SECTOR - QUEBEC HEALTH AND SOCIAL SERVICES

IAM COMPLIANCE - CISSS AND CIUSSS

RAC/M IDENTITY AND COREVIEW
A REQUIRED COMBINATION FOR IGA COMPLIANCE

In the context of the RSSS digital transformation and the provincial rollout of the Dossier Santé Québec (DSQ), how to complement the government-wide deployment of CoreView to meet the legal, regulatory and operational obligations around digital identity and access management.

RAC/M IDENTITY

PREPARED BY
OKIOK Data Ltd

VERSION
1.0

DATE
Mai 2026

OKIOK
CYBERSECURITY SIMPLIFIED

EXECUTIVE SUMMARY

WHY COREVIEW ALONE IS NOT ENOUGH, AND WHAT IS REQUIRED

The Government of Québec is progressively deploying CoreView across the health and social services network (RSSS) to strengthen Microsoft 365 governance. This is an important step forward, but one strictly limited to the Microsoft ecosystem, a subset of the perimeter that the law imposes on CISSS and CIUSSS.

The obligations of CISSS and CIUSSS, including *Law 5* (health information), *Law 25*, the MCN directives (14.1, 14.2, 14.3), the *LGGRI*, the *MSSS normative framework* (BCH/TGV, RPSO, GMVI) and the *Access Act*, require end-to-end identity lifecycle management across all CISSS or CIUSSS assets, well beyond Microsoft 365.

This includes HR systems (payroll HRIS, often Logibec, Virtuo, Espresso), the care provider registry, clinical applications (patient records, lab, imaging, pharmacy), LDAP and SQL directories, and ITSM tools (Octopus, GLPI, C2 Atom).

As an illustration, RFP 2023-1771 from CCSMTL (IGA component, excluding PAM) includes 211 requirements, 67 of which are MANDATORY in the eliminatory sense. An analysis shows CoreView alone would cover only approximately 35–40% of all criteria; the 67 mandatory requirements address a multi-system IGA scope that CoreView does not cover by design.

This white paper demonstrates that RAC/M Identity is not an alternative to CoreView: it is the required complement for a CISSS or CIUSSS to meet its legal obligations, respond to RSSS IGA specifications, and maximize the return on the investment already made in CoreView.

211

Requirements (excl. PAM) in the RFP 2023-1771 standard grid (CCSMTL), including 67 MANDATORY eliminatory criteria.

~65 %

Estimated share of criteria outside CoreView's scope alone.

10 M$

Maximum administrative penalty under Law 25 (or 2% of global revenue).

SCOPE

This white paper deals exclusively with the digital identity governance (IGA) component. The privileged access management (PAM) component appearing in certain combined IGA+PAM RFPs (including RFP 2023-1771) is deliberately excluded; it falls under separate solutions and rationale.

SECTION OVERVIEW

TABLE OF CONTENTS

SECTION 01

01 THE RSSS DIGITAL TRANSFORMATION CONTEXT

1.1, A Strategic Trajectory and Health Sovereignty Challenges

The RSSS digital transformation is part of the Québec government's *Digital Transformation Strategy*, the creation of the Ministry of Cybersecurity and Digital Technology (MCN) and the priorities of the Ministry of Health and Social Services (MSSS) in clinical interoperability, information security and infrastructure modernization. CISSS and CIUSSS must simultaneously:

- Deliver safe and effective services to users (care, social services, prevention, university education integrated in CIUSSS);
- Reduce cyber risks in a heavily targeted sector (ransomware, intrusion, privileged account compromise);
- Ensure the confidentiality of health and social services information, among the most sensitive data processed by the State.

Adding to this is the provincial rollout of the Dossier Santé Québec (DSQ), one of the most structuring projects in the network's digital transformation. By centralizing access to users' health information for all authorized care providers across Québec, the DSQ demands more rigorous identity governance: each CISSS and CIUSSS must precisely determine who is entitled to access the DSQ, at what privilege level, and ensure those entitlements evolve in real time with staff roles and movements. CoreView contributes to securing the Microsoft environment that partially supports this deployment, but it is RAC/M Identity that enables the organization to define, automate and certify DSQ entitlements at the organizational scale.

