UK Government Cloud Strategy & GGCL Adaptation – Context and Key Policies

Overview: The United Kingdom was an early adopter of cloud in government, launching a **"Cloud First"** policy back in 2013 – a full five years before Canada introduced a similar cloud-first approach[1] [2]. Today, roughly **60% of UK government IT systems run on cloud services** (as of 2023)[3], reflecting substantial progress in digital transformation. The UK's strategy emphasises **using public cloud by default**, leveraging commercial cloud platforms (like AWS, Microsoft Azure, Google Cloud) hosted in UK data centres, while **maintaining robust security and compliance** via National Cyber Security Centre (NCSC) guidelines and UK-specific regulations. This approach parallels Canada's GGCL in promoting cloud adoption and strong security, but with some differences in execution: **whereas Canada places strict data residency requirements on sensitive data (Protected B/C must stay in-country)[4] and is exploring sovereign cloud options, the UK has largely embraced global cloud providers under a framework of UK sovereignty safeguards**. For example, UK policy permits storing even sensitive "OFFICIAL" data in public clouds, provided vendors adhere to UK security principles and the data remains under UK/European jurisdictions[5] [6]. Only the most sensitive classified information (SECRET and above) is generally kept off public clouds (similar to how Canada keeps classified info off commercial cloud)[7]. In sum, **both the UK and Canada treat cloud as the new normal for government IT**, but the UK relies more on **central policy and market frameworks** (like the G-Cloud procurement marketplace and NCSC's 14 Cloud Security Principles) to manage risks, rather than imposing strict localization or building

[1] https://www.gov.uk/guidance/government-cloud-first-policy

[2] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/

[3] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/

[4] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/_layouts/15/Doc.aspx?sourcedoc=%7B90A2B40F-7842-4C2F-A0A2-318B5CFA566F%7D&file=From%20Concept%20to%20Care%20Health%20Te%202.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[5] https://www.gov.uk/guidance/government-cloud-first-policy

[6] https://www.gov.uk/guidance/government-cloud-first-policy

[7] https://www.gov.uk/guidance/government-cloud-first-policy

sovereign cloud platforms. Below, we detail the UK's cloud policies, compliance regime, adoption status, and compare where relevant with Canadian practices.

UK Government Cloud Policies and Strategy Evolution

"Cloud First" Policy (2013, updated 2023): The UK government formally adopted a Cloud First policy in 2013, mandating that central government departments **must consider cloud solutions before any others** when procuring or building IT services[8]. This was part of the broader G-Cloud programme launched in 2011, which aimed for 50% of new government IT spend to be cloud-based by 2015[9]. Cloud First was reaffirmed and expanded in a June 2023 update by the Central Digital and Data Office (CDDO) and Government Digital Service (GDS)[10] [11]. The policy now makes it **"Public Cloud by default"**: public sector organisations should adopt **public cloud services (including SaaS) as a first choice**, and only use private cloud or on-premises solutions if they can show a clear business case (e.g. cost or critical requirements that public cloud cannot meet)[12] [13]. This rule is mandatory for central government and "strongly recommended" for the wider public sector (local authorities, NHS, etc.)[14]. The core objective is similar to Canada's – *spend less time managing servers, more time improving services*[15] [16]. Notably, the UK policy explicitly says departments *should default to* ***public*** *cloud* (community or private cloud being acceptable only in specific cases)[17]. By contrast, Canada's 2018 cloud adoption strategy allowed both public and private clouds for Protected B data, but practically many Canadian departments also chose major public clouds (with data residency in Canada) for unclassified and Protected B systems.

One Government Cloud Strategy & Principles: In practice, Cloud First in the UK is implemented through centrally issued guidance and a set of **"Government Cloud Principles"**

[8] https://www.gov.uk/guidance/government-cloud-first-policy

[9] https://en.wikipedia.org/wiki/UK_Government_G-Cloud

[10] https://www.gov.uk/guidance/government-cloud-first-policy

[11] https://www.gov.uk/guidance/government-cloud-first-policy

[12] https://www.gov.uk/guidance/government-cloud-first-policy

[13] https://www.gov.uk/guidance/government-cloud-first-policy

[14] https://www.gov.uk/guidance/government-cloud-first-policy

[15] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/

[16] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/

[17] https://www.gov.uk/guidance/government-cloud-first-policy

that agencies must follow[18]. In June 2023, alongside the policy update, CDDO published **9 Cloud Principles** that supplement Cloud First with best practices on architecture, vendor management, and security[19] [20]. Key points include:

