réduit le risque de migration et permet une adoption progressive.

NIVEAU 3 | APPROFONDIR

La carte est conceptuelle, non un classement de produits. L'intégration exige pour chaque donnée un owner, une fréquence, un statut et une règle de conflit.

De la donnée à la décision démontrable

La valeur apparaît quand la chaîne conserve l'autorité de la source, expose les relations et place l'arbitrage au bon niveau.



POINT DE GOUVERNANCE

L'IA peut extraire, expliquer, challenger et rédiger. Les règles calculent ; l'humain valide ; le système trace.

NIVEAU 2 | COMPRENDRE

Une donnée isolée ne produit pas une décision fiable. Elle doit être qualifiée, reliée à un objet et confrontée aux règles applicables. La chaîne SoReady conserve le passage de la source à la preuve : qui a fourni l'information, quelle version était valide, quel calcul a été exécuté et quelle personne a arbitré. Cette continuité permet d'expliquer une décision après coup et de la remettre en cause lorsque son contexte change.

NIVEAU 3 | APPROFONDIR

Séparer systématiquement fait, calcul, proposition IA et décision. Le retour arrière doit restaurer l'état métier et son historique, pas seulement l'affichage.

Une architecture modulaire remise en ordre

Les modules sont organisés en couches : gouvernance, données de référence, planification et ressources, puis exploitation événementielle.

01 - GOUVERNANCE

Sécurité, administration fonctionnelle et technique

Identités, rôles, politiques, audit, configuration, supervision et assistance utilisateur intégrée.

02 - CONNAISSANCE

GED/OCR, référentiels et peuplement automatique

Lecture documentaire, extraction contrôlée, provenance, validation et données de référence.

03 - PRÉPARATION

Planning, contention, risques, budget, BOM et infrastructure

Dépendances, capacités, coûts, moyens, calculs et readiness par objet.

04 - OPÉRATIONS

EOS, EDF, flux externes, reporting et command center

Observation, corrélation événementielle, synthèses assistées et décisions tracées.

NIVEAU 2 | COMPRENDRE

L'ordre des modules traduit un ordre de confiance. La gouvernance et la sécurité définissent d'abord qui peut voir, modifier ou valider. La couche connaissance transforme documents et référentiels en faits sourcés. La préparation relie planning, infrastructure, FoP, ressources, budget, BOM, VIK et risques. Enfin, l'EOS et l'Event Data Fabric soutiennent l'exploitation. Les modules peuvent être activés séparément, mais partagent la même grammaire d'objets et de preuves.

NIVEAU 3 | APPROFONDIR

Éviter les silos de modules : identifiants stables, contrats de données versionnés et journal d'audit commun. Administration fonctionnelle et technique restent distinctes.

Treize capacités, une seule chaîne de confiance

Le découpage distingue modules fonctionnels, services transverses et fondation technologique.

Ordre	Capacité	Rôle dans la chaîne
01	Gouvernance / sécurité	Droits, responsabilités, politiques, preuves
02	GED / OCR	Documents vers faits sourcés et validables
03	Référentiels / flux externes	Autorités, versions, mappings, qualité
04	Infrastructure / moteurs de calcul	Sites, espaces, capacités, scénarios
05	FoP / matériels / consommables	Besoins, configurations, turnover, disponibilité
06	Planning / contention	Dépendances, transitions, collisions, capacités
07	Budget / BOM / VIK / workforce	Coûts, contributions, ressources et arbitrages
08	Risk Assessment / readiness	Exposition, traitement, preuves, gates
09	EOS / EDF	État événementiel et corrélations opérationnelles
10	Reporting assisté par IA	Synthèses sourcées, dossiers, décisions
11	IAs croisées	Extraction, contradiction, simulation, explication
12	Assistance utilisateur	Aide contextuelle intégrée et gouvernée
13	Administration	CRUD métier, exploitation, RBAC/MAC selon criticité