1.2, The Central Role of Microsoft 365 in Healthcare Organizations

The technological environment of CISSS and CIUSSS relies heavily on Microsoft 365: Active Directory and Entra ID (often hybrid), Teams for clinical and administrative collaboration, SharePoint and OneDrive, Exchange Online, Power BI for dashboards, all in a context of identity federation, partner guests and multiple physical locations (hospitals, CHSLD, CLSC, administrative centres).

This foundation justifies a powerful M365 governance layer: that is the natural role of CoreView.

1.3, The Deployment of CoreView in the RSSS

As with other public sectors, the Government of Québec is directing the deployment of CoreView to strengthen controlled delegation, Teams / SharePoint / OneDrive governance, licence optimization, Entra application monitoring and access reviews within the Microsoft 365 perimeter. CoreView substantially improves the operational posture on M365.

> **KEY TAKEAWAY**
>
> CoreView is an excellent product within its scope: the governance and administration of Microsoft 365 and Entra ID. But that scope is strictly limited to the Microsoft ecosystem, whereas the legal and regulatory obligations of CISSS and CIUSSS require end-to-end management across the entire application and organizational landscape.

SECTION 02

02 THE REAL IGA REQUIREMENTS FOR A CISSS OR CIUSSS

2.1, Illustrative Case: CCSMTL RFP 2023-1771 (IGA Component)

The Centre intégré universitaire de santé et de services sociaux du Centre-Sud-de-l'Île-de-Montréal (CCSMTL) published technical specification RFP 2023-1771 for a combined PAM and IGA solution. Isolating the IGA component and non-PAM cross-cutting requirements yields 211 requirements, of which 67 are MANDATORY in the eliminatory sense.

The technical specification notably requires a SaaS IGA solution meeting a DIC 3-4-4 rating, identification of source systems (HRIS, care provider registry), definition of at least six (6) personas, lifecycle integration toward a minimum of six (6) clinical applications, Octopus ticketing, MCN and MSSS compliance, and log export to Microsoft Sentinel or Splunk.

> *These expectations are representative of large-scale IGA projects in the RSSS: any CISSS or CIUSSS modernizing its IGA will face an analogous combination of multiple authority sources, critical clinical applications and regulatory evidence requirements.*

2.2, Structural Characteristics of CISSS and CIUSSS

- Multiple authority sources: payroll HRIS (Logibec, Virtuo, Espresso or equivalent), care provider registry, scheduling and attendance systems, profession-specific HR records (nurses, physicians, orderlies), ITSM (Octopus, GLPI, C2 Atom);
- Clinical and business applications: patient records, laboratory, imaging, pharmacy, university applications for CIUSSS, in addition to Microsoft 365;
- Heterogeneous populations: unionized employees, managers, physicians, residents, interns, community partners, consultants, external users;
- Multiple practice locations: a single staff member may work across several facilities or programs;
- Functional and technical accounts: temps, shared clinical workstations, kiosks, service accounts;
- Enhanced legal constraints on health information (Law 5) and personal information (Law 25).

SECTION 02, CONTINUED

2.3, Summary of Standard Requirement Blocks (RFP 2023-1771 Grid, Excl. PAM)

These requirements exceed the functional scope of a tool limited to Microsoft 365, however capable it may be within that scope.

BLOCK	EXPECTATION HIGHLIGHTS
A – Lifecycle and Integration	Automated provisioning/deprovisioning; self-service and workflows; RBAC/ABAC; scheduled access reviews; REST API; Entra ID, AD, LDAP, SQL, SaaS connectors; HR synchronization.
B – Services and Hosting	SaaS; data in Canada (ideally Québec); data ownership; SLA; backups; non-prod environments; API documentation.
C – Security and Compliance	Security architecture; detailed logging and SIEM export; encryption; BCP/DRP; vulnerability management; MFA, OIDC, SAML, OAuth2; console administrative RBAC; secondary use prohibition; MSSS/MCN framework.
E – Enterprise	Project plans; references; French guides; 24/7 availability; commitment to RFP service levels.

ESTIMATED COVERAGE

PERSPECTIVE	COREVIEW ALONE	RAC/M IDENTITY
All 211 requirements (excl. PAM)	~35–40 %	Conforme
Block A (IGA functions)	~20–25 %	Conforme
MANDATORY requirements (67)	Majority uncovered → rejection	Conforme

CONSEQUENCE

CoreView deployed alone could not constitute an acceptable IGA solution response to an RFP such as RFP 2023-1771. The 67 mandatory requirements predominantly address a multi-system IGA scope that CoreView, by design, does not cover.

