

SECTEUR · SANTÉ ET SERVICES SOCIAUX DU QUÉBEC
CONFORMITÉ GIA · CISSS ET CIUSSS

RAC/M IDENTITY ET COREVIEW UNE COMBINAISON REQUISE POUR LA CONFORMITÉ GIA

Dans le cadre de la transformation numérique du RSSS et du déploiement provincial du Dossier Santé Québec (DSQ), comment compléter le déploiement gouvernemental de CoreView pour répondre aux obligations légales, réglementaires et opérationnelles en matière de gestion des identités numériques et des accès.



PRÉPARÉ PAR
OKIOK Data Itée

VERSION
1.0

DATE
Mai 2026



LA CYBERSÉCURITÉ SIMPLIFIÉE

SOMMAIRE EXÉCUTIF

POURQUOI COREVIEW SEUL NE SUFFIT PAS, ET CE QUI EST REQUIS

Le gouvernement du Québec déploie progressivement CoreView dans le réseau de la santé et des services sociaux (RSSS) pour rehausser la gouvernance de Microsoft 365. C'est une avancée importante, mais strictement limitée à l'écosystème Microsoft, un sous-ensemble du périmètre que la loi impose aux CISSS et CIUSSS.

Les obligations des CISSS et CIUSSS, notamment la *Loi 5* (renseignements de santé), la *Loi 25*, les directives du MCN (14.1, 14.2, 14.3), la *LGRI*, le *cadre normatif MSSS* (BCH/TGV, RPSO, GMVI) et la *Loi sur l'accès*, exigent une gestion de bout en bout du cycle de vie des identités sur l'ensemble des actifs du CISSS ou CIUSSS, bien au-delà de Microsoft 365.

Cela inclut les systèmes RH (SIRH paie, souvent Logibec, Virtuo, Espresso), le registre des intervenants, les applications cliniques (dossier patient, labo, imagerie, pharmacie), les annuaires LDAP et SQL, et les ITSM (Octopus, GLPI, C2 Atom).

À titre illustratif, l'AO 2023-1771 du CCSMTL (volet GIA, hors PAM) comporte 211 exigences dont 67 OBLIGATOIRES au sens éliminatoire. Une analyse démontre que CoreView seul ne couvrirait qu'environ 35–40 % de l'ensemble des critères, les 67 exigences obligatoires touchent un périmètre IGA multi-systèmes que CoreView ne couvre pas par construction.

Ce livre blanc démontre que RAC/M Identity n'est pas une alternative à CoreView : il en est le complément requis pour qu'un CISSS ou CIUSSS puisse satisfaire ses obligations légales, répondre aux devis GIA du RSSS, et maximiser le retour sur l'investissement déjà engagé dans CoreView.

211

Exigences hors PAM dans la grille type AO 2023-1771 (CCSMTL), dont 67 OBLIGATOIRES éliminatoires.

~65 %

Part estimée des critères hors champ d'application de CoreView seul.

10 M\$

Sanction administrative maximale prévue par la Loi 25 (ou 2 % du CA mondial).

PÉRIMÈTRE

Ce livre blanc traite exclusivement du volet gouvernance des identités numériques (GIA). Le volet gestion des comptes privilégiés (PAM) figurant dans certains appels d'offres combinés GIA+PAM (dont l'AO 2023-1771) est volontairement exclu ; il relève de solutions et d'argumentaires distincts.

SOMMAIRE DES SECTIONS

TABLE DES MATIÈRES

01	Le contexte de transformation numérique du RSSS	p. 04
	Stratégie gouvernementale, place de Microsoft 365, déploiement de CoreView dans le RSSS	
02	Les exigences réelles de GIA dans un CISSS ou CIUSSS	p. 05
	Cas illustratif AO 2023-1771 (CCSMTL), caractéristiques structurelles communes	
03	Le cadre légal et réglementaire applicable	p. 07
	Loi 5 · Loi 25 · MCN 14.x · LGGRI · Cadre MSSS (BCH/TGV, RPSO)	
04	CoreView : forces et limites structurelles	p. 09
	Ce qu'il fait remarquablement bien, et l'écart critique pour un CISSS/CIUSSS	
05	RAC/M Identity : la plateforme IGA qui complète CoreView	p. 10
	Couverture fonctionnelle, adéquation au secteur de la santé	
06	Architecture de référence — RAC/M Identity + CoreView pour un CISSS/CIUSSS	p. 12
	Diagramme de flux d'identités et répartition des responsabilités	
07	Bénéfices, mise en œuvre et conclusion	p. 13
	Cinq jalons d'implantation, bénéfices clés, conclusion, annexe réglementaire	
A	Annexe – Références réglementaires et techniques	p. 14
	Cadre légal, AO de référence, documentation produits	