- **Use services, not servers:** Prioritise higher-level cloud services (PaaS, SaaS) over raw VMs, to maximise benefits like resilience and managed security[21]. Modernise legacy systems during cloud migration instead of a simple lift-and-shift[22].
- **Public cloud or SaaS first:** For most needs, use public cloud or SaaS. If data sensitivity or other constraints prevent that, use private cloud on an **infrastructure-as-code** basis with cloud-like characteristics[23]. On-prem hosting should be last resort; and if used, it should be via **Crown Hosting** (more on that below) to ensure efficiency[24].
- **Multi-vendor and avoid lock-in:** Don't rely on a single cloud provider for everything. Departments are urged to **spread risk across multiple vendors** and actively manage the risk of vendor lock-in[25] [26]. They should scrutinise incumbent suppliers and consider alternate vendors for new services[27] [28]. *(Indeed, a 2024 Cabinet Office review noted that heavy concentration with a few big cloud vendors was limiting government's bargaining power*[29] [30]*, so Principle 9 pushes agencies to rebalance this.)*
- **Preference for commodity frameworks:** The policy stresses using existing government procurement frameworks and collective agreements (via Crown

[18] https://www.gov.uk/guidance/government-cloud-first-policy

[19] https://www.gov.uk/guidance/government-cloud-first-policy

[20] https://www.gov.uk/guidance/government-cloud-first-policy

[21] https://www.gov.uk/guidance/government-cloud-first-policy

[22] https://www.gov.uk/guidance/government-cloud-first-policy

[23] https://www.gov.uk/guidance/government-cloud-first-policy

[24] https://www.gov.uk/guidance/government-cloud-first-policy

[25] https://www.gov.uk/guidance/government-cloud-first-policy

[26] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

[27] https://www.gov.uk/guidance/government-cloud-first-policy

[28] https://www.gov.uk/guidance/government-cloud-first-policy

[29] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

[30] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

Commercial Service) to get best value[31] [32]. This includes leveraging "one-government" volume deals and memoranda of understanding (MoUs) with major cloud providers, similar to how Canada uses Shared Services Canada for bulk procurement.

- **Consider overseas cloud with due diligence:** Uniquely, one principle acknowledges that some cloud services might be hosted globally (outside the UK). It instructs teams to **"perform due diligence" using ICO (Information Commissioner's Office) guidance and NCSC guidance** before using any overseas-based service[33]. In practice, this means assessing legal risks (like CLOUD Act exposure) and ensuring GDPR/UK Data Protection Act compliance for any data leaving UK jurisdiction. *This is roughly analogous to Canada's risk assessments for using U.S. clouds for Protected A data.* The UK allows use of global cloud offerings if departments are satisfied on data protection grounds; for example, some UK agencies use worldwide SaaS like ServiceNow or Salesforce, but typically with contractual clauses and encryption to mitigate risk. (See **Data Sovereignty** below for more on how UK addresses this, which differs from Canada's stricter residency mandate[34].)
- **Use Crown Hosting for any on-prem needs:** The policy explicitly directs that if a department truly cannot use cloud and must host onsite, they should use **Crown Hosting Data Centres** rather than maintain their own server rooms[35]. Crown Hosting is a joint venture between the Cabinet Office and Ark Data Centres, set up in 2015 to provide energy-efficient, cost-effective co-location facilities for legacy government systems. Essentially, it's a shared government data centre service that offers quick contracting and is considered the "least bad" option when not using cloud[36]. (This is somewhat akin to Shared Services Canada's role in providing data centre space to federal departments; it acknowledges that while cloud is preferred, a centrally managed on-prem solution is better than dozens of separate ones.)

[31] https://www.gov.uk/guidance/government-cloud-first-policy

[32] https://www.gov.uk/guidance/government-cloud-first-policy

[33] https://www.gov.uk/guidance/government-cloud-first-policy

[34] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/_layouts/15/Doc.aspx?sourcedoc=%7B90A2B40F-7842-4C2F-A0A2-318B5CFA566F%7D&file=From%20Concept%20to%20Care%20Health%20Te%202.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[35] https://www.gov.uk/guidance/government-cloud-first-policy

[36] https://www.gov.uk/guidance/government-cloud-first-policy

- **Secure by design & align with NCSC:** Cloud solutions must be built with security from the start, following **NCSC's Cloud Security Principles** and general best practices (more in next section)[37]. Automation (Infrastructure as Code, CI/CD) and DevSecOps are encouraged to maintain consistent security patching and configurations[38].