SECTION 03

03 THE LEGAL AND REGULATORY FRAMEWORK APPLICABLE TO CISSS AND CIUSSS

IGA is not merely an operational best practice: for a CISSS or CIUSSS, it is a multi-level legal obligation.

3.1, Law 5: Health and Social Services Information

The *Act Respecting Health and Social Services Information* (Law 5, chapter R-22.1) governs the collection, retention, access to and communication of personal information in the user's record. It notably requires compliance with the circle-of-care principle, legitimate purposes, the minimum-necessary standard and individual rights.

Implications for IGA: the CISSS or CIUSSS must be able to demonstrate who accesses which systems and records, on what basis (role, mandate, care relationship), with traceability and periodic controls. A platform covering only M365 does not satisfy this requirement for clinical records and business applications outside the Microsoft cloud.

The DSQ rollout reinforces this requirement: care providers at CISSS and CIUSSS who access the user's record through the DSQ must do so strictly within the circle-of-care framework defined by Law 5. RAC/M Identity provides the authority repository that enables the organization to ensure each provider has the right level of DSQ access based on their role, program and practice location, and that this access is revoked without delay upon departure or a change of position.

3.2, Law 25: Personal Information Protection

LAW 25 OBLIGATION	IGA IMPLICATION FOR A CISSS/CIUSSS
Privacy Officer for personal information	Must demonstrate who accesses which PI, across all systems where nominative data resides.
PIA for any project involving PI	Requires precise knowledge of the access model and its governance.
Incident register and notification to the CAI	Requires complete access logging and anomaly detection.
Least privilege, purpose limitation, time-limited access	Automatic assignment and revocation rules; periodic certification campaigns.
Access, rectification and portability rights (users, employees)	Historical traceability of access and modifications.
Penalties up to $10M or 2% of global revenue	Direct financial risk and personal liability for executives.

> *Health information is among the most sensitive data processed by the Québec government. CoreView cannot demonstrate who accesses what information in non-Microsoft clinical systems, yet that is precisely where the majority of care data resides.*

SECTION 03, CONTINUED

3.3, MCN Directives: Requirements 14.1, 14.2 and 14.3

MEASURE	DESCRIPTION	COVERAGE REQUIRED FOR A CISSS/CIUSSS
14.1	Process for adding, reviewing and revoking access to manage staff movement.	Full lifecycle (joiner-mover-leaver) for all assets, clinical applications, AD/LDAP directories, ITSM.
14.2	Dedicated and reviewed process for highly privileged/administrator accounts.	AD domain admins, critical clinical application pilot accounts, DBAs, often beyond Microsoft 365 alone.
14.3	Access and identity logging tool implemented.	Central multi-platform logging, verifiable by CGCD and CO-CD.

3.4, LGGRI and Information Governance

The LGGRI (CQLR chapter G-1.03) mandates a master plan, information asset inventory, accountability and security reports to the MCN. IGA is a central lever for the compliance evidence expected by ministerial bodies.

3.5, MSSS Framework: BCH, TGV, RPSO and Incident Management

Recent RSSS RFPs frequently require BCH certification and the Global Verification Toolkit (TGV), compliance with the Specific Organizational Security Rules (RPSO) and GMVI processes. An IGA solution must integrate with these evidentiary requirements: documented architecture, actionable logs, alignment with Sentinel/Splunk flows.

3.6. Summary: Why IGA Is Legally Mandatory for a CISSS and a CIUSSS

QUESTION	ANSWER
Can a CISSS or CIUSSS do without an enterprise IGA platform?	No. Without IGA, it cannot demonstrate compliance with Law 5, Law 25, MCN and LGGRI across all critical assets.
Is CoreView alone sufficient?	No, for the multi-system scope including HR, care provider registry, clinical applications and evidence outside M365.
What does the organization risk?	Law 25 penalties, audit non-compliance, reputational incidents and clinical risks from inappropriate access.

> **INTERIM CONCLUSION**
>
> CISSS and CIUSSS must be able to prove their compliance, not merely assert it. An enterprise IGA platform covering the entire application landscape is, for all practical purposes, indispensable to produce that proof.