NIVEAU 2 | COMPRENDRE

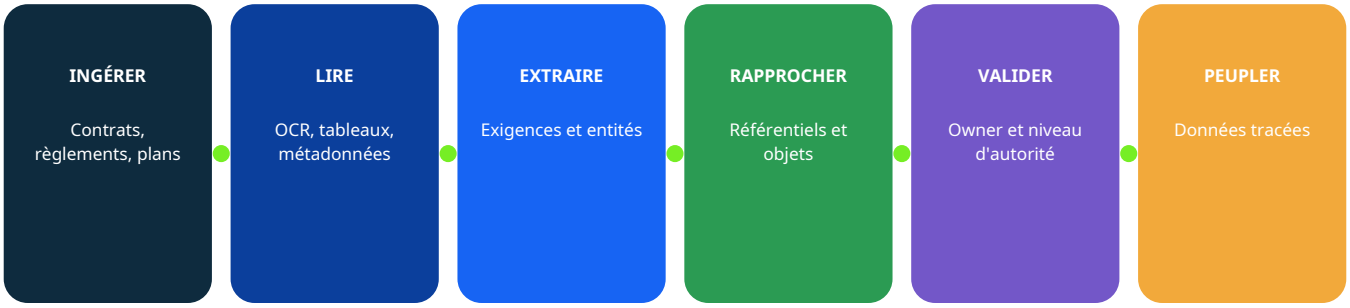
Le découpage ne décrit pas treize applications juxtaposées. Il expose les capacités nécessaires pour aller d'une obligation documentaire à une condition d'ouverture, puis à une situation live. Budget, BOM, VIK et workforce matérialisent les moyens ; planning et contention vérifient leur disponibilité ; le Risk Assessment mesure l'exposition ; EOS/EDF observe les signaux. Reporting et IAs croisées rendent cette information lisible, sans modifier seules les données certifiées.

NIVEAU 3 | APPROFONDIR

Le CRUD métier est soumis aux droits. Pour les informations critiques ou certifiées, appliquer séparation des rôles, double validation et RBAC/MAC lorsque requis.

Du document au contexte exploitable

La GED/OCR ne remplit pas silencieusement le système. Elle propose des faits, conserve la preuve et organise leur validation.



POINT DE GOUVERNANCE

Aucune extraction automatique ne devient une vérité opérationnelle sans provenance, statut et contrôle adaptés à sa criticité.

NIVEAU 2 | COMPRENDRE

L'OCR n'est que la première étape. SoReady doit distinguer texte détecté, fait proposé et information validée. Une exigence extraite d'un règlement est rapprochée d'une discipline, d'un site, d'une date et d'un responsable ; l'extrait d'origine reste consultable. Lorsqu'une version change, le système identifie les objets affectés au lieu d'écraser silencieusement l'ancienne connaissance. Le peuplement automatique devient ainsi un accélérateur contrôlé, non une source d'opacité.

NIVEAU 3 | APPROFONDIR

Conserver document, page, zone, hash, date d'extraction, modèle utilisé et statut de validation. Une valeur sans provenance reste une proposition.

Prévoir les collisions avant l'événement

Le moteur de contention croise calendrier, espaces, ressources, capacités, turnover et dépendances. Budget et BOM donnent une matérialité aux arbitrages.

TEMPS

Planning & transitions

Jalons, séquences, temps de bascule et chemins critiques.

CAPACITÉ

Contention

Conflits de sites, équipes, actifs, transports et fournisseurs.

MOYENS

BOM / FoP

Équipements, consommables, configurations et disponibilité.

ÉCONOMIE

Budget, VIK et workforce

Coûts, contributions en nature, ressources, mutualisations et décision.

NIVEAU 2 | COMPRENDRE

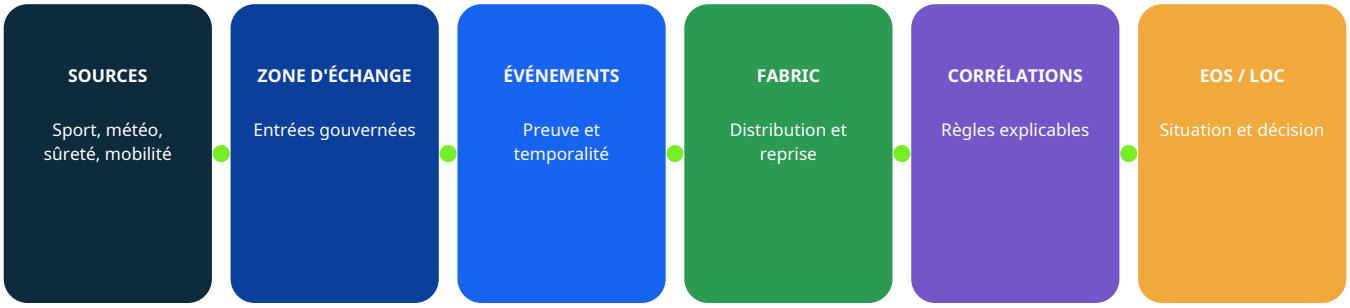
La contention apparaît lorsqu'une même ressource est promise à plusieurs séquences incompatibles : espace, équipe, équipement, transport, énergie ou temps de turnover. Le moteur croise les calendriers avec les capacités réelles et les dépendances. Il ne se limite pas à signaler une collision ; il prépare les options d'arbitrage avec leurs effets sur le budget, les VIK, la workforce et la readiness. Le management peut alors décider avant que le conflit n'atteigne l'exploitation.

