LIVRE BLANC TECHNOLOGIQUE

SoReady™
Architecture multi-IA gouvernée

MCP, contexte événementiel, agents spécialisés, souveraineté et moteurs locaux / on-premise.

THÈSE

L'IA recherche, extrait, explique et propose. Les règles calculent. L'humain valide. SoReady trace - quel que soit le modèle ou le lieu d'exécution.

Know more. Decide earlier. Be ready.

Analyse LSE - édition publique - sans divulgation des mécanismes propriétaires

Septembre 2026

Plusieurs IA, une seule gouvernance

La performance ne vient pas du nombre de modèles mais de rôles explicites, d'un contexte maîtrisé et d'une séparation stricte entre assistance et autorité.

IA

Recherche et proposition

Extraction, synthèse, contradiction, simulation et aide à l'utilisateur.

RÈGLES

Calcul déterministe

Contention, readiness, corrélations, seuils et contrôles versionnés.

HUMAIN

Validation et arbitrage

Responsabilité, autorisation, publication et action sensible.

SYSTÈME

Traçabilité

Sources, versions, droits, décisions et retour arrière.

NIVEAU 2 | COMPRENDRE

Une architecture multi-IA sépare les aptitudes au lieu de demander à un modèle unique de tout faire. Un agent extrait, un autre recherche, un troisième challenge, tandis que des moteurs déterministes calculent les états. Cette spécialisation améliore la contrôlabilité, mais augmente le besoin de gouvernance. SoReady doit savoir quel modèle a reçu quel contexte, avec quels outils et pour produire quelle proposition. L'humain reste l'autorité de publication et d'action.

NIVEAU 3 | APPROFONDIR

Définir un contrat par rôle : entrées autorisées, sorties attendues, tests, seuil de confiance, outils accessibles et procédure d'escalade.

Un conseil de rôles, pas une IA toute-puissante

Les modèles sont remplaçables et assignés à des tâches bornées. Une IA peut challenger une autre sans créer une autorité autonome.

01

Extraire

OCR, tableaux, exigences, entités.

02

Rechercher

Sources, versions, faits et preuves.

03

Contradicteur

Hypothèses, écarts, incohérences.

04

Simuler

Impacts, options et scénarios.

05

Synthétiser

Briefs, rapports et décisions attendues.

06

Assister

Aide contextuelle intégrée par rôle.

NIVEAU 2 | COMPRENDRE

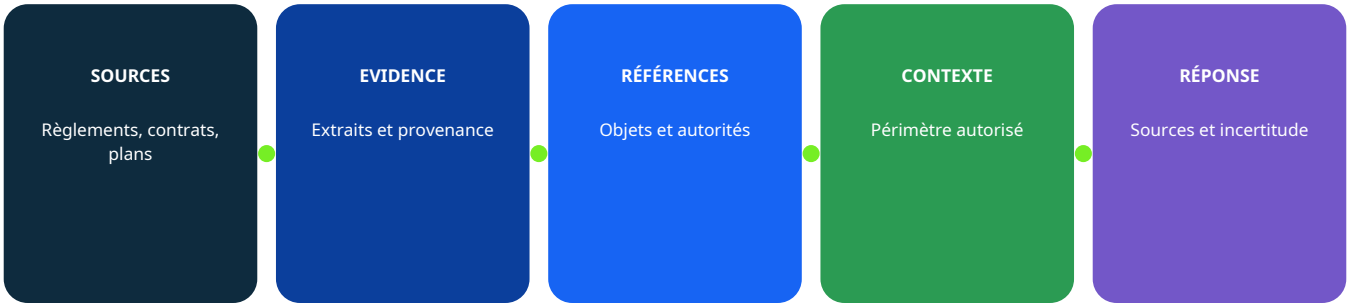
Les rôles IA correspondent à des tâches observables. L'extracteur traite les documents ; le chercheur rassemble les sources ; le contradicteur recherche les incohérences ; le simulateur formule des scénarios ; le synthétiseur prépare un brief. Ces rôles peuvent utiliser des modèles différents et être remplacés. Leur coopération n'est utile que si les désaccords restent visibles et si une réponse ne devient jamais une vérité métier par simple consensus entre modèles.

NIVEAU 3 | APPROFONDIR

Le nombre d'agents n'est pas un indicateur de maturité. Mesurer exactitude, couverture, citations, stabilité, coût, latence et taux d'escalade humaine.