SECTION 04

04 COREVIEW: ITS STRENGTHS AND STRUCTURAL LIMITATIONS

4.1, What CoreView Does Exceptionally Well

CAPABILITY	DESCRIPTION
Granular M365 Delegation	Virtual Tenants, reduction of escalations to the service desk.
Teams / SharePoint / OneDrive Governance	Politiques, external sharing, sites et équipes à grande échelle.
Licence Optimization	Recovery and reallocation of M365 seats.
Entra Applications	Visibility into permissions, secrets and owners.
Unified M365 Audit	Investigation and correlation within the Microsoft perimeter.
M365 Access Reviews	Campaigns on groups, Teams, SharePoint, mailboxes, guests.

4.2, Structural Limitations for a CISSS / CIUSSS

STANDARD REQUIREMENT (E.G. RFP 2023-1771, GRID EXCL. PAM)	LIMITATION
Multi-source repository (SQL HR, CSV registry, LDAP, business SQL) with correlation and history	Focused on M365/Entra; not a complete multi-asset IGA repository.
Bidirectional provisioning to six clinical applications + Octopus per RSSS processes	Outside native scope; requires an IGA with business connectors.
RBAC/ABAC on business roles for hospital personas and complex profiles	CoreView RBAC = M365 platform operators, not the CIUSSS organizational model.
Certifications and reviews across all RSSS IT assets	Limited to Microsoft 365 resources.
REST API with an IGA-complete function inventory	Not equivalent to a complete IGA API for enterprise lifecycle.
Law 5 evidence on patient record access in business information systems	Does not cover these systems.

> **CONCLUSION**
>
> CoreView is necessary but not sufficient. It must be complemented by an IGA platform such as RAC/M Identity.

SECTION 05

05 RAC/M IDENTITY: THE IGA PLATFORM THAT COMPLEMENTS COREVIEW

5.1, Overview

RAC/M Identity is the IGA platform developed by OKIOK Data Ltd, a Québec-based company. It provides a central identity and access repository, connectors to source and target systems, certification campaigns, self-service, approval workflows and compliance-oriented logging.

ATTRIBUTE	VALUE
Deployment model	SaaS (client-dedicated Microsoft Azure), managed services or on-premise.
Hosting	Data centres in Canada, Law 25 compliant.
Langues	Full French (interface, documentation, support).
Certifications	SOC 2 Type II, ISO 9001, ISO 27001/27002, tests d'intrusion périodiques.
Editions	Gouvernance et Premium (libre-service et automation avancée).

5.2. Functional Coverage Aligned with CISSS and CIUSSS Requirements

RAC/M IDENTITY FUNCTIONAL BLOCK	REQUIREMENTS COVERED, CISSS AND CIUSSS
Central identity and access repository, complete multi-system history	Loi 5, Loi 25, MCN 14.3, LGGRI, Loi sur l'accès.
ICF Connectors: AD/LDAP, Entra ID, M365, SQL, JDBC, CSV, SCIM, Octopus; sector-specific: HRIS (Logibec / Virtuo / Espresso), care provider registry, clinical apps (HL7, REST)	RSSS multi-system integration, HR, clinical and administrative systems.
Automated joiner-mover-leaver cycle; multi-facility orchestration	MCN 14.1, Law 25 (least privilege), RSSS staff movement.
Multi-attribute RBAC + ABAC; RSSS personas (physicians, nurses, residents, interns, consultants, functional accounts)	Least privilege, Law 5 (circle of care), segregation of duties.
Bilingual self-service portal (Premium); approval by clinical managers	Access requests, approvals, delegation, certifications by facility.
Multi-level approval workflows; temporary accounts, shared workstations, emergency access	MCN 14.1, management of exceptional access and clinical kiosks.
Scheduled certifications: identities, roles, clinical privileged accounts	MCN 14.1/14.2, Law 25, Law 5, by program, facility, department.
Analytics: orphan access, entitlement drift, clinical risk indicators	Detection across the entire clinical and administrative landscape.
Bidirectional provisioning: create, modify, deactivate toward target applications	MCN 14.1, automated lifecycle compliant with RSSS practices.
Complete logging: who-what-when, archiving, SIEM export (Sentinel, Splunk)	MCN 14.3, Law 25 (incident register), BCH/TGV, RPSO.
Predefined reports: by person, role, application, history	LGGRI, MCN audit, PIA Law 25, Law 5 evidence (patient record access).