NIVEAU 3 | APPROFONDIR

Les règles de calcul doivent être déterministes, versionnées et testables. L'IA peut expliquer les options, jamais inventer une capacité disponible.

Comprendre l'événement pendant qu'il se déroule

L'EOS porte l'état opérationnel ; l'EDF accepte des signaux hétérogènes, les qualifie et permet des corrélations multi-domaines sans effacer l'autorité des sources.



POINT DE GOUVERNANCE

L'EDF est une fabrique événementielle évolutive. Les détails de routage, seuils, modèles et règles propriétaires ne sont pas exposés.

NIVEAU 2 | COMPRENDRE

L'EOS fournit une représentation opérationnelle de l'événement ; l'EDF lui apporte des événements qualifiés issus de domaines hétérogènes. Entre la source et l'état métier, une zone d'échange gouvernée vérifie l'identité, la forme, l'autorité, la sensibilité et la temporalité du signal. Les événements acceptés restent rattachés à leur preuve et peuvent être diffusés, rejoués ou isolés. La corrélation fait alors émerger une situation que chaque source, prise séparément, ne pouvait révéler.

NIVEAU 3 | APPROFONDIR

Architecture observationnelle par défaut. Aucun flux externe n'écrit directement dans le cœur métier ; les systèmes OT et life-safety gardent leur chaîne d'action.

L'Event Data Fabric est un module complet, pas un simple connecteur

Son rôle couvre le cycle de vie du signal : admission, qualification, preuve, diffusion, reprise, corrélation et pilotage opérationnel des flux.

FRONTIÈRE DE CONFIANCE

Admission et isolation par flux

Identité de source, autorité, sensibilité, limites, contrôles de format et arrêt indépendant.

PREUVE ET QUALITÉ

Validation, quarantaine et provenance

Original ou référence probante, horodatage, version, statut et traitement visible des rejets.

CONTINUITÉ DE SERVICE

Distribution durable, déduplication et rejeu

Consommateurs indépendants, reprise après interruption, store-and-forward site et réconciliation.

INTELLIGENCE ÉVÉNEMENTIELLE

Contrat canonique et corrélations explicables

Événements comparables, règles versionnées, impacts contextualisés et alimentation de l'EOS.

NIVEAU 2 | COMPRENDRE

L'EDF industrialise le cycle de vie d'un signal. Il enregistre le contrat du flux et son owner, contrôle l'admission, conserve une preuve ou une référence probante, met les messages non conformes en quarantaine et distribue les événements acceptés vers des consommateurs indépendants. Déduplication, rejeu, reprise après coupure et store-and-forward protègent la continuité. Un contrat canonique permet ensuite des corrélations explicables sans écraser la source autoritative. Le module évolue source par source sans déstabiliser l'EOS.

NIVEAU 3 | APPROFONDIR

Séparer contrôle d'entrée, échange durable et état métier. Chaque flux dispose d'un arrêt indépendant, d'une politique de rétention et d'une procédure de reprise testée.

Dix domaines, une lecture transversale

La base de conception couvre plusieurs dizaines de familles de flux, dix grands domaines opérationnels et des scénarios de corrélation multi-domaines. Ce périmètre est extensible et ne constitue pas une promesse figée.

SIGNAL

Sport + résultats

Programme, statut des sessions, timing et preuves associées.

CONTEXTE

Météo + mobilité

Prévisions, alertes, transport, trafic et arrivées.

SITUATION

Sûreté + foule + médical

Accès, densité, incidents et capacité de réponse.