Alongside these principles, the UK published a **"Cloud Guide for the Public Sector"** (latest update Nov 2023) that consolidates all cloud guidance, including technical advice and case studies[39] [40]. The Cloud Guide serves a similar purpose to Canada's Cloud Adoption Playbook: it helps agencies decide what to move and how, covering topics like selecting cloud service models, managing costs, and meeting compliance standards[41] [42].

Adoption Progress: After 10+ years of G-Cloud and Cloud First, the UK public sector's cloud uptake is relatively high. As noted, ~60% of systems are now cloud-based (this includes many "OFFICIAL" workloads such as websites, internal collaboration tools, case management systems, etc.)[43]. The **State of Digital Government Review (2023)** even found that this cloud adoption rate is "a good percentage compared to big private companies and other countries"[44]. By comparison, Canada does not publish an exact percentage, but anecdotal evidence suggests Canada's cloud adoption (especially for Protected B data) has lagged the UK slightly – due in part to stricter data residency rules, which only recently began to loosen for certain use cases. The UK's head start and aggressive policy have led to notable successes, e.g. the Ministry of Justice built a cloud-based data analytics platform serving 500+ staff and retired many legacy systems[45]. At the same time, challenges familiar to any government remain: departments grapple with migrating complex legacy applications, addressing cloud skill gaps, and ensuring security across hybrid environments[46]. The UK government has acknowledged these hurdles and, much like Canada's efforts with the Digital Academy, has programs to **train civil servants in cloud**

[37] https://www.gov.uk/guidance/government-cloud-first-policy

[38] https://www.gov.uk/guidance/government-cloud-first-policy

[39] https://www.gov.uk/guidance/government-cloud-first-policy

[40] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/

[41] https://www.gov.uk/guidance/government-cloud-first-policy

[42] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

[43] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/

[44] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/

[45] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/

[46] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/

skills (for example, GDS's "Get Cloud Certified" bootcamps with AWS and Microsoft)[47] and to **foster cross-government cloud communities** for sharing best practices[48].

*(**Comparison:** The UK's timeline shows an earlier and more centralized push to cloud. Canada's equivalent timeline would start later – e.g., a formal Cloud Adoption Strategy in 2018, the "Cloud First" direction in 2019, and refreshed in 2021 – and includes steps like establishing SSC cloud brokering and a 2022 Cloud Guardrails policy. Both countries eventually align on cloud-first norms by mid-2020s, but the UK had already achieved broad adoption by the time Canada was scaling up. Notably, the UKCloud episode in 2022 underscores that the UK government tried nurturing a sovereign cloud provider, but ultimately most workload gravitated to AWS, Azure, etc., whereas Canada in 2023–25 is still exploring sovereign cloud possibilities through pilots and policy papers[49] [50].)*

Security, Compliance and Data Sovereignty in UK Government Cloud

Security Framework – NCSC Cloud Principles: The UK does not have an exact counterpart to Canada's "Protected B cloud" accreditation or FedRAMP; instead, it uses guidance and standards set by the National Cyber Security Centre (NCSC). Key among these are the **14 Cloud Security Principles** (published 2016, updated thereafter), which articulate best-practice goals for cloud providers. These principles cover areas very similar to Canada's ITSG-33 controls and cloud security profile, such as: **data in transit protection, asset resilience (including lawful interception and location concerns), separation between tenants, secure governance and operations, personnel vetting, secure development, supply chain security, identity and access control, auditing, and secure data deletion**, etc.[51] [52]. The UK government expects agencies to **assess prospective cloud services against these 14 principles** to ensure the provider meets an adequate standard for the sensitivity of data

[47] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/

[48] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/

[49] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/_layouts/15/Doc.aspx?sourcedoc=%7B90A2B40F-7842-4C2F-A0A2-318B5CFA566F%7D&file=From%20Concept%20to%20Care%20Health%20Te%202.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[50] https://www.datacenterdynamics.com/en/news/ukcloud-enters-liquidation/

[51] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

[52] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

in question[53] [54]. Many cloud suppliers publish "NCSC Principles Compliance" statements to help customers judge their security (for example, Microsoft and Amazon have publicly documented how they meet each principle)[55] [56]. This framework is broadly analogous to Canada's use of the CIO Cloud Control Profile and third-party attestations (e.g. Canadian departments also examine if a cloud service has ISO 27001, SOC 2, etc., and map it to their security requirements). In both countries, **the onus is on departments to choose a vetted, secure service and then configure/use it securely**. The UK's Cloud Guide explicitly references the **"shared responsibility model"** – meaning agencies must still implement sound configurations and controls on top of what the vendor provides[57]. For example, an agency should enforce strong IAM, encrypt sensitive data at rest (the big cloud platforms offer easy keys management, including customer-managed keys if needed), and monitor their cloud workloads for vulnerabilities or anomalies[58] [59]. NCSC provides detailed guidance on these topics (secure cloud configuration, auditing, incident response in cloud, etc.)[60] [61].