SECTION 05, CONTINUED

5.3. Specific Fit for the Quebec Health Sector

HEALTH SECTOR EXPECTATION	RAC/M IDENTITY RESPONSE
Canadian Hosting	Microsoft Azure Canada (primary centre + redundancy ≥ 150 km).
Data Sovereignty	OKIOK is a Québec company; the CISSS or CIUSSS remains the sole owner of its data; non-proprietary formats.
Bilingual Support	Interface, documentation, training, support and professional services fully bilingual.
Law 5 and Law 25 Compliance	Architecture designed to meet access governance obligations for health information and sensitive personal information.
MCN 14.1, 14.2, 14.3 Compliance	Direct and demonstrable response to CGCD and CO-CD, with audit reports and logging.
LGGRI and MSSS Framework (BCH/TGV, RPSO) Compliance	Access repository, compliance reports, management indicators, contribution to accountability reporting to MCN and MSSS.
Health Sector Identity Model	Native support for multiple personas (nurse + orderly), multiple practice locations (several facilities), complex populations (physicians, residents, interns, consultants, community partners, functional accounts).
Professional Services Hours Bank for Functional Evolution and New Integrations	Proven service model to evolve features, improve processes and rapidly deploy new integrations toward CISSS or CIUSSS-specific systems, in line with its digital transformation.
SaaS Mode and Twin Environments	Identical production and non-production environments, compliant with public sector RFP practices.
Dossier Santé Québec (DSQ) Deployment - determining who should have access to the DSQ, at what privilege level, and keeping entitlements up to date	Centralized repository of DSQ roles and entitlements, fed by HR sources and the care provider registry; automated joiner-mover-leaver cycle; periodic certifications compliant with Law 5.

> RAC/M Identity is not an alternative to CoreView: it is the required complement for a CISSS or CIUSSS to meet its legal obligations, respond to MCN and MSSS directives, cover the IGA specification scope in the RSSS and maximize the return on the investment already made in CoreView.

About OKIOK

Founded in 1973, OKIOK Data Ltd is a private Québec company entirely dedicated to cybersecurity.

Over 40 years of cybersecurity experience serving Québec organizations. Based in Montréal, OKIOK designs, develops and operates security solutions tailored to the specific requirements of the Québec market.

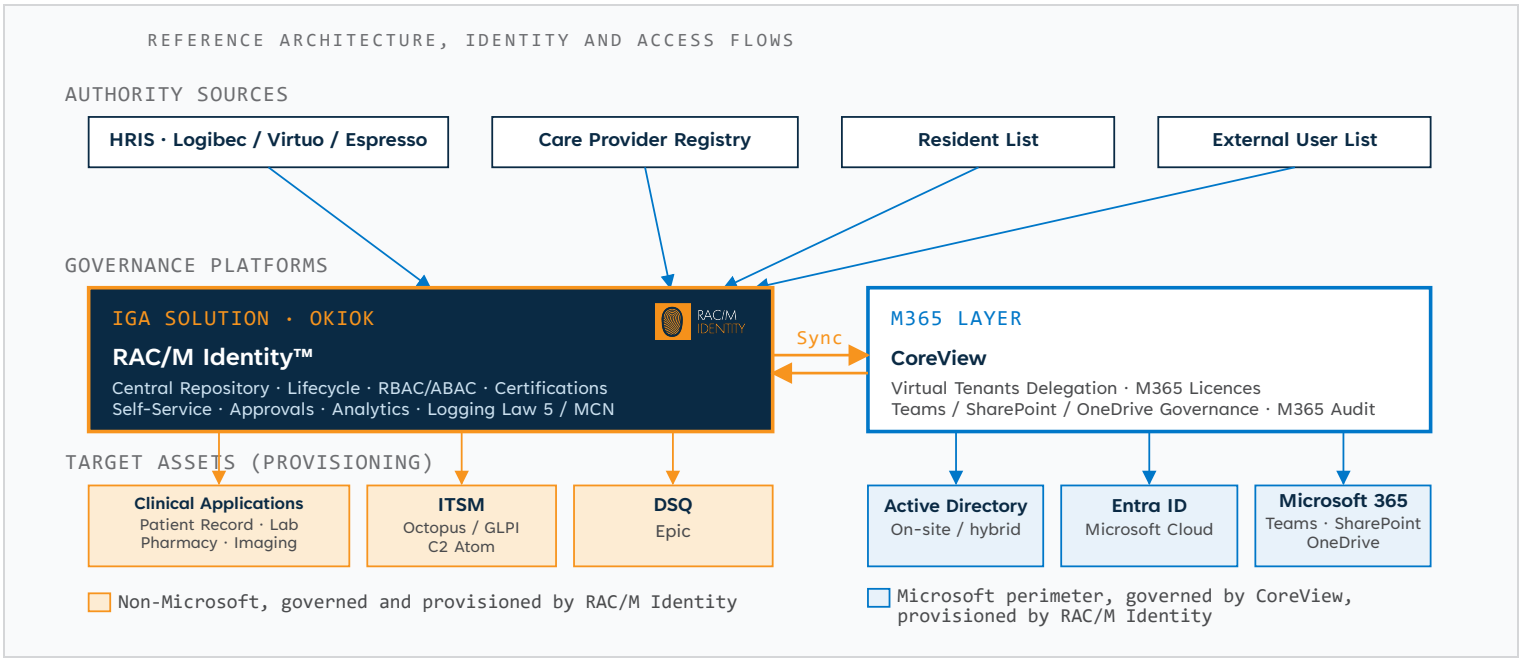
OKIOK designs, develops and operates RAC/M Identity in Québec, with a local team familiar with the specific characteristics of the health and social services network (RSSS).