SECTION 01

01 LE CONTEXTE DE TRANSFORMATION NUMÉRIQUE DU RSSS

1.1, Une trajectoire stratégique et des enjeux de souveraineté sanitaire

La transformation numérique du RSSS s'inscrit dans la *Stratégie de transformation numérique* de l'État québécois, la création du ministère de la Cybersécurité et du Numérique (MCN) et les priorités du ministère de la Santé et des Services sociaux (MSSS) en matière d'interopérabilité clinique, de sécurité de l'information et de modernisation des infrastructures. Les CISSS et CIUSSS doivent simultanément :

- Offrir des services sécuritaires et efficaces aux usagers (soins, services sociaux, prévention, enseignement universitaire intégré aux CIUSSS) ;
- Réduire les risques cyber dans un secteur fortement ciblé (rançongiciel, intrusion, compromission de comptes à privilèges) ;
- Assurer la confidentialité des renseignements de santé et de services sociaux, parmi les données les plus sensibles traitées par l'État.

À cela s'ajoute le déploiement provincial du Dossier Santé Québec (DSQ), l'un des projets les plus structurants de la transformation numérique du réseau. En centralisant l'accès aux renseignements de santé des usagers pour tous les intervenants autorisés à l'échelle du Québec, le DSQ impose une gouvernance des identités d'une rigueur accrue : chaque CISSS et CIUSSS doit déterminer précisément qui a le droit d'accéder au DSQ, à quel niveau de privilège, et s'assurer que ces habilitations évoluent en temps réel avec les rôles et les mouvements du personnel. CoreView contribue à la sécurisation de l'environnement Microsoft qui supporte en partie ce déploiement, mais c'est RAC/M Identity qui permet à l'établissement de définir, automatiser et certifier les habilitations DSQ à l'échelle organisationnelle.

1.2, La place centrale de Microsoft 365 dans les établissements

L'environnement technologique des CISSS et CIUSSS repose largement sur Microsoft 365 : Active Directory et Entra ID (souvent hybrides), Teams pour la collaboration clinique et administrative, SharePoint et OneDrive, Exchange Online, Power BI pour les indicateurs, le tout dans un contexte de fédération d'identités, d'invités partenaires et de multiples sites physiques (hôpitaux, CHSLD, CLSC, centres administratifs).

Ce socle justifie une couche de gouvernance M365 puissante : c'est le rôle naturel de CoreView.

1.3, Le déploiement de CoreView dans le RSSS

À l'instar d'autres secteurs publics, le gouvernement du Québec oriente le déploiement de CoreView pour renforcer la délégation contrôlée, la gouvernance Teams / SharePoint / OneDrive, l'optimisation des licences, la surveillance des applications Entra et les revues d'accès sur le périmètre Microsoft 365. CoreView améliore substantiellement la posture opérationnelle sur M365.

À RETENIR

CoreView est un excellent produit dans son champ d'application, la gouvernance et l'administration de Microsoft 365 et Entra ID. Mais ce champ est strictement limité à l'écosystème Microsoft, alors que les obligations légales et réglementaires des CISSS et CIUSSS imposent une gestion de bout en bout sur l'ensemble du parc applicatif et organisationnel.

SECTION 02

02 LES EXIGENCES RÉELLES DE GIA DANS UN CISSS OU CIUSSS

2.1, Cas illustratif : l'appel d'offres CCSMTL 2023-1771 (volet GIA)

Le Centre intégré universitaire de santé et de services sociaux du Centre-Sud-de-l'Île-de-Montréal (CCSMTL) a publié le devis technique AO 2023-1771 pour une solution combinant PAM et GIA. En isolant le volet GIA et les exigences transverses non-PAM, on dénombre 211 exigences, dont 67 OBLIGATOIRES au sens éliminatoire.

Le devis technique impose notamment une solution GIA SaaS répondant à une cote DIC 3-4-4, l'identification de systèmes sources (SIRH SQL, registre des intervenants CSV), la définition d'au moins six (6) personnat, l'intégration du cycle de vie vers minimum six (6) applications cliniques, la billetterie Octopus, la conformité MCN et MSSS, et l'export des journaux vers Microsoft Sentinel ou Splunk.

Ces attentes sont représentatives des projets GIA à grande échelle dans le RSSS : tout CISSS ou CIUSSS qui modernise son IGA sera confronté à une combinaison analogue de sources d'autorité multiples, d'applications cliniques critiques et de preuves réglementaires.