Data Classification and Cloud Eligibility: The UK's **Government Security Classifications (GSC)** scheme (introduced 2014) plays a major role in determining if data can go to public cloud. Under GSC, the vast majority of government information is classified as **OFFICIAL** (which can include sensitive personal data, health records, routine security information, etc.), with only a small fraction marked SECRET or TOP SECRET (higher national security and defence material)[62]. Officially, **OFFICIAL information *can be stored in the public cloud*** as long as the cloud service meets the required security controls (usually aligned with NCSC principles and a **Cyber Essentials Plus** certification or ISO 27001 at minimum) and the department is satisfied regarding the provider's governance[63] [64]. Even data considered

[53] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

[54] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

[55] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

[56] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

[57] https://www.ncsc.gov.uk/collection/cloud

[58] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

[59] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

[60] https://www.ncsc.gov.uk/collection/cloud

[61] https://www.ncsc.gov.uk/collection/cloud

[62] https://www.gov.uk/guidance/government-cloud-first-policy

[63] https://www.gov.uk/guidance/government-cloud-first-policy

[64] https://www.gov.uk/guidance/government-cloud-first-policy

“OFFICIAL-SENSITIVE” (a handling caveat for particularly sensitive personal or policy data) is not automatically barred from public cloud – it just means that stronger access controls and encryption should be in place. This stance is notably more permissive than Canada’s approach, where data roughly equivalent to OFFICIAL-SENSITIVE (i.e. Protected B) is subject to a formal requirement to be hosted on **cloud infrastructure within Canada** or with approval by Treasury Board if outside[65]. The UK balances this by requiring case-by-case due diligence (see below on GDPR and legal considerations), but it does not categorically require OFFICIAL data to reside on UK soil – it’s strongly preferred, but not a hard mandate. For **SECRET and TOP SECRET** data, the UK very much like Canada keeps these off general public cloud. The Cloud First policy states services handling SECRET or above are *“unlikely to be suitable for Public Cloud”* and specialist advice should be sought[66]. In practice, such systems either remain on dedicated government networks or use tightly vetted community clouds. (E.g. the Ministry of Defence runs **MODCloud**, a set of private cloud environments at OFFICIAL-SENSITIVE and SECRET tiers, some of which use AWS/Azure but in dedicated UK sovereign regions.) Canada similarly does not allow classified info on public cloud – it uses separate networks or SSC-run facilities for Secret and Top Secret.

UK GDPR and Data Protection: As of 2021 (post-Brexit), the UK enforces its own version of GDPR (virtually identical to the EU GDPR) and the Data Protection Act 2018, overseen by the ICO. These laws impose strict rules on processing personal data, including when transferring it outside the UK. Consequently, **any cloud service used must comply with UK GDPR requirements** for safeguarding personal data. In practical terms:

- **Data Residency & Overseas Access:** The UK government does *not* have an absolute rule that all sensitive data must stay in the UK, but GDPR requires that personal data only be transferred to countries with adequate protection or under appropriate safeguards (like standard contractual clauses). The ICO has issued guidance on use of cloud and international transfers. The Cloud First policy Principle #5 explicitly tells teams to consult **ICO guidance and NCSC guidance before using a cloud service provided overseas**[67]. This implies performing a risk assessment of foreign jurisdiction risks (e.g. US CLOUD Act). In many cases, major providers mitigate this by hosting UK government data in UK or European regions and offering contractual commitments

[65] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/_layouts/15/Doc.aspx?sourcedoc=%7B90A2B40F-7842-4C2F-A0A2-318B5CFA566F%7D&file=From%20Concept%20to%20Care%20Health%20Te%202.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[66] https://www.gov.uk/guidance/government-cloud-first-policy

[67] https://www.gov.uk/guidance/government-cloud-first-policy

that no data will be moved without notice. Indeed, most UK departments choose cloud regions in the UK (London, Cardiff, etc.) or occasionally in EU (Dublin, Amsterdam) for resilience. Thus, by architecture, their data stays within jurisdictions deemed adequate under UK law. For example, Microsoft's Azure UK South/North regions and AWS's London region are widely used – keeping data on British soil and under UK law. The **NCSC's principle on Asset Protection** also advises customers to understand which country's laws their data could be subject to and use encryption and other measures accordingly[68] [69]. So while the UK hasn't legally mandated "data must remain in UK," the practical outcome is similar: public sector contracts almost always stipulate UK or EU data residency. (In contrast, the Canadian government **does** mandate Protected B data residency in Canada by policy[70], reflecting a more rigid stance born from sovereignty concerns.)