CONTINUITÉ

OT + IT + logistique

Énergie, réseau, équipements, services et turnover.

NIVEAU 2 | COMPRENDRE

Sport, résultats, météo, mobilité, foule, médical, sûreté, OT, IT, logistique et médias évoluent à des rythmes différents. L'intérêt de l'EDF est de conserver cette diversité tout en donnant une temporalité commune. Le périmètre de démonstration couvre plusieurs dizaines de familles de flux et des scénarios multi-domaines ; il reste extensible. La valeur réside moins dans le nombre de connecteurs que dans la capacité à qualifier la fraîcheur, la confiance et l'impact opérationnel de chaque signal.

NIVEAU 3 | APPROFONDIR

Chaque feed possède un owner, une autorité, une sensibilité, un mode simulé/sandbox/réel, une quarantaine et un kill switch indépendant.

La sécurité est incluse - mais ne se résume pas à une norme événementielle

ISO 20121 traite le management responsable des événements ; elle ne constitue pas une norme de cybersécurité. SoReady s'aligne sur un portefeuille de cadres complémentaires, sans revendiquer de certification.

Référence	Apport	Couverture SoReady
ISO 20121:2024	Management responsable de l'événement	Objectifs, parties prenantes, amélioration
ISO 31000:2018	Principes de management du risque	Risk Assessment, traitements, escalades
ISO 22301:2019	Continuité d'activité	Scénarios, reprise, exercices, preuves
ISO/IEC 27001:2022	Management de la sécurité de l'information	Identités, risques SI, audit, contrôles
ISO/IEC 42001:2023	Management des systèmes d'IA	Rôles IA, risques, suivi, responsabilité
OWASP / NIST AI RMF	Risques applicatifs et IA	Menaces, tests, gouvernance technique
WCAG 2.2 / W3C PROV-O	Accessibilité et provenance	Interfaces utilisables, faits traçables

NIVEAU 2 | COMPRENDRE

La sécurité traverse le produit : identité, droits, confidentialité, intégrité, disponibilité, continuité et audit. ISO 20121 structure le management responsable de l'événement mais ne couvre pas à elle seule la cybersécurité. ISO/IEC 27001, ISO 22301 et les cadres OWASP complètent donc l'approche ; ISO/IEC 42001 traite la gouvernance de l'IA. SoReady peut soutenir les preuves et les contrôles d'un dispositif, sans transformer cet alignement en revendication de certification.

NIVEAU 3 | APPROFONDIR

Distinguer sécurité du produit, sécurité de son exploitation et sécurité globale de l'événement. Chacune possède son propriétaire, ses risques et ses tests.

Trois niveaux d'IA, une même doctrine

Le niveau de déploiement dépend de la sensibilité, de la latence, de la connectivité et des exigences de souveraineté.

NIVEAU 1

IA externe contrôlée

Données autorisées, minimisation, passerelle gouvernée, usages à faible sensibilité.

NIVEAU 2

Architecture hybride

Routage par classe de données ; modèles privés pour les contenus sensibles ; services spécialisés interchangeables.

NIVEAU 3

IA souveraine / on-premise

Moteurs locaux ou isolés, contexte sur site, continuité hors ligne et contrôle d'exploitation renforcé.

NIVEAU 2 | COMPRENDRE

Le choix entre IA externe, hybride ou souveraine dépend des données et du contexte, non d'une préférence technologique abstraite. Les contenus publics ou peu sensibles peuvent utiliser un service contrôlé. Les données contractuelles, financières ou opérationnelles peuvent être routées vers un environnement privé. Les fonctions critiques ou soumises à forte exigence de continuité peuvent fonctionner localement. Une passerelle d'outils de type MCP peut préserver des contrats d'accès communs. Dans les trois cas : contexte minimal, sources visibles, actions bornées et validation humaine.

NIVEAU 3 | APPROFONDIR

La souveraineté inclut modèles, données, journaux, administration, clés, dépendances et capacité de fonctionner en mode dégradé ; MCP ne déplace ni les droits ni l'autorité métier.

Une grammaire stable, des règles configurables

SoReady est universel parce qu'il modélise les invariants d'un grand événement, puis adapte taxonomies, preuves, autorités et workflows.

QUOI

Programme et obligations

Promesses, exigences, livrables, règles et décisions.

