



DCS Data Residency Assessment

Sample Executive Report for Sample Municipality

Sample report only

This document uses fictional tenant data with real Microsoft 365, Azure, Google Workspace, Google Cloud, and AI service categories. It demonstrates the report style, evidence model, charts, flags, and roadmap DCS can provide after a real read-only assessment.

Your data under **your** control.

Methodology and Evidence Boundary

The DCS assessment is metadata-only by default. It does not collect mailbox, file, Drive, SharePoint, Teams, or prompt content in the MVP assessment profile. Findings are traced to collected evidence records and assigned a confidence class.

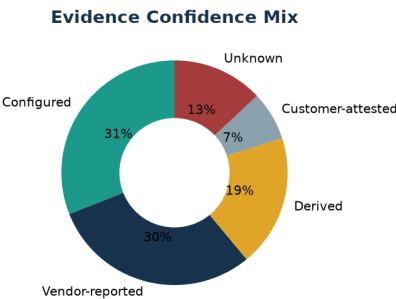
Evidence class	Meaning	Example source
Configured	Customer-controlled setting or policy read directly.	Graph user preferredDataLocation; bucket location
Vendor-reported	Microsoft or Google reports a current or committed geography.	M365 Data Location Card; Google Data Regions
Derived	Likely location inferred from related metadata.	Site owner, group mailbox, OU inheritance
Customer-attested	Customer-provided contracts, screenshots, exports, or questionnaires.	Admin screenshots; contract extracts
Unknown	No reliable evidence found or dashboard-only evidence needs follow-up.	AI path; support/cache path

Important limitation

The assessment reports configured, vendor-reported, derived, customer-attested, and unknown evidence. It does not claim to prove every physical replica, cache, support workflow, transient processing path, or internal vendor dependency.

Executive Findings

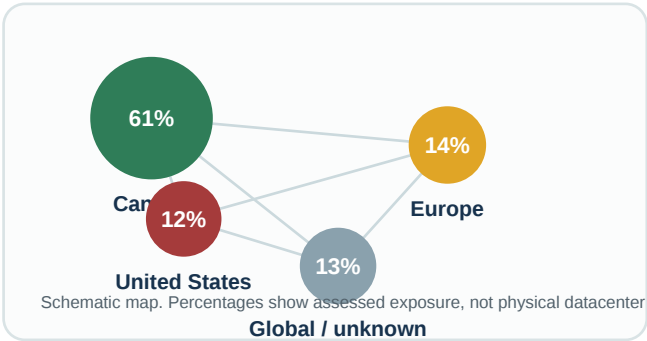
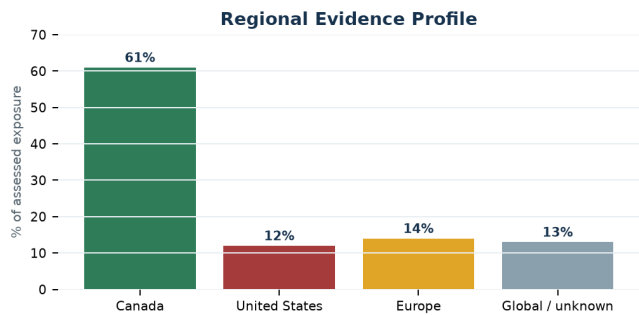
Workloads assessed	High-risk flags	Local / acceptable coverage	Unknown exposure
14	4	61%	13%



Interpretation

- The highest risk is not basic mailbox residency; it is control around sensitive collaboration sites, standing administrator access, third-party grants, and AI exposure.
- The tenant has useful vendor-reported and configured evidence, but 32% of the assessment relies on derived or unknown signals that require follow-up.
- A DCS pilot should start with sensitive records repositories and private AI workflows, not a broad rip-and-replace migration.

Residency and Control Heat Map



Area	Residency	Control	AI exposure	DCS priority
Exchange Online mailboxes	Moderate	Moderate	Moderate	Lower
SharePoint council and HR sites	Weak	Weak	Moderate	High
OneDrive for Business	Moderate	Moderate	Moderate	Lower
Teams and Microsoft 365 Groups	Weak	Weak	Moderate	Watch
Privileged admin roles	Weak	Weak	Moderate	High
Enterprise apps and OAuth grants	Weak	Weak	Moderate	High
Copilot for Microsoft 365	Weak	Weak	Weak	High
Gmail	Moderate	Weak	Moderate	Watch
Drive shared drives	Weak	Weak	Moderate	Watch
Google Groups	Moderate	Weak	Moderate	Lower

Exception Register and DCS Roadmap

Severity	Finding	Affected scope	Recommendation
High	SharePoint sensitive sites have unknown or mixed residency evidence.	Council, HR, legal sites	Run site-level evidence capture, then pilot DCS-controlled repository for council and HR records.
High	Standing privileged accounts weaken customer control.	Global admins, app admins	Introduce privileged access workflow and quarterly role review.
High	AI services are enabled before prompt and records governance are mapped.	119 enabled or licensed users	Route sensitive AI use cases through DCS private AI gateway first.
Medium	Google Workspace policy coverage is partial across OUs.	Drive, Gmail, Groups	Normalize OU policy inheritance and remediate uncovered users.
Medium	Google Cloud data assets include US and multi-region datasets.	Storage, BigQuery	Classify affected assets and move sensitive buckets/datasets to Canada where feasible.
Medium	Third-party apps hold broad file and directory grants.	12 high-risk apps	Review app consent, owners, data access, and business justification.

30 days	60 days	90 days
Confirm evidence gaps, reduce standing admin exposure, and freeze high-risk app consent.	Pilot DCS-controlled sensitive repository and private AI gateway for selected workflows.	Formalize coexistence roadmap, migration criteria, and quarterly evidence refresh.