- **Privacy by Design:** Departments using cloud services must ensure compliance with privacy principles like data minimisation, purpose limitation, and individual rights. This includes configuring cloud services to limit data access and retention. For instance, if a UK department uses an analytics cloud service, it should pseudonymise personal identifiers where possible, and ensure it can fulfill subject access requests or deletion requests. Under GDPR, the department (not the cloud provider) remains the **data controller** accountable for proper handling of personal data. This is similar to Canada's approach under the Privacy Act and policies – the department must ensure a cloud provider meets all requirements (e.g. through contractual terms, which both countries include in cloud contracts).
- **Certification and Standards:** The UK doesn't run a government-exclusive cloud certification like FedRAMP/ISMAP, but many procurement frameworks (including G-Cloud) require that cloud suppliers have certain certifications, notably **ISO/IEC 27001** for information security, ISO/IEC 27018 for cloud privacy, and adherence to the NCSC 14 principles. The **Cyber Essentials Plus** scheme (a UK government-backed cybersecurity certification) is often mandated as a minimum for suppliers handling OFFICIAL data. Essentially, before a service is listed on the Digital Marketplace, suppliers must assert their compliance with these standards and answer detailed security questions (covering data location, incident history, etc.). Departments then

[68] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

[69] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

[70] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/_layouts/15/Doc.aspx?sourcedoc=%7B90A2B40F-7842-4C2F-A0A2-318B5CFA566F%7D&file=From%20Concept%20to%20Care%20Health%20Te%202.docx&action=default&mobileredirect=true&DefaultItemOpen=1

select a suitably certified service and perform their own privacy impact assessments. This lighter-weight approach contrasts with Canada's more centralised assessment: for example, Canada's Shared Services does some cloud security assessments and TB policy requires threat risk assessments for each system. But in effect both systems achieve scrutiny – the UK pushes most of it to the procurement pre-checks and departments' due diligence, guided by NCSC/ICO.

Crown Hosting Data Centres: One element unique to the UK approach is the aforementioned **Crown Hosting**. Recognising that not everything can move to public cloud immediately (some legacy systems or highly sensitive databases might not be ready), the government in 2015 created Crown Hosting as a halfway house. It's a public-private JV that offers co-location space in secure, energy-efficient data centres for government systems, with on-demand contracts. Cloud First principle #4 endorses Crown Hosting as the preferred option if on-prem is needed[71]. Many departments migrated old servers from in-house data rooms to Crown Hosting facilities as an interim step to later move into cloud. This has saved costs (typical savings cited are 20-40% on hosting) and improved resilience by shutting small server rooms. For example, DWP and HMRC moved hundreds of servers to Crown Hosting while they refactor applications for cloud. Canada doesn't have an exact equivalent JV, though Shared Services Canada's enterprise data centres serve a similar consolidation role. The difference is the UK separates that from core government and lets departments contract it quickly, whereas Canada's SSC directly provides those hosting services.

Procurement Mechanisms – G-Cloud and Multi-Cloud: Cloud First in the UK is supported by agile procurement. The **G-Cloud framework** (now on iteration 14) is central to this. Rather than each department running lengthy tenders for cloud services, G-Cloud is a pre-competed framework where providers list their services and pricing on the **Digital Marketplace** (now Public Procurement Gateway)[72]. Public bodies can simply pick from this catalogue, which greatly reduces procurement friction. As of 2024, **over 5,000 suppliers** are available via G-Cloud, 91% of which are SMEs[73]. This includes all the major hyperscalers (AWS, Azure, Google – all joined by 2018)[74], a range of UK-based firms, and niche SaaS vendors. G-Cloud spend has soared year on year: from £18M in 2012/13 to nearly **£2.9B in 2024/25**[75]. Cumulatively, **£14.7B** of cloud services were procured through G-Cloud in the

[71] https://www.gov.uk/guidance/government-cloud-first-policy

[72] https://en.wikipedia.org/wiki/UK_Government_G-Cloud

[73] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

[74] https://en.wikipedia.org/wiki/UK_Government_G-Cloud

[75] https://en.wikipedia.org/wiki/UK_Government_G-Cloud

last five years (approx. FY2019–2023)[76]. This open market approach was intended to prevent lock-in to a handful of legacy integrators and to **give SME providers a level playing field** – indeed ~37% of spend has gone to SMEs[77], which is higher than traditional IT contracts. Canada's counterpart is the Shared Services Canada cloud framework and GC Digital Marketplace, which list authorised cloud vendors for departments, though Canada's vendor pool is smaller; the UK's inclusion of thousands of SMEs was a distinctive pro-competition move.