2.2, Caractéristiques structurelles des CISSS et CIUSSS

- Pluralité des sources d'autorité : SIRH/paie (Logibec, Virtuo, Espresso ou équivalent), registre des intervenants, systèmes de planification et de présence, dossiers RH spécifiques aux professions (infirmières, médecins, préposés), ITSM (Octopus, GLPI, C2 Atom) ;
- Applications cliniques et métier : dossiers patients, laboratoire, imagerie, pharmacie, applications universitaires pour les CIUSSS, en complément de Microsoft 365 ;
- Populations hétérogènes : employés syndiqués, cadres, médecins, résidents, stagiaires, partenaires communautaires, consultants, utilisateurs externes ;
- Multiples lieux d'exercice : un même collaborateur peut œuvrer dans plusieurs installations ou programmes ;
- Comptes fonctionnels et techniques : intérimaires, postes cliniques partagés, kiosques, comptes de service ;
- Contraintes légales renforcées sur les renseignements de santé (Loi 5) et les renseignements personnels (Loi 25).

SECTION 02, SUITE

2.3, Synthèse des blocs d'exigences types (grille AO 2023-1771, hors PAM)

Ces exigences dépassent le périmètre fonctionnel d'un outil limité à Microsoft 365, aussi performant soit-il sur ce périmètre.

BLOC	ILLUSTRATION DES ATTENTES
A – Cycle de vie et intégration	Provisionnement/dépro. automatisés ; libre-service et workflows ; RBAC/ABAC ; revues d'accès planifiées ; API REST ; connecteurs Entra ID, AD, LDAP, SQL, SaaS ; synchronisation RH.
B – Services et hébergement	SaaS ; données au Canada (idéalement Québec) ; propriété des données ; SLA ; sauvegardes ; environnements non-prod ; documentation API.
C – Sécurité et conformité	Architecture de sécurité ; journalisation détaillée et export SIEM ; chiffrement ; PCA/PRI ; gestion des vulnérabilités ; MFA, OIDC, SAML, OAuth2 ; RBAC administratif de la console ; interdiction d'usage secondaire ; cadre MSSS/MCN.
E – Entreprise	Plans de projet ; références ; guides français ; disponibilité 24/7 ; engagement sur niveaux de service du devis.

COUVERTURE ESTIMÉE

PERSPECTIVE	COREVIEW SEUL	RAC/M IDENTITY
Ensemble des 211 exigences hors PAM	~35–40 %	Conforme
Bloc A (fonctions IGA)	~20–25 %	Conforme
Exigences OBLIGATOIRES (67)	Majorité non couverte → rejet	Conforme

CONSÉQUENCE

CoreView déployé seul ne pourrait pas constituer une réponse recevable à titre de solution GIA pour un appel d'offres tel que l'AO 2023-1771. Les 67 exigences obligatoires touchent en majorité un périmètre IGA multi-systèmes que CoreView, par conception, ne couvre pas.

SECTION 03

03 LE CADRE LÉGAL ET RÉGLEMENTAIRE APPLICABLE AUX CISSS ET CIUSSS

La GIA n'est pas qu'une bonne pratique opérationnelle : pour un CISSS ou CIUSSS, elle est une obligation légale multi-niveaux.

3.1, Loi 5 : renseignements de santé et de services sociaux

La *Loi concernant les renseignements de santé et des services sociaux* (Loi 5, chapitre R-22.1) encadre la collecte, la conservation, l'accès et la communication des renseignements personnels dans le dossier de l'utilisateur. Elle impose notamment le respect du principe du cercle de soins, des finalités légitimes, du minimum nécessaire et des droits des personnes.

Implications pour la GIA : le CISSS ou CIUSSS doit pouvoir démontrer qui accède à quels systèmes et dossiers, sur quelle base (rôle, mandat, lien de soins), avec traçabilité et contrôles périodiques. Une plateforme qui ne couvre que M365 ne répond pas à cette démonstration pour les dossiers cliniques et les applications métier hors nuage Microsoft.

Le déploiement du DSQ renforce cette exigence : les intervenants des CISSS et CIUSSS qui accèdent au dossier de l'utilisateur via le DSQ doivent le faire dans le cadre strict du cercle de soins défini par la Loi 5. RAC/M Identity fournit le référentiel d'autorité qui permet à l'établissement de s'assurer que chaque intervenant dispose du bon niveau d'accès au DSQ selon son rôle, son programme et son lieu d'exercice, et que cet accès est retiré sans délai lors d'un départ ou d'un changement de poste.