OÙ / QUAND

Sites et séquences

Espaces, jalons, transitions, capacités et dépendances.

QUI / AVEC QUOI

Responsabilités et moyens

Owners, workforce, budget, actifs, fournisseurs et BOM.

ET SI

Risque et continuité

Scénarios, signaux, traitements, tests et preuves.

NIVEAU 2 | COMPRENDRE

Tous les événements complexes partagent des invariants : programme, lieux, séquences, responsables, ressources, règles, risques et preuves. SoReady stabilise cette grammaire, puis configure le vocabulaire et les obligations du contexte. Une compétition internationale met l'accent sur les disciplines et FoP ; un sommet sur les délégations et le protocole ; un festival sur les scènes et autorisations. L'universalité vient donc d'un noyau cohérent et d'une contextualisation explicite, pas d'un modèle générique appauvri.

NIVEAU 3 | APPROFONDIR

Versionner taxonomies, règles et niveaux de preuve par événement. Une configuration locale ne doit pas casser le noyau commun ni les migrations.

Ouvert, administrable et gouverné

L'acceptation des flux externes est contrôlée. L'administration fonctionnelle configure le métier ; l'administration technique exploite la plateforme ; la sécurité traverse les deux.

FONCTIONNEL

Taxonomies, règles, responsabilités, gates

Paramétrage par événement, disciplines, sites, fonctions et niveaux de preuve.

TECHNIQUE

Connecteurs, disponibilité, observabilité, sauvegarde

Exploitation, supervision, gestion des versions, continuité et performance.

SÉCURITÉ

Identités, séparation des rôles, audit, intégrité

Contrôles d'accès, journalisation, validation humaine et traitement des incidents.

NIVEAU 2 | COMPRENDRE

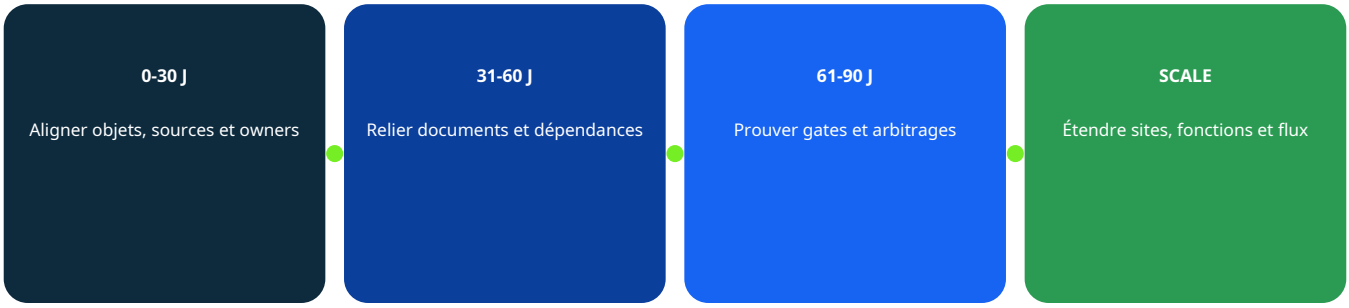
L'ouverture vers l'extérieur n'est fiable que si les frontières sont administrables. L'administration fonctionnelle configure taxonomies, workflows, gates et responsabilités. L'administration technique exploite connecteurs, performances, sauvegardes et observabilité. La sécurité impose les identités, la séparation des rôles et les contrôles d'intégrité. Cette organisation permet d'accepter des flux externes sans leur déléguer l'autorité sur les objets du programme.

NIVEAU 3 | APPROFONDIR

Documenter les changements de configuration comme des changements de production : auteur, motif, validation, date d'effet, test et rollback.

Déployer par chemins critiques

La valeur se démontre sur un périmètre précis, puis s'étend sans imposer un remplacement global des outils existants.



POINT DE GOUVERNANCE

Mesures : couverture sourcée, conflits détectés avant exécution, délai d'arbitrage, gates démontrables et réduction du travail de réconciliation.

NIVEAU 2 | COMPRENDRE

Un déploiement utile commence par une question de management, par exemple la readiness d'un cluster ou le turnover de plusieurs disciplines sur un site. Les trente premiers jours alignent objets, owners et sources ; les suivants relient documents, dépendances et règles ; la dernière étape démontre un gate avec preuves et arbitrages. Ce pilote produit une valeur vérifiable et révèle les écarts de données avant l'extension à l'ensemble des fonctions.