RAC/M Identity is deployed in Québec government entities as well as in the health, education, gaming, media, manufacturing and insurance sectors.

This proximity translates into responsive bilingual support, professional services aligned with public sector RFP practices and a long-term partnership.

SECTION 06

06 REFERENCE ARCHITECTURE, RAC/M IDENTITY + COREVIEW FOR A CISSS/CIUSSS



6.1, Responsibility Distribution

DOMAIN	RAC/M IDENTITY	COREVIEW
Authority identity source, lifecycle	✓	○
Single multi-system repository	✓	○
Non-Microsoft connectors (DSQ, clinical apps, ITSM, care provider registry)	✓	○
Enterprise RBAC + role mining	✓	○
Self-service + multi-system workflows	✓	○
Automated multi-system provisioning	✓	○
Enterprise certifications (all assets)	✓	○
Law 5 / Law 25 / MCN 14.x / LGGRI / MSSS Framework (BCH/TGV, RPSO) Compliance	✓	~
Granular M365 delegation to facilities, clinical programs, departments	○	✓
Teams / SharePoint / OneDrive Governance	○	✓
M365 Licence Optimization	○	✓
Unified M365 audit and M365 access reviews	○	✓

SECTION 07

07 BENEFITS AND RECOMMENDED IMPLEMENTATION APPROACH

7.1, Benefits for a CISSS or CIUSSS

BENEFIT	DESCRIPTION
Demonstrable Compliance	Direct response to Law 5, Law 25, MCN 14.x, LGGRI, MSSS framework (BCH/TGV, RPSO) obligations, with audit evidence actionable by CGCD and CO-CD.
Complete Response to IGA Specifications	RAC/M + CoreView fully covers sector specifications (e.g. RFP 2023-1771, CCSMTL, 211 requirements excl. PAM).
CoreView Investment Maximized	RAC/M provides the enterprise multi-system IGA layer that CoreView lacks, without replacing it.
Reduced Operational Risks	Automated deprovisioning upon departure, elimination of clinical orphan accounts, segregation of duties and least privilege enforced.
Operational Efficiency	Provisioning in minutes for mass movements (hires, transfers, terminations), French self-service for clinical and administrative managers.
Budget Control	M365 licence optimization, avoidance of Law 25 penalties (up to $10 M), predictable professional services hours banks.
Québec Sovereignty	OKIOK as a local partner, data hosted on Microsoft Azure Canada, full French-language support and interface.
Scalability	Edition *Governance→Premium* ; continuous functional evolution and new clinical integrations at the pace of the RSSS digital transformation.