Apprendre l'événement sans boîte noire

Le contexte spécifique est une mémoire sourcée, versionnée et réversible. Le réentraînement opaque n'est pas le mécanisme par défaut.



POINT DE GOUVERNANCE

Le contexte fourni à chaque modèle est minimal, autorisé et adapté à la tâche. Les faits sensibles peuvent rester sur site.

NIVEAU 2 | COMPRENDRE

Le contexte événementiel est construit à partir de documents, référentiels et décisions versionnés. SoReady privilégie une mémoire récupérable et sourcée à un réentraînement opaque. Lorsqu'un règlement change, le système peut identifier la nouvelle source et les objets impactés ; il n'a pas à deviner ce que le modèle a mémorisé. Le contexte transmis à chaque IA reste limité à sa tâche, à ses droits et à la période pertinente.

NIVEAU 3 | APPROFONDIR

Séparer RAW, EVIDENCE et RULES. Exposer aux IA surtout les règles validées et les preuves nécessaires, avec recette de récupération et fraîcheur.

Trois niveaux jusqu'à la souveraineté

Les mêmes contrats de qualité, d'audit et de décision s'appliquent quel que soit le lieu d'exécution.

NIVEAU 1

Services IA externes contrôlés

Passerelle, minimisation, données autorisées et modèles spécialisés.

NIVEAU 2

Routage hybride par sensibilité

Cloud privé, services dédiés et modèles locaux selon la classe de données.

NIVEAU 3

Moteurs souverains / on-premise

Exécution locale ou isolée, continuité hors ligne, administration et contexte maîtrisés.

NIVEAU 2 | COMPRENDRE

Le niveau 1 s'appuie sur des services externes sous contrôle pour des tâches compatibles avec leur politique de données. Le niveau 2 route les demandes selon la sensibilité vers des environnements privés ou locaux. Le niveau 3 conserve modèles, contexte et exécution sur une infrastructure souveraine ou isolée. Cette gradation permet de concilier innovation, coûts, confidentialité et continuité, sans modifier la doctrine de preuve et d'autorité.

NIVEAU 3 | APPROFONDIR

Classifier avant de router. Tester perte de connectivité, indisponibilité fournisseur, changement de modèle et restauration locale avant le games time.

MCP est une couche d'accès gouvernée, pas le métier

MCP expose des ressources, outils et workflows explicitement autorisés. Il ne remplace ni le Business Core, ni les règles, ni les contrôles d'accès.

POINT DE GOUVERNANCE

Pas d'accès direct de l'IA ou de MCP aux bases opérationnelles. Les actions de type COMMIT restent séparées, autorisées et validées.

NIVEAU 2 | COMPRENDRE

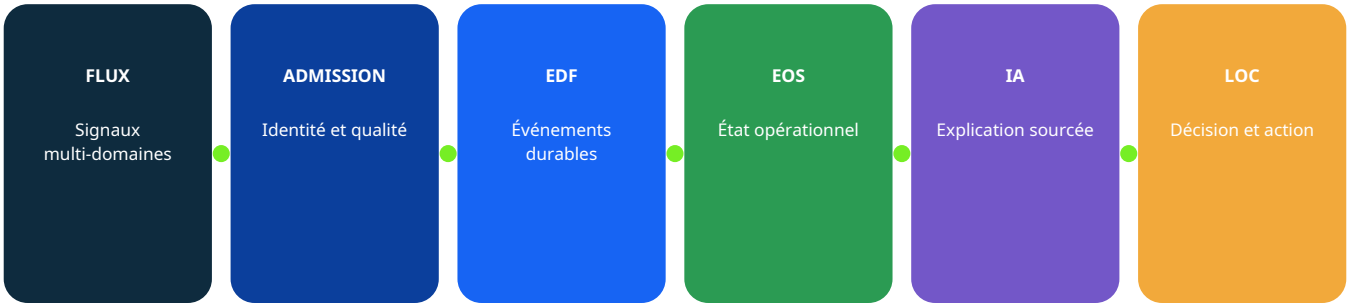
MCP fournit un langage commun pour présenter aux modèles des ressources, des outils et des workflows. Il ne porte ni la règle métier ni l'autorité sur les données. Une passerelle unique contrôle identité, consentement, droits, journalisation et limites d'usage. Les outils READ, ANALYSE et DRAFT peuvent être ouverts progressivement ; COMMIT reste une capacité distincte, soumise aux contrôles du Business Core et à une validation explicite.