3.2, Loi 25 : protection des renseignements personnels

OBLIGATION LOI 25	IMPLICATION GIA POUR UN CISSS/CIUSSS
Responsable de la protection des renseignements personnels	Doit démontrer qui accède à quels RP, sur tous les systèmes où résident des données nominatives.
EFVP pour tout projet impliquant des RP	Exige la connaissance précise du modèle d'accès et de sa gouvernance.
Registre des incidents et notification à la CAI	Exige une journalisation complète des accès et la détection des anomalies.
Moindre privilège, limitation de la finalité, durée limitée	Règles d'attribution et de retrait automatiques ; campagnes de certification périodiques.
Droits d'accès, rectification, portabilité (usagers, employés)	Traçabilité historique des accès et des modifications.
Sanctions jusqu'à 10 M\$ ou 2 % du CA mondial	Risque financier direct et responsabilité personnelle des dirigeants.

Les renseignements de santé comptent parmi les données les plus sensibles traitées par l'État québécois. CoreView ne peut pas démontrer qui accède à quels renseignements dans les systèmes cliniques hors Microsoft, or c'est précisément là que résident la majorité des données de soins.

SECTION 03, SUITE

3.3, Directives du MCN : exigences 14.1, 14.2 et 14.3

MESURE	DESCRIPTION	COUVERTURE EXIGÉE POUR UN CISSS/CIUSSS
14.1	Processus d'ajout, révision et retrait des accès pour la gestion du mouvement du personnel.	Cycle de vie complet (joiner-mover-leaver) pour tous les actifs, applications cliniques, annuaires AD/LDAP, ITSM.
14.2	Processus dédié et révisé pour les comptes à privilèges élevés/administrateur.	Domain admins AD, comptes pilotes d'applications cliniques critiques, DBA, souvent au-delà du seul volet Microsoft 365.
14.3	Outil de journalisation des accès et des identités implanté.	Journalisation centrale multi-plateformes, vérifiable par le CGCD et le CO-CD.

3.4, LGGRI et gouvernance informationnelle

La LGGRI (RLRQ chapitre G-1.03) impose plan directeur, inventaire des actifs informationnels, reddition de comptes et bilans de sécurité auprès du MCN. La GIA est un levier central pour les preuves de conformité attendues par les instances ministérielles.

3.5, Cadre MSSS : BCH, TGV, RPSO et gestion des incidents

Les appels d'offres récents du RSSS exigent fréquemment la certification BCH et la Trousse globale de vérification (TGV), la conformité aux Règles particulières sur la sécurité organisationnelle (RPSO) et aux processus GMVI. Une solution GIA doit s'intégrer à cette exigence probatoire : architecture documentée, journaux exploitables, alignement sur les flux Sentinel/Splunk.

3.6. Synthèse : pourquoi la GIA est légalement obligatoire pour un CISSS et un CIUSSS

QUESTION	RÉPONSE
Un CISSS ou CIUSSS peut-il se passer d'une plateforme IGA d'entreprise ?	Non. Sans GIA, il ne peut démontrer la conformité à la Loi 5, la Loi 25, au MCN et à la LGGRI sur l'ensemble des actifs critiques.
CoreView seul suffit-il ?	Non pour le périmètre multi-systèmes, RH, registre des intervenants, applications cliniques et preuves hors M365.
Que risque l'organisme ?	Sanctions Loi 25, non-conformité aux audits, incidents réputationnels et risques cliniques liés aux accès inappropriés.

CONCLUSION INTERMÉDIAIRE

Les CISSS et CIUSSS doivent pouvoir prouver leur conformité, pas seulement l'affirmer. Une plateforme GIA d'entreprise couvrant l'ensemble du parc applicatif est, à toutes fins pratiques, indispensable pour produire cette démonstration.

SECTION 04

04 COREVIEW : SES FORCES ET SES LIMITES STRUCTURELLES

4.1, Ce que CoreView fait remarquablement bien

CAPACITÉ	DESCRIPTION
Délégation granulaire M365	Virtual Tenants, réduction des escalades vers le centre de services.
Gouvernance Teams / SharePoint / OneDrive	Politiques, external sharing, sites et équipes à grande échelle.
Optimisation des licences	Récupération et réaffectation des sièges M365.
Applications Entra	Visibilité sur les permissions, secrets, propriétaires.
Audit unifié M365	Investigation et corrélation sur le périmètre Microsoft.
Revue d'accès M365	Campagnes sur groupes, Teams, SharePoint, BAL, invités.

4.2, Limites structurelles pour un CISSS / CIUSSS

EXIGENCE TYPE (EX. AO 2023-1771, GRILLE HORS PAM)	LIMITATION
Référentiel multi-sources (RH SQL, registre CSV, LDAP, SQL métier) avec corrélation et historique	Axé M365/Entra ; pas un référentiel IGA complet multi-actifs.
Provisionnement bidirectionnel vers six applications cliniques + Octopus selon processus du RSSS	Hors périmètre natif ; nécessite une IGA et des connecteurs métier.
RBAC/ABAC sur les rôles métiers hospitaliers et personnalités complexes	RBAC CoreView = opérateurs de la plateforme M365, pas modèle organisationnel du CIUSSS.
Certifications et revues sur l'ensemble des actifs TI du RSSS	Limité aux ressources Microsoft 365.
API REST à inventaire de fonctions au sens IGA	Pas équivalent à une API IGA complète pour le cycle de vie entreprise.
Preuve Loi 5 sur les accès dossier patient dans les SI métier	Ne couvre pas ces systèmes.