The **Crown Commercial Service (CCS)** continuously updates these frameworks (G-Cloud 14 launched in Oct 2024)[78]. They've also added specialist "Lots" for cloud support services. For example, a **£1B Cloud Migration & Advisory framework** was awarded in Dec 2024 to help departments with moving complex systems and avoiding getting stuck with one vendor[79] [80]. This ties into the anti–lock-in focus: 42 companies (big consultancies and integrators) are pre-approved to assist agencies in planning multi-cloud architectures, migrating email, ERPs, etc., including ensuring exit strategies and interoperability[81]. The UK government is aware that once in the cloud, it must not become complacent with cost or competition. A **CDDO document in 2024** pointed out that departments' cloud adoption practices had led to "*risk concentration and vendor lock-in that inhibit negotiation power*"[82]. In response, Cloud First policy reminds orgs to "scrutinize their selection of vendors" and leverage collective buying power (the UK has central MoUs with AWS, Microsoft, Google that yield discounts for government volume)[83]. Similarly, Canada in 2022 negotiated a Government of Canada Azure Agreement to get better pricing. Both countries seek to balance **the efficiency of using a few big platforms with the prudence of not being beholden to them**. The UK's multi-cloud principle and diversified framework are practical tools towards that; Canada's approach is evolving (e.g. exploring interchangeability via cloud-agnostic container platforms, and encouraging departments to have "exit plans" in their project approvals).

Recent Developments and International Alignment: In 2023–2024, the UK has doubled down on cloud as an enabler for broader digital government goals. The **2025 Blueprint for**

[76] https://en.wikipedia.org/wiki/UK_Government_G-Cloud

[77] https://en.wikipedia.org/wiki/UK_Government_G-Cloud

[78] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

[79] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

[80] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

[81] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

[82] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

[83] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

Modern Digital Government explicitly calls cloud a "utility" that allows faster innovation across departments[84]. The UK is also aligning its cloud and digital strategies with international partners. For instance, the UK and Canada have an ongoing cooperation on cloud and AI compute (they signed a memorandum in 2023 to collaborate on best practices for sovereign cloud and AI infrastructure). However, the concept of "sovereign cloud" is less central in the UK narrative than in Canada or EU countries like France. The UK takes a pragmatic view: it uses **global cloud tech within a UK governance wrapper**. As noted, it lost its main local cloud champion (UKCloud), but found that hyperscalers could meet most sovereignty needs by offering UK-hosted services and transparency. The UK's **NCSC is deeply involved with these providers** – e.g., NCSC performs architectural reviews and shares threat intel, ensuring that the public cloud offerings for UK gov meet national security expectations. So rather than government building its own cloud, it works closely with industry to make commercial clouds "trusted" for UK use. Canada is trending similarly (using Azure/AWS in Canada for Protected B, while pursuing projects like a potential secure cloud for defence), though Canada voices "digital sovereignty" concerns more strongly in policy.

Both the UK and Canada adhere to **international standards** in cloud security and procurement. The UK was part of the EU for many years, so UK cloud implementations complied with EU regs like GDPR (still do under UK law) and follow ISO standards; the Government Security Policy aligns with ISO 27001 controls. Canada likewise maps its ITSG-33 controls to NIST/ISO benchmarks, and both nations engage in the **Five Eyes** security partnership (with US, Aus, NZ) – meaning their approaches to cloud risk (especially regarding foreign interference) are shared. For example, the UK's principle of checking foreign legal risks and Canada's insistence on Canadian residency both stem from similar concerns about extraterritorial access to data. In practice, a UK department and a Canadian department might end up using the **same cloud service (say, Microsoft 365)** configured to their respective rules: the UK tenant might allow some services running out of EU datacenters, whereas the Canadian tenant would strictly pin to Canadian regions[85] [86]. Both will implement strong encryption and key management, and both will rely on contractual

[84] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/

[85] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/_layouts/15/Doc.aspx?sourcedoc=%7B90A2B40F-7842-4C2F-A0A2-318B5CFA566F%7D&file=From%20Concept%20to%20Care%20Health%20Te%202.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[86] https://www.gov.uk/guidance/government-cloud-first-policy

protections (Canada requires cloud contracts to include breach notification and foreign request notification clauses, which the UK likely also inserts case-by-case).