NIVEAU 3 | APPROFONDIR

Aucun MCP-vers-PostgreSQL direct. Toutes les opérations passent par des services métier validés, idempotents, auditables et protégés par les mêmes règles que l'API.

L'événement fournit des faits ; l'IA fournit du sens

L'EDF qualifie et corrèle des événements ; l'EOS construit un état opérationnel ; l'IA explique les signaux et prépare les options.



POINT DE GOUVERNANCE

L'IA ne déclenche pas seule une alerte critique et n'actionne pas les systèmes OT ou life-safety.

NIVEAU 2 | COMPRENDRE

L'EDF admet, qualifie et distribue les événements ; les règles déterministes construisent les corrélations ; l'EOS maintient l'état opérationnel. L'IA intervient ensuite pour expliquer la situation, résumer les preuves, formuler des hypothèses et préparer des options. Cette séquence évite qu'une hallucination devienne un signal opérationnel. Elle permet aussi de remplacer un modèle sans modifier les contrats de flux, la logique de détection ou les responsabilités du LOC.

NIVEAU 3 | APPROFONDIR

Conserver les identifiants sources, la version de règle et le contexte IA du brief. L'alerte reste déterministe ; le modèle n'accède pas directement au broker ni au cœur métier.

Concevoir l'EDF comme une frontière de confiance

La fabric sépare l'entrée hostile, l'événement accepté et l'état métier. Cette séparation protège l'EOS et permet de faire évoluer les sources sans fragiliser le noyau.

ENTRÉE CONTRÔLÉE

Autoriser une source, pas seulement un protocole

Identité par flux, droits, limites de charge, formats attendus, coupure indépendante et aucune écriture directe au cœur.

VALIDATION PROBANTE

Conserver, vérifier ou mettre en quarantaine

Preuve brute ou référence, contrôle syntaxique et sémantique, provenance, horodatage et statut explicite.

ÉCHANGE DURABLE

Absorber les pannes et permettre le rejeu

Déduplication, ordre, reprise, consommateurs indépendants, store-and-forward et réconciliation des écarts.

ÉVÉNEMENT CANONIQUE

Corréler sans perdre l'autorité

Contrat commun, source et sensibilité préservées, règles versionnées ; l'IA intervient après la qualification.

NIVEAU 2 | COMPRENDRE

La fabric reçoit des entrées potentiellement hostiles sans les confondre avec des faits acceptés. La frontière d'admission contrôle identité, droits, taille, rythme, format et cohérence sémantique. Une preuve brute ou une référence est conservée lorsque la politique le permet ; les rejets deviennent une quarantaine observable. L'échange durable absorbe les pannes, déduplique et rejoue. Enfin, le contrat canonique transporte source, autorité, sensibilité et temporalité vers l'EOS et les règles de corrélation.

NIVEAU 3 | APPROFONDIR

Aucun flux externe n'écrit directement dans le cœur. Tester message malformé, duplicata, retard, dérive d'horloge, coupure WAN, compromission d'un flux, reprise et reconstruction temporelle.

Croiser les IA pour rendre l'incertitude visible

La confrontation est utile lorsque les rôles, critères et sources sont différents. Un désaccord devient une information gouvernable.

PROPOSITION

Agent principal

Formule une synthèse et cite ses sources.

CHALLENGE

Agent contradicteur

Cherche les omissions, conflits et hypothèses.

CONTRÔLE

Moteur de règles

Vérifie critères, droits et états calculés.

ARBITRAGE

Owner humain

Accepte, corrige, refuse ou demande une preuve.

NIVEAU 2 | COMPRENDRE

Le croisement n'a pas pour but de fabriquer artificiellement un consensus. Un agent principal expose une réponse ; un contradicteur teste les hypothèses et recherche les sources manquantes ; le moteur de règles vérifie les contraintes formelles. L'owner humain dispose alors d'une synthèse qui montre aussi les désaccords. Cette méthode est particulièrement utile lorsque les documents sont incomplets ou lorsque plusieurs interprétations produisent des impacts différents.

NIVEAU 3 | APPROFONDIR

Définir des critères de contradiction indépendants. Un second modèle utilisant le même contexte et les mêmes biais n'est pas une assurance suffisante.

