ISRM

THE INSTITUTE OF STRATEGIC
RISK MANAGEMENT

RISKS AND OPPORTUNITIES ASSOCIATED WITH COMPETING OPTIONS FOR ACHIEVING A SOVEREIGN CLOUD INFRASTRUCTURE

by David Aanye M.ISRM

Data sovereignty and autonomy are increasingly critical to national security. Canadians' growing dependence on digital services for daily needs, accelerated by rapid digital transformation, generates vast quantities of data. As a result, ensuring data sovereignty and autonomy is essential for protecting Canada's national security and independence. Achieving this requires a sovereign cloud: advanced computing infrastructure and data centers hosting Canadian data located within national borders, with domestic control over the data and no foreign access. However, most leading global cloud providers used by Canadian businesses, agencies, and federal departments are non-Canadian corporations, placing Canadian data at risk of foreign government access. Consequently, Canada must pursue financially viable, competitive, and strategically sound measures to leverage leading global cloud technologies in achieving data sovereignty.

DEVELOPMENT: BACKGROUND AND CURRENT SITUATION

Prime Minister Mark Carney, in September 2025, while announcing the Major Project Office (MPO) inaugural priorities in Edmonton, intimated that investing in sovereign cloud "… would build compute capacity and data centers that we need to underpin Canada's competitiveness, to protect our security, and to boost our independence and sovereignty". He intimated further that "This will give Canada independent control over advanced computing power while reinforcing our leadership in AI and quantum," thereby highlighting the national imperative of building a sovereign Canadian cloud.

Furthermore, under Budget 2025, the Canadian government allocated $925.6 million, starting in 2025-2026, to develop large-scale sovereign cloud and compute infrastructure. Commentators and analysts are divided on whether Canada should focus on building homegrown cloud infrastructure or leverage global cloud technology with sovereignty embedded in contractual and procurement rules to build Canadian-based servers.

In addition, the seemingly changing relationship between Canada and the US increasingly gives impetus to the discourse that Canada needs a sovereign cloud. Some Canadian businesses and federal departments rely on major global cloud providers such as Google and Amazon to run their services. Amazon, for instance, hosts applications that support Canada's Department of National Defense's operational readiness and national security data. Moreover, a Senate hearing in France in June this year, during which Microsoft could not guarantee that the company would not transmit French citizens' data to the US authorities without the explicit authorization of the French authorities. This signals that Canadians could have their data provided to the US government under the US Cloud Act, as some Canadian businesses and federal departments depend on US-based corporations such as Microsoft. This brings renewed interest in commentaries on Canadian data autonomy and sovereignty.

ANALYSIS AND CONSIDERATION

HOMEGROWN SOVEREIGN CLOUD INFRASTRUCTURE

Proponents argue that aside from the data sovereignty and autonomy that the homegrown cloud infrastructure potentially promises, investing in local cloud infrastructure will create jobs through Canadian businesses and innovators, which will ultimately boost the domestic economy. However, Canada risks pouring scarce financial resources into expensive new cloud infrastructure that will essentially seek to duplicate global systems with no guaranteed performance quality and competitiveness. For instance, project Gaia-X was initially a European cloud initiative aimed at replicating cloud infrastructure to counter the dominance of cloud technology by non-European corporations and ensure data sovereignty. However, its focus over time got narrowed to focus on interoperability, standards, and governance because its original focus was found to be, among other challenges, financially exhausting. Additionally, a Canadian-only cloud might lag well-established global cloud providers in terms of features, standards, and interoperability.

LEVERAGE GLOBAL CLOUD TECHNOLOGY WITH SOVEREIGNTY EMBEDDED IN CONTRACTUAL/PROCUREMENT RULES TO BUILD A SOVEREIGN CLOUD

Proponents argue that adopting appropriate contractual agreements to leverage global cloud technology in building a sovereign cloud in Canada is strategically effective and guarantees better cloud services. Sovereign cloud is better achieved when embedded in enforceable contracts, cryptography, and procurement rules that grant only Canadian-cleared personnel access to Canadian data while monitoring to enforce access rules. Contractual rules and smart procurement governed under only Canadian laws will ensure domestic control over data while leveraging the best global technology. The UK Ministry of Defense, for instance, recently signed a sovereign cloud contract that is staffed and governed entirely under UK law. This approach ensures continuous interoperability with Five Eyes partners for exchanging highly classified defense, national security, and intelligence data, and will boost Canada's potential negotiations to join the high-technology portion of the AUKUS agreement.

CONCLUSION

The increasing reliance on digital services by Canadians for everyday living needs, spurred by the rapid rate of digital transformation, generates a huge quantity of data daily. This underscores the urgency and importance of ensuring data sovereignty and autonomy to protect Canada's national security and independence. Below are concluding recommendations on how Canada could achieve sovereign cloud.

- Partner with major global cloud providers through enhanced procurement rules and standards, contractual and encryption agreements that guarantee domestic control over access to Canadian data stored on Canadian-owned servers.
- Channeling more investment capital towards exploring niches in emerging technologies, including Artificial intelligence and quantum computing to enhance Canada's sovereign capabilities in these technologies.

While the idea of building new, homegrown cloud platforms has received considerable commentary and attention in various countries, including Canada, it is becoming quite clear that partnerships with well-established global cloud providers, through contracts and procurement rules that guarantee domestic control over access to data, are financially plausible and strategically effective.

Key Message: **Canada's path to digital sovereignty lies in securing control over its data through strong partnerships, smart investment in emerging technologies, and clear national standards.**

ISRM

ABOUT

THE INSTITUTE OF STRATEGIC RISK MANAGEMENT

The Institute of Strategic Risk Management (ISRM) is a leading global centre for the promotion and sharing of best-practice strategic risk and crisis management capabilities and thought leadership amongst practitioners, academics and policy makers. Across the Institute's global chapter network, our Members and Fellows help progress and promote the underlying understanding and capabilities associated with strategic risk and crisis management, alongside developing their own personal and professional networks.

The ISRM provides best-practice training, hosts leading events across its global and local networks, and provides strategic advice to support organisations' management of complex risks.

www.theisrm.org

info@theisrm.org