Summing Up Compliance: For a UK public body to host data (especially personal or mission-critical data) in the cloud, it must:

- Choose a provider that is **ISMAP-like vetted** – in UK's case via G-Cloud supplier accreditation – meeting standards akin to ISO 27001 and the NCSC principles.
- Ensure the service is configured to meet **NCSC cloud security guidance**, and that the department upholds its share of security (e.g. using SSO, monitoring logs, restricting admin access). NCSC often works with departments on architecture reviews for high-risk deployments.
- Conduct a **Data Protection Impact Assessment** if personal data is involved, showing compliance with UK GDPR (similar to Canada's PIA under the Privacy Act).
- If data will leave the UK, ensure there are **adequacy or contractual safeguards** (post-Brexit UK treats the EU as adequate until at least 2025, and has new agreements like the UK-US Data Access Agreement and exploring the "Data Bridge" with the US – these developments aim to smooth lawful cloud usage across borders).
- Obtain internal security accreditation (some departments still run a process to issue an Authority to Operate for new cloud systems, akin to Canada's ATO under ITSG-33). In UK, formal accreditation for OFFICIAL systems was somewhat deprecated with the 2014 reforms, but in practice many agencies do internal risk sign-offs.

From a **governance and oversight** perspective, the UK's Cloud First policy is enforced through mechanisms like:

- **Spend Controls:** GDS reviews large tech spend proposals (above certain thresholds) – any attempt to host a system on-prem or not use cloud will be questioned. Departments have to justify deviating from Cloud First, in line with the policy that they should document why if not using public cloud[87].
- **Portfolio Dashboards:** The Central Digital & Data Office tracks cloud adoption and reports progress (the 60% figure came from such a review)[88]. This creates peer pressure among departments and informs central support (like identifying those struggling with legacy migrations).
- **Audits and Value-for-Money checks:** National Audit Office and others have looked at whether Cloud First is delivering savings. Early on, some NAO reports found that while G-Cloud increased SME procurement, some agencies still weren't fully optimising cost in cloud. This feedback has led to the 2024 focus on **FinOps** (cloud financial management) and not over-provisioning resources. The UK is now investing

[87] https://www.gov.uk/guidance/government-cloud-first-policy

[88] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/

in training civil servants on cloud cost optimisation, something Canada's GGCL also emphasizes (e.g. avoiding paying for idle capacity, managing egress fees, etc. – both learned those lessons).

Key UK Policies & Initiatives (Summary Table):

Policy / Framework	Description & Requirements	Introduced / Latest
Cloud First Policy (Cabinet Office, CDDO)	Mandates public cloud be the default for new IT procurements. Central govt must use cloud unless not value-for-money. Reinforced in 2023 with 9 Cloud Principles (public cloud first, use SaaS/PaaS, no on-prem except Crown Hosting, multi-vendor, etc.)[89] [90].	2013 (updated 2023)[91] [92]
Government Cloud Principles (CDDO/GDS)	Nine detailed principles to guide cloud adoption (e.g. "Services, not servers"; "Public or SaaS first"; "Consider overseas cloud with due diligence"; "Use Crown Hosting if on-prem"; "Secure by design with NCSC guidance"; "Avoid lock-in")[93] [94]. Ensures consistency across departments.	2023 (current version)
G-Cloud Procurement Framework (CCS)	A series of framework agreements allowing quick procurement of cloud services via the **Digital Marketplace**. Thousands of pre-vetted services (IaaS, PaaS, SaaS, support) available. Emphasises SME inclusion and transparent pricing. G-Cloud 14 (2024) adds £7.5B	Launched 2012; refreshes ~annually (G-Cloud 14 in 2024)[98] [99]