NIVEAU 3 | APPROFONDIR

Définir dès le départ les métriques de succès : couverture sourcée, délai de décision, conflits anticipés, preuves acceptées et charge de réconciliation.

Ce que SoReady affirme - et ce qu'il n'affirme pas

Le produit renforce la maîtrise. Il ne remplace ni les autorités, ni les systèmes certifiés, ni les responsabilités du LOC.

AFFIRME

Continuité et preuve

Relier, contrôler, expliquer, tracer, assister et préparer.

N'AFFIRME PAS

Certification automatique

Aucune norme, conformité réglementaire ou homologation n'est revendiquée sans audit dédié.

PROTÈGE

Secrets de fabrication

Modèles détaillés, calculs, règles, seuils, routage et configurations restent confidentiels.

RESPONSABILISE

Décision humaine

Les actions sensibles restent soumises aux droits, validations et autorités compétentes.

NIVEAU 2 | COMPRENDRE

La crédibilité du produit dépend autant de ses limites que de ses capacités. SoReady peut contrôler la cohérence, tracer la provenance, calculer des états et assister l'analyse. Il ne remplace pas l'autorité d'une fédération, d'un service de sécurité, d'un auditeur ou du LOC. Il ne transforme pas une donnée en certification par simple passage dans la plateforme. Les secrets de fabrication restent protégés tandis que les principes de gouvernance demeurent explicables.

NIVEAU 3 | APPROFONDIR

Toute promesse commerciale doit distinguer capacité disponible, configuration requise, intégration tierce, assurance attendue et responsabilité finale.

Faire de la readiness un actif de gouvernance

SoReady préserve la profondeur des outils existants, ajoute la continuité qui leur manque et donne à chaque décision son contexte, sa preuve et son responsable.

VOIR

Plus tôt

Signaux faibles, trous de couverture et contradictions.

RELIER

Plus largement

Fonctions, sites, disciplines, moyens et événements.

DÉCIDER

Plus clairement

Options, impacts, responsabilités et preuves.

CAPITALISER

Au-delà de l'événement

Historique, retour d'expérience et actifs réutilisables.

NIVEAU 2 | COMPRENDRE

La readiness devient un actif lorsque le board peut la questionner : pourquoi cet objet est-il déclaré prêt, quelle preuve le démontre, quelle réserve subsiste et qui l'a acceptée ? SoReady crée cette capacité d'interrogation et conserve l'historique des changements. Après l'événement, le même corpus facilite le retour d'expérience, la transmission aux équipes futures et la réutilisation des référentiels. La plateforme relie ainsi performance immédiate et héritage organisationnel.

NIVEAU 3 | APPROFONDIR

Évaluer la readiness par conditions et preuves, jamais par un pourcentage isolé. Conserver les réserves acceptées et leur autorité.

Cadres mobilisés et périmètre des affirmations

Les références structurent l'analyse. Elles ne constituent ni une certification de SoReady, ni une validation automatique de la conformité d'un événement.

Référence publique	Domaine	Usage dans le document
ISO 20121:2024	Management responsable des événements	Gouvernance et amélioration
ISO 31000:2018	Management du risque	Traitement et exposition résiduelle
ISO 22301:2019	Continuité d'activité	Scénarios, exercices et reprise
ISO/IEC 27001:2022	Sécurité de l'information	Identités, contrôles et audit
ISO/IEC 42001:2023	Management des systèmes d'IA	Rôles, risques et responsabilité
NIST AI RMF / OWASP	Risques IA et applicatifs	Menaces et assurance
W3C PROV-O / WCAG 2.2	Provenance et accessibilité	Traçabilité et usage inclusif

NIVEAU 2 | COMPRENDRE

Les normes et cadres cités fournissent des angles complémentaires : management d'événement, risque, continuité, sécurité, IA, provenance et accessibilité. Ils permettent de vérifier que l'architecture n'oublie pas une dimension majeure. Le document n'en reproduit pas le contenu normatif et ne prétend pas démontrer une conformité. Une certification éventuelle relève d'un périmètre, d'un système de management et d'un audit formel.

NIVEAU 3 | APPROFONDIR

Références officielles : iso.org, nist.gov, owasp.org et w3.org. Vérifier l'édition applicable au moment du projet.