Une surface IA plus large exige une gouvernance plus forte

Sécurité des données, des outils, des modèles et des décisions sont traitées ensemble.

Risque	Contrôle attendu	Autorité
Injection documentaire	Isolation, provenance, filtrage, validation	Data / sécurité
Fuite de données	Minimisation, classification, routage	DPO / RSSI
Hallucination	Sources, incertitude, règles, challenge	Owner métier
Action non autorisée	Séparation READ / DRAFT / COMMIT	Administration
Dérive modèle	Évaluation, version, rollback	AI governance
Indisponibilité externe	Fallback hybride / local	Exploitation

NIVEAU 2 | COMPRENDRE

L'IA élargit les risques classiques : injection par document, exfiltration via un outil, action non autorisée, dépendance à un fournisseur ou dérive d'un modèle. La sécurité doit couvrir la chaîne complète, du contenu ingéré à l'action proposée. Provenance, filtrage, minimisation, séparation READ/DRAFT/COMMIT et surveillance des anomalies se complètent. L'owner métier reste responsable du sens ; le RSSI et l'exploitation contrôlent la plateforme.

NIVEAU 3 | APPROFONDIR

Tester les attaques sur documents, prompts, outils et API. Journaliser sans exposer de données sensibles ; prévoir révocation, kill switch et procédure d'incident.

Le local protège aussi la continuité

Les réseaux OT, sécurité et life-safety restent isolés. Une passerelle locale observationnelle peut assurer store-and-forward et reprise contrôlée.

ZONE SITE

Systèmes OT et sûreté

Autorités locales, segmentation, aucune action implicite depuis l'IA.

PASSERELLE LOCALE

Lecture gouvernée et buffer

Filtrage, temporalité, mode dégradé et synchronisation contrôlée.

NOYAU SOREADY

EOS / EDF / contexte / IA locale

État opérationnel, corrélation, assistance et audit.

SERVICES EXTERNES

Optionnels selon politique

Uniquement les données et tâches explicitement autorisées.

NIVEAU 2 | COMPRENDRE

Le déploiement local ne sert pas uniquement la confidentialité. Il permet de continuer à exploiter un contexte critique lorsque la connectivité externe est dégradée. Les systèmes OT et de sûreté restent dans leurs zones ; une passerelle observationnelle filtre et temporise les données utiles. Le noyau local peut maintenir EOS, EDF et assistance IA dans un périmètre contrôlé, puis synchroniser lorsque les conditions le permettent.

NIVEAU 3 | APPROFONDIR

Le store-and-forward doit préserver ordre, horodatage, déduplication et provenance. L'actionnement OT utilise une voie séparée et gouvernée.

L'IA traverse les modules sans les confondre

Chaque capacité IA s'ancre dans un objet métier, une source et une décision attendue.

Module	Apport IA	Garde-fou
GED / OCR	Extraire et rapprocher	Validation et provenance
Référentiels / flux externes	Qualifier sources et mappings	Autorité et réconciliation
Planning / contention	Expliquer collisions et options	Calcul déterministe
Infrastructure / FoP	Lire capacités et configurations	Moteurs métier
Risk Assessment	Synthétiser exposition et traitements	Owner du risque
Budget / BOM / VIK	Détecter écarts et scénarios	Source financière autoritative
EOS / EDF	Expliquer corrélations	Règles et seuils gouvernés
Reporting	Rédiger rapports et briefs	Citations et approbation
Assistance utilisateur	Aide contextuelle par rôle	Droits et périmètre
Administration / sécurité	Assister contrôle et diagnostic	Séparation des rôles

NIVEAU 2 | COMPRENDRE

Chaque module conserve sa logique métier. L'IA peut lire un règlement, qualifier un flux externe, expliquer une collision de planning, détecter un écart de BOM ou rédiger un rapport, mais elle n'effectue pas les calculs à la place des moteurs concernés. Le contexte commun relie budget, VIK, workforce, infrastructure, FoP, risques et signaux live. Assistance utilisateur, administration et sécurité restent soumises aux droits. La valeur vient de cette transversalité contrôlée, non d'une fusion des responsabilités.

NIVEAU 3 | APPROFONDIR

Pour chaque usage, documenter source autoritative, calcul déterministe, rôle IA, validation attendue, données sensibles, preuve conservée et séparation des rôles.