CONCLUSION

CoreView est nécessaire mais non suffisant. Il doit être complété par une plateforme IGA, telle que RAC/M Identity.

SECTION 05

05 RAC/M IDENTITY : LA PLATEFORME IGA QUI COMPLÈTE COREVIEW

5.1, Présentation

RAC/M Identity est la plateforme IGA développée par OKIOK Data Itée, entreprise québécoise. Elle fournit un référentiel central des identités et des accès, des connecteurs vers les systèmes sources et cibles, des campagnes de certification, du libre-service, des workflows d'approbation et une journalisation orientée conformité.

ATTRIBUT	VALEUR
Modèle	SaaS (Microsoft Azure dédié client), services gérés ou on-premise.
Hébergement	Centres de données au Canada, conformes Loi 25.
Langues	Français intégral (interface, documentation, support).
Certifications	SOC 2 Type II, ISO 9001, ISO 27001/27002, tests d'intrusion périodiques.
Éditions	Gouvernance et Premium (libre-service et automation avancée).

5.2. Couverture fonctionnelle alignée avec les exigences des CISSS et CIUSSS

BLOC FONCTIONNEL RAC/M IDENTITY	EXIGENCES COUVERTES — CISSS ET CIUSSS
Référentiel central d'identités et d'accès, historique complet multi-systèmes	Loi 5, Loi 25, MCN 14.3, LGGRI, Loi sur l'accès.
Connecteurs ICF : AD/LDAP, Entra ID, M365, SQL, JDBC, CSV, SCIM, Octopus ; sectoriels : SIRH (Logibec / Virtuo / Espresso), registre des intervenants, apps cliniques (HL7, REST)	Intégration multi-systèmes RSSS — systèmes RH, cliniques et administratifs.
Cycle joiner-mover-leaver automatisé ; orchestration multi-établissements	MCN 14.1, Loi 25 (moindre privilège), mouvement de personnel RSSS.
RBAC + ABAC multi-attributs ; personnat RSSS (médecins, infirmières, résidents, stagiaires, consultants, comptes fonctionnels)	Moindre privilège, Loi 5 (cercle de soins), séparation des tâches.
Portail libre-service (Premium) en français ; approbation par gestionnaires cliniques	Demandes d'accès, approbations, délégation, certifications par établissement.
Flux d'approbation multi-niveaux ; comptes temporaires, postes partagés, accès d'urgence	MCN 14.1, gestion des accès exceptionnels et des kiosques cliniques.
Certifications planifiées : identités, rôles, comptes à privilèges cliniques	MCN 14.1/14.2, Loi 25, Loi 5 — par programme, établissement, direction.
Analytique : accès orphelins, dérives de droits, indicateurs de risque clinique	Détection sur l'ensemble du parc clinique et administratif.
Provisionnement bidirectionnel : créer, modifier, désactiver vers applications cibles	MCN 14.1, cycle de vie automatisé conforme aux pratiques RSSS.
Journalisation complète : qui-quoi-quand, archivage, export SIEM (Sentinel, Splunk)	MCN 14.3, Loi 25 (registre d'incidents), BCH/TGV, RPSO.
Rapports prédéfinis : par personne, rôle, application, historique	LGGRI, audit MCN, EFVP Loi 25, preuves Loi 5 (accès aux dossiers patients).