7.2, 5-Phase Implementation Approach

PHASE 01
Discovery and Architecture
Law 5/25 workshop; inventory of critical sources and applications; persona definition; BCH/TGV obligations if applicable; integration master plan.
1 to 2 months

PHASE 02
Repository
RAC/M Identity deployment; AD, Entra ID, HRIS, authority source connections; DSQ, first clinical and ITSM connectors.
2 to 4 months

PHASE 03
Modelling and Pilots
Role mining and modelling; pilots at one facility and one clinical program; first certification campaigns.
2 to 4 months

PHASE 04
Self-Service and Automation
Portal go-live; approval workflows; automated provisioning for onboarding and offboarding of permanent staff, physicians, care providers, residents, externals and temps.
3 to 5 months

PHASE 05
Evolution and CoreView
Additional integrations at the pace of digital transformation; fine-grained synchronization with CoreView Virtual Tenants; evolution toward the target IGA maturity.
Ongoing

7.3, Conclusion

RAC/M Identity is not an alternative to CoreView: it is the required complement. Together, they constitute the complete answer to IGA compliance for a Québec CISSS or CIUSSS.

The Government of Québec's deployment of CoreView is a major initiative for Microsoft 365 governance in the RSSS. It does not, however, substitute for an enterprise IGA solution capable of integrating the source systems, clinical applications and regulatory evidence expected of CISSS and CIUSSS.

RFP 2023-1771 (CCSMTL) illustrates the level of requirements: 211 requirements excluding PAM, of which 67 are mandatory. CoreView alone cannot cover this grid; RAC/M Identity does.

ANNEX

REGULATORY AND TECHNICAL REFERENCES

LEGAL AND REGULATORY FRAMEWORK

- *Act Respecting Health and Social Services Information*, CQLR c. R-22.1 (Law 5).
- *Act to Modernize Legislative Provisions as Regards the Protection of Personal Information* ("Law 25"), S.Q. 2021, c. 25.
- *Act Respecting the Governance and Management of Information Resources*, CQLR chapter G-1.03 (LGGRI).
- *Act Respecting Health Services and Social Services*, CQLR chapter S-4.2 (LSSSS).
- *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, CQLR chapter A-2.1.
- *Act to Establish a Legal Framework for Information Technology*, CQLR chapter C-1.1.
- Ministry of Cybersecurity and Digital Technology, *Government Information Security Management Framework*, requirements 14.1, 14.2, 14.3.
- Ministry of Health and Social Services, *Information Security Normative Framework*: BCH / Global Verification Toolkit (TGV), Specific Organizational Security Rules (RPSO), GMVI.

REFERENCED RFP

- Centre intégré universitaire de santé et de services sociaux du Centre-Sud-de-l'Île-de-Montréal (CCSMTL), *Technical Specification, Acquisition of a PAM and IGA Solution, RFP No. 2023-1771*, cited as a representative example of an IGA specification in the RSSS; PAM component is outside the scope of this document.

PRODUCT DOCUMENTATION

- OKIOK Data Ltd, RAC/M Identity Documentation (French).
- CoreView, CoreView ONE Overview.
- CoreView, Microsoft 365 Governance & Lifecycle Management.
- CoreView, Access Reviews.

ABOUT THIS DOCUMENT

This white paper was prepared by OKIOK Data Ltd for IT executives, CISOs, compliance managers, general management and procurement officers of Québec's integrated health and social services centres (CISSS) and integrated university health and social services centres (CIUSSS), as well as any public body in the health and social services network (RSSS) subject to MCN directives and MSSS guidance.

Information relating to CoreView reflects the publicly known state of the solution at the time of writing. All trademarks mentioned are the property of their respective owners.

PROCHAINE ÉTAPE

LET'S DISCUSS YOUR CISSS OR CIUSSS COMPLIANCE PATH

Move from reflection to action: schedule a conversation with OKIOK today to discover how RAC/M Identity can address your needs, meet your challenges and help you achieve your compliance, productivity and risk-reduction goals, by completing our online request form here, or by writing to us at info@okiok.com.

SOLUTION

RAC/M Identity

100 % Québec-based IGA solution

Documentation

HÉBERGEMENT

Microsoft Azure Canada

Law 25 compliant · SOC 2 Type II

SUPPORT

French, English

Fully bilingual team, based in Québec

www.okiok.com

OKIOK

© 2026 OKIOK DATA LTD, ALL RIGHTS RESERVED.
ALL TRADEMARKS AND REGISTERED TRADEMARKS MENTIONED IN THIS DOCUMENT ARE THE EXCLUSIVE PROPERTY OF THEIR RESPECTIVE OWNERS.