Une architecture alignée, sans sur-promesse

Les cadres structurent le système de management et les contrôles. Ils ne valent ni certification produit ni conformité automatique.

Cadre	Question couverte	Application
ISO/IEC 42001:2023	Comment gouverner l'IA ?	Rôles, risques, suivi, amélioration
NIST AI RMF 1.0	Comment cartographier et traiter les risques ?	Govern, Map, Measure, Manage
ISO/IEC 27001:2022	Comment gouverner la sécurité SI ?	Risques, contrôles, audit
OWASP GenAI / API	Comment tester les menaces applicatives ?	Injection, accès, données, outils
MCP 2026-07-28	Comment interopérer de façon gouvernée ?	Autorisation, outils, ressources
W3C PROV-O	Comment conserver la provenance ?	Sources, transformations, responsabilité

NIVEAU 2 | COMPRENDRE

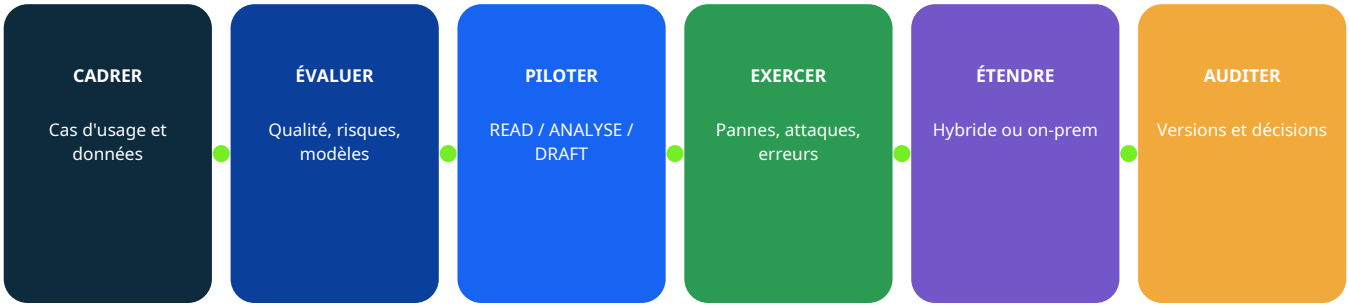
ISO/IEC 42001 structure la gouvernance des systèmes d'IA ; le NIST AI RMF offre une grille de risque ; ISO/IEC 27001 traite le management de la sécurité ; OWASP cible les menaces applicatives. MCP et W3C PROV-O complètent l'interopérabilité et la provenance. SoReady utilise ces cadres pour concevoir et challenger ses contrôles. L'alignement ne vaut ni certification, ni garantie qu'un usage particulier est conforme sans analyse de contexte.

NIVEAU 3 | APPROFONDIR

Maintenir un registre de contrôles reliant exigence, risque, mesure, test, résultat, owner et exception. Réviser les références à chaque version majeure.

Passer du pilote à l'exploitation souveraine

La trajectoire est progressive : périmètre, mesures de qualité, droits, exercices, puis extension.



POINT DE GOUVERNANCE

Un passage au COMMIT ou à l'actionnement nécessite une décision d'architecture et de gouvernance distincte.

NIVEAU 2 | COMPRENDRE

Le pilote commence par des usages sans action : recherche, analyse et rédaction. Les résultats sont mesurés sur un corpus représentatif, puis confrontés aux erreurs, pannes et attaques. L'extension vers l'hybride ou le local intervient lorsque les contrats de qualité et d'exploitation sont établis. Une capacité COMMIT n'est ouverte qu'après une décision distincte, des tests d'idempotence, des droits adaptés et une validation humaine vérifiable.

NIVEAU 3 | APPROFONDIR

Le passage en production exige versionnement, évaluation récurrente, rollback, observabilité, gestion des secrets et procédure de retrait d'un modèle.

Trois lignes de contrôle

La qualité IA n'est pas un score unique. Elle combine performance, sécurité, robustesse, explicabilité et valeur métier.

LIGNE 1

Équipes produit et métier

Tests fonctionnels, sources, droits, qualité des réponses.

LIGNE 2

Sécurité et gouvernance IA

Menaces, modèles, données, accès, incidents et exceptions.

LIGNE 3

Audit et direction

Efficacité des contrôles, responsabilité et exposition résiduelle.