SECTION 05, SUITE

5.3. Adéquation spécifique au secteur de la santé québécois

ATTENTE DU MILIEU DE LA SANTÉ	RÉPONSE RAC/M IDENTITY
Hébergement au Canada	Microsoft Azure Canada (centre principal + redondance ≥ 150 km).
Souveraineté des données	OKIOK est une entreprise québécoise ; le CISSS ou CIUSSS demeure l'unique propriétaire de ses données ; formats non propriétaires.
Soutien en français	Interface, documentation, formation, support et services professionnels en français intégral.
Conformité Loi 5 et Loi 25	Architecture conçue pour répondre aux obligations de gouvernance des accès aux renseignements de santé et aux renseignements personnels sensibles.
Conformité MCN 14.1, 14.2, 14.3	Réponse directe et démontrable au CGCD et CO-CD, avec rapports d'audit et journalisation.
Conformité LGGRI, Cadre MSSS (BCH/TGV, RPSO)	Référentiel des accès, rapports de conformité, indicateurs de gestion, contribution à la reddition de comptes au MCN et au MSSS.
Modèle d'identité du milieu de la santé	Prise en charge native des emplois multiples (infirmière + préposée), des lieux d'exercice multiples (plusieurs installations), des populations complexes (médecins, résidents, stagiaires, consultants, partenaires communautaires, comptes fonctionnels).
Banque d'heures pour l'évolution fonctionnelle et nouvelles intégrations	Modèle de service éprouvé pour faire évoluer les fonctionnalités, bonifier les processus et déployer rapidement de nouvelles intégrations vers les systèmes propres au CISSS ou CIUSSS, en cohérence avec sa transformation numérique.
Mode SaaS et environnements jumeaux	Environnement de production et environnement de non-production identiques, conformes aux pratiques d'AO du secteur public.
Déploiement du Dossier Santé Québec (DSQ) - déterminer qui devrait avoir accès au DSQ, à quel niveau de privilège, et maintenir ces habilitations à jour	Référentiel centralisé des rôles et des habilitations DSQ, alimenté par les sources RH et le registre des intervenants ; cycle joiner-mover-leaver automatisé ; certifications périodiques conformes à la Loi 5.

RAC/M Identity n'est pas une alternative à CoreView : il en est le complément requis pour qu'un CISSS ou CIUSSS puisse satisfaire ses obligations légales, répondre aux directives du MCN et du MSSS, couvrir le périmètre des devis GIA dans le RSSS et maximiser le retour sur l'investissement déjà engagé dans CoreView.

À propos d'OKIOK

Fondée en 1973, OKIOK Data Itée est une entreprise québécoise privée entièrement vouée à la cybersécurité.

Plus de 40 ans d'expérience en cybersécurité au service des organisations québécoises. Basée à Montréal, OKIOK conçoit, développe et exploite des solutions de sécurité adaptées aux exigences particulières du marché québécois.

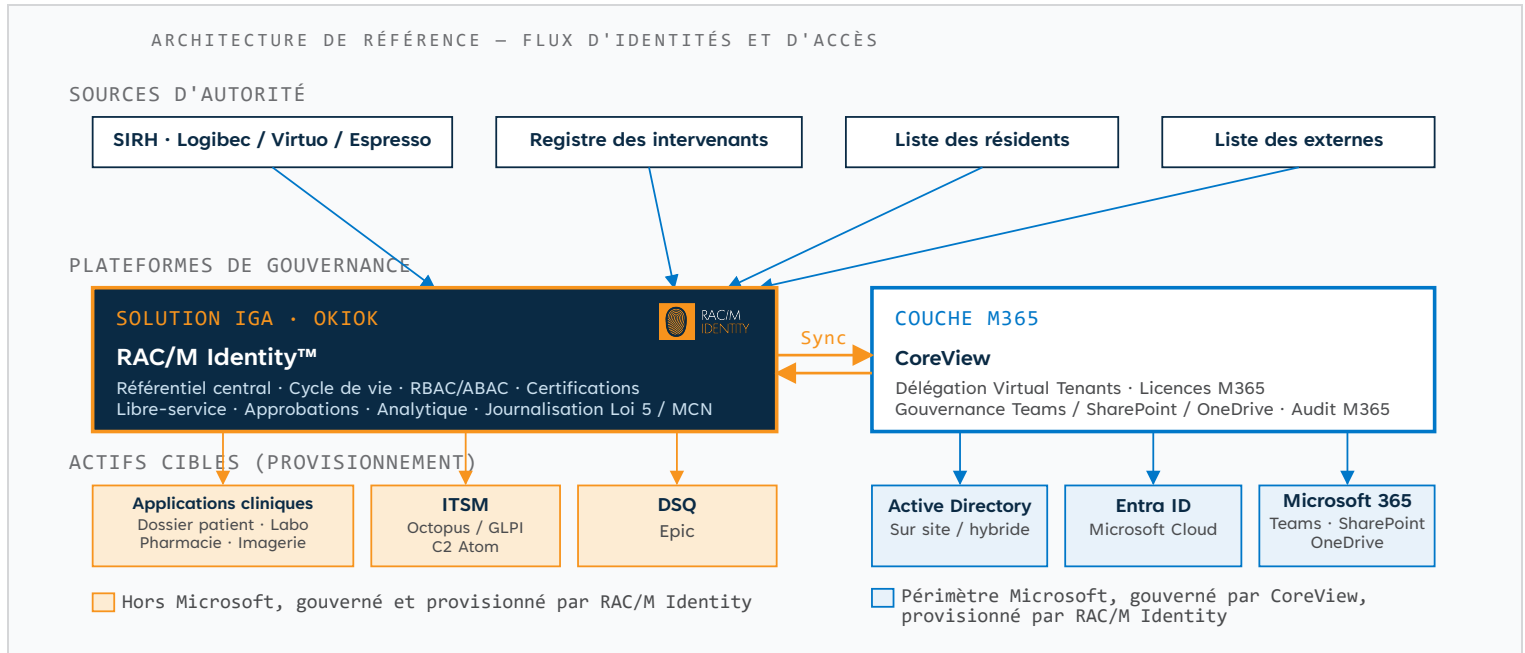
OKIOK conçoit, développe et exploite RAC/M Identity au Québec, avec une équipe locale familière des particularités du réseau de la santé et des services sociaux (RSSS).

RAC/M Identity est déployé dans des entités du gouvernement du Québec ainsi que dans les secteurs de la santé, de l'éducation, du jeu, des médias, de la fabrication et de l'assurance.

Cette proximité se traduit par un soutien réactif en français, des services professionnels conformes aux pratiques d'appel d'offres du secteur public et un partenariat de long terme.

SECTION 06

06 ARCHITECTURE DE RÉFÉRENCE — RAC/M IDENTITY + COREVIEW POUR UN CISSS/CIUSSS



6.1, Répartition des responsabilités

DOMAINE	RAC/M IDENTITY	COREVIEW
Source d'identité d'autorité, cycle de vie	✓	○
Référentiel unique multi-systèmes	✓	○
Connecteurs hors Microsoft (applications cliniques, ITSM, registre des intervenants)	✓	○
RBAC d'entreprise + forage de rôles	✓	○
Libre-service + flux multi-systèmes	✓	○
Approvisionnement automatisé multi-systèmes	✓	○
Certifications d'entreprise (tous actifs)	✓	○
Conformité Loi 5 / Loi 25 / MCN 14.x / LGRI / Cadre MSSS (BCH/TGV, RPSO)	✓	~
Délégation fine M365 aux installations, programmes cliniques, services	○	✓
Gouvernance Teams / SharePoint / OneDrive	○	✓
Optimisation licences M365	○	✓
Audit unifié M365 et revues d'accès M365	○	✓

SECTION 07

07 BÉNÉFICES ET APPROCHE DE MISE EN ŒUVRE RECOMMANDÉE

7.1, Bénéfices pour un CISSS ou CIUSSS

BÉNÉFICE	DESCRIPTION
Conformité démontrable	Réponse directe aux obligations Loi 5, Loi 25, MCN 14.x, LGGRI, cadre MSSS (BCH/TGV, RPSO), avec preuves d'audit exploitables par le CGCD et le CO-CD.
Réponse complète aux devis GIA	RAC/M + CoreView couvre intégralement les devis du milieu (ex. AO 2023-1771, CCSMTL, 211 exigences hors PAM).
Investissement CoreView maximisé	RAC/M apporte la couche IGA d'entreprise multi-systèmes qui manque à CoreView, sans le remplacer.
Risques opérationnels réduits	Désapprovisionnement automatisé au départ, élimination des comptes orphelins cliniques, séparation des tâches et moindre privilège matérialisés.
Efficacité opérationnelle	Provisionnement en minutes pour les mouvements massifs (embauches, mutations, fins de contrat), libre-service en français pour les gestionnaires cliniques et administratifs.
Maîtrise budgétaire	Optimisation des licences M365, évitement des sanctions Loi 25 (jusqu'à 10 M\$), banques d'heures de services professionnels prévisibles.
Souveraineté québécoise	OKIOK partenaire local, données hébergées sur Microsoft Azure Canada, soutien et interface en français intégral.
Évolutivité	Édition <i>Gouvernance</i> → <i>Premium</i> ; évolution fonctionnelle continue et nouvelles intégrations cliniques au rythme de la transformation numérique du RSSS.

7.2, Approche de mise en œuvre en 5 phases

PHASE 01 Découverte et architecture Atelier Loi 5/25 ; inventaire des sources et applications critiques ; définition des personats ; obligations BCH/TGV si applicables ; plan directeur d'intégration. 1 à 2 mois	PHASE 02 Référentiel Déploiement RAC/M Identity ; connexion AD, Entra ID, SIRH, sources autoritaires ; DSQ, premiers connecteurs cliniques et ITSM. 2 à 4 mois	PHASE 03 Modélisation et pilotes Forage et modélisation des rôles ; pilotes sur une installation et un programme clinique ; premières campagnes de certification. 2 à 4 mois	PHASE 04 Libre-service et automatisations Mise en service du portail ; flux d'approbation ; provisionnement automatisé pour arrivée, départ des permanents, médecins, intervenants, résidents, externes, temporaires. 3 à 5 mois	PHASE 05 Évolution et Coreview Intégrations supplémentaires au rythme de la transformation numérique ; synchronisation fine avec les Virtual Tenants Core-View ; évolution vers la maturité IGA cible. En continu
---	---	---	---	--

7.3, Conclusion

RAC/M Identity n'est pas une alternative à CoreView : c'est le complément requis. Ensemble, ils constituent la réponse complète à la conformité GIA d'un CISSS ou CIUSSS québécois.