PREUVE

Journal de décision

Modèle, contexte, sources, règles, validation et version.

NIVEAU 2 | COMPRENDRE

La première ligne appartient aux équipes produit et métier, qui vérifient sources, exactitude et utilité. La deuxième regroupe sécurité, data et gouvernance IA ; elle contrôle les risques, modèles, accès et incidents. La troisième donne à l'audit et à la direction une vue indépendante sur l'efficacité du dispositif. Le journal de décision relie ces trois niveaux et permet de comprendre les exceptions acceptées.

NIVEAU 3 | APPROFONDIR

Éviter l'auto-certification par l'équipe qui construit. Définir périodicité, seuils de revalidation et propriétaires des plans correctifs.

Ouverture technologique, responsabilité stable

SoReady peut changer de modèles et de modes de déploiement sans changer la doctrine de décision.

MODÈLE

Interchangeable

Un fournisseur n'est pas l'architecture.

CONTEXTE

Maîtrisé

Version, autorité, sensibilité et finalité.

ACTION

Gouvernée

Droits, validation et séparation des rôles.

PREUVE

Persistante

Sources, calculs, propositions et décisions.

NIVEAU 2 | COMPRENDRE

Un modèle, un fournisseur ou un protocole peut évoluer sans déplacer la responsabilité. SoReady conserve des contrats de rôle et des services métier stables ; le contexte reste classifié et la preuve persiste. Cette neutralité réduit le verrouillage technologique et permet de choisir localement le meilleur moteur. Elle impose toutefois une discipline d'évaluation : deux modèles interchangeables ne sont jamais supposés équivalents sans test.

NIVEAU 3 | APPROFONDIR

Versionner modèle, paramètres, contexte, outils et politique de routage. Une substitution déclenche une campagne de non-régression.

Une IA utile parce qu'elle connaît ses limites

La multi-IA SoReady augmente la capacité d'analyse sans diluer l'autorité. MCP ouvre l'accès ; le Business Core gouverne ; l'EOS/EDF observe et corrèle ; l'humain décide.

EXPLIQUER

La situation

Avec sources, temporalité et incertitude.

CHALLENGER

Les hypothèses

Avec plusieurs rôles et critères.

PROPOSER

Des options

Avec impacts, risques et preuves.

RESTER À SA PLACE

Sans action autonome

Sur les décisions sensibles et opérationnelles.

NIVEAU 2 | COMPRENDRE

L'architecture atteint son objectif lorsque l'IA améliore la compréhension sans masquer l'incertitude. Elle explique les faits issus de l'EOS/EDF, challenge des hypothèses et prépare des options, mais laisse les règles calculer et les personnes habilitées décider. Cette limitation n'est pas une faiblesse : elle rend l'IA acceptable dans un environnement où les conséquences opérationnelles, financières ou de sécurité sont réelles.

NIVEAU 3 | APPROFONDIR

L'interface doit montrer sources, date, niveau de confiance, hypothèses et action attendue. Une réponse non sourcée ne doit pas sembler certifiée.

Les cadres qui bornent l'architecture

Ces cadres sont utilisés comme grilles de conception et d'assurance. Leur citation ne signifie pas que le produit ou son exploitant sont certifiés.

Référence publique	Question structurante	Application SoReady
ISO/IEC 42001:2023	Gouverner un système d'IA	Rôles, risques, suivi
NIST AI RMF 1.0	Traiter les risques IA	Govern, Map, Measure, Manage
ISO/IEC 27001:2022	Protéger l'information	Classification, accès, audit
OWASP GenAI / API	Tester la surface applicative	Injection, outils, secrets
MCP 2026-07-28	Exposer ressources et outils	Passerelle, consentement, droits
W3C PROV-O	Conserver l'origine d'un fait	Sources et transformations

NIVEAU 2 | COMPRENDRE

Les références réunissent management de l'IA, risque, sécurité, menaces applicatives, interopérabilité et provenance. Elles forment une grille de lecture cohérente pour auditer la conception. Aucune ne remplace l'analyse métier de l'événement ni les obligations juridiques applicables. Les contrôles doivent être traduits en exigences testables dans l'architecture et l'exploitation.

NIVEAU 3 | APPROFONDIR

Utiliser les éditions officielles et tenir un registre de conformité séparant applicable, implémenté, testé, accepté et hors périmètre.