Le déploiement de CoreView par le gouvernement du Québec est une initiative majeure pour la gouvernance Microsoft 365 dans le RSSS. Il ne supplée toutefois pas une solution IGA d'entreprise capable d'intégrer les systèmes sources, les applications cliniques et les preuves réglementaires attendues des CISSS et CIUSSS.

L'AO 2023-1771 (CCSMTL) illustre le niveau d'exigence : 211 exigences hors PAM, dont 67 obligatoires. CoreView seul ne saurait couvrir cette grille ; RAC/M Identity y répond.

ANNEXE

RÉFÉRENCES RÉGLEMENTAIRES ET TECHNIQUES

CADRE LÉGAL ET RÉGLEMENTAIRE

- *Loi concernant les renseignements de santé et des services sociaux*, RLRQ c. R-22.1 (Loi 5).
- *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (« Loi 25 »), L.Q. 2021, c. 25.
- *Loi sur la gouvernance et la gestion des ressources informationnelles*, RLRQ chapitre G-1.03 (LGRI).
- *Loi sur les services de santé et les services sociaux*, RLRQ chapitre S-4.2 (LSSSS).
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ chapitre A-2.1.
- *Loi concernant le cadre juridique des technologies de l'information*, RLRQ chapitre C-1.1.
- Ministère de la Cybersécurité et du Numérique, *Cadre gouvernemental de gestion de la sécurité de l'information*, exigences 14.1, 14.2, 14.3.
- Ministère de la Santé et des Services sociaux, *Cadre normatif de sécurité de l'information* : BCH / Trousse globale de vérification (TGV), Règles particulières sur la sécurité organisationnelle (RPSO), GMVI.

RÉFÉRENCE D'APPEL D'OFFRES CITÉE

- Centre intégré universitaire de santé et de services sociaux du Centre-Sud-de-l'Île-de-Montréal (CCSMTL), *Devis technique, Acquisition d'une solution PAM et GIA, Appel d'offres n° 2023-1771*, cité comme exemple représentatif d'un devis GIA dans le RSSS ; volet PAM hors périmètre du présent document.

DOCUMENTATION PRODUITS

- OKIOK Data Itée, [Documentation RAC/M Identity \(français\)](#).
- CoreView, [CoreView ONE Overview](#).
- CoreView, [Microsoft 365 Governance & Lifecycle Management](#).
- CoreView, [Access Reviews](#).

À PROPOS DU PRÉSENT DOCUMENT

Ce livre blanc a été préparé par OKIOK Data Itée à l'intention des dirigeants TI, RSSI, gestionnaires de la conformité, directions générales et responsables de l'approvisionnement des centres intégrés de santé et de services sociaux (CISSS) et des centres intégrés universitaires de santé et de services sociaux (CIUSSS) du Québec, ainsi que de tout organisme public du réseau de la santé et des services sociaux (RSSS) assujetti aux directives du MCN et aux orientations du MSSS.

Les informations relatives à CoreView reflètent l'état public connu de la solution au moment de la rédaction. Les marques de commerce mentionnées appartiennent à leurs détenteurs respectifs.

— PROCHAINE ÉTAPE

DISCUTONS DU CHEMIN DE CONFORMITÉ DE VOTRE CISSS OU CIUSSS

Passez de la réflexion à l'action : planifiez dès aujourd'hui une session d'échange avec OKIOK afin de découvrir comment RAC/M Identity peut répondre à vos besoins, relever vos défis et vous aider à atteindre vos objectifs de conformité, de productivité et de réduction des risques, en remplissant notre formulaire de demande en ligne [ici](#), ou en nous écrivant à info@okiok.com.

SOLUTION

RAC/M Identity

Solution IGA 100 % québécoise

[Documentation](#)

HÉBERGEMENT

Microsoft Azure Canada

Conforme Loi 25 · SOC 2 Type II

SOUTIEN

Français, anglais

Équipe francophone, basée au Québec

www.okiok.com

© 2026 OKIOK DATA LTÉE, TOUS DROITS RÉSERVÉS.
TOUTES LES MARQUES DE COMMERCE ET MARQUES DÉPOSÉES
MENTIONNÉES DANS CE DOCUMENT SONT LA PROPRIÉTÉ
EXCLUSIVE DE LEURS DÉTENTEURS RESPECTIFS.