[89] https://www.gov.uk/guidance/government-cloud-first-policy

[90] https://www.gov.uk/guidance/government-cloud-first-policy

[91] https://www.gov.uk/guidance/government-cloud-first-policy

[92] https://www.gov.uk/guidance/government-cloud-first-policy

[93] https://www.gov.uk/guidance/government-cloud-first-policy

[94] https://www.gov.uk/guidance/government-cloud-first-policy

[98] https://en.wikipedia.org/wiki/UK_Government_G-Cloud

[99] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

	capacity[95] [96]. Lot 4 focuses on migration services to handle legacy workloads[97].	
Crown Hosting Data Centres (CO & Ark)	Joint venture providing co-location facilities for government legacy systems. Offers high-efficiency, PSN-connected data centres for OFFICIAL and SECRET workloads. Cloud First directs any on-premises hosting to use Crown Hosting (for cost-effectiveness and easier exit)[100]. Many agencies use it as a stepping stone while refactoring apps for cloud.	Established 2015 (ongoing)[101]
NCSC Cloud Security Guidance (NCSC)	Comprehensive guidance collection for secure cloud adoption[102]. Includes the **14 Cloud Security Principles** for providers (data protection, separation, governance, etc.)[103] [104], plus advice on selecting cloud services, configuration (shared responsibility), monitoring, and incident response in cloud. Public sector solutions should align with these principles for adequate security.	Published 2016; updated continuously[105] [106]
Technology Code of Practice (CDDO)	Broader IT management best practices for UK gov, which reinforce Cloud First. Principle 11 of the code: "Make things cloud agnostic" – build services that are portable and avoid proprietary lock-in; use internet-ready tech. Also mandates considering SaaS and using existing platforms (e.g. GOV.UK PaaS was an option, now deprecated) in line with Cloud First.	Initial 2016; updated 2021

[95] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

[96] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

[97] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

[100] https://www.gov.uk/guidance/government-cloud-first-policy

[101] https://www.gov.uk/guidance/government-cloud-first-policy

[102] https://www.ncsc.gov.uk/collection/cloud

[103] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

[104] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

[105] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

[106] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

Data Protection Act & UK GDPR (ICO)	Legal regime for personal data. Requires departments to ensure any cloud provider processing personal data implements GDPR-level protections. If using processors outside UK, need certain safeguards (Standard Contractual Clauses, adequacy decisions – note: EU is adequate and new UK-US “Data Bridge” is anticipated). Departments do Data Protection Impact Assessments for new cloud systems handling citizens’ data. ICO can audit or penalize non-compliance.	GDPR effective 2018 (retained post-Brexit); DPA 2018
Government Security Policy (Cabinet Office)	Requires departments to apply the Government Security Classifications and protect info accordingly. In cloud context: OFFICIAL information must be protected against accidental disclosure (follow NCSC principles, provider must have suitable security). Secret/TOP SECRET require HMG-approved dedicated systems (e.g. private cloud on secure networks). Policy also stresses supply chain security – cloud suppliers should be vetted for hostile influence (NCSC evaluates major cloud providers for this).	Current policy from 2014 (GSC); refreshes in Security Policy Framework updates

(This table highlights how the UK’s cloud governance is spread across multiple documents and bodies – GDS/CDDO for digital strategy, CCS for procurement, NCSC for security, ICO for privacy, Cabinet Office for overall policy. By contrast, Canada’s GGCL and related cloud guidance consolidate many of these concerns under Treasury Board policies and SSC frameworks, but ultimately cover similar ground.)

Data Sovereignty and International Issues: One of the most interesting facets of the UK approach is its nuanced take on data sovereignty. The UK is mindful of risks like extraterritorial action (e.g. US subpoenas) but tackles it through **guidance and contracts** rather than outright bans. For instance, NCSC’s **Principle 2: Asset Protection & Resilience** explicitly includes considering *which country your data will be stored in and governed by*, and advises technologies like encryption to mitigate foreign access risks[107]. The **Principle 5** listed in Cloud First says essentially: teams can use non-UK cloud, but must follow ICO and NCSC advice, meaning they should weigh **legal protections** (is the provider based in a country with a UK data adequacy agreement? does the contract ensure compliance with UK law? will the provider contest undue foreign government demands?). In practice, the big cloud providers have set up separate UK companies for public sector (e.g. AWS’s UK entity, Azure operated by Microsoft in UK) and often offer contractual assurances around transfer. Moreover, since the UK is part of the **Five Eyes** intelligence alliance with the US, there is

[107] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

arguably a bit more mutual trust at government level when UK data is hosted by an American company, compared to EU countries' stance – the UK has even signed a CLOUD Act agreement with the US to streamline lawful data access requests, which somewhat clarifies the process.

All that said, the **strong preference is to keep data in UK regions**. The Cloud Guide 2023 notes that for **Official-Sensitive data, departments are recommended to use UK-sovereign cloud options (UK data centres, UK support)** unless there's a compelling reason otherwise[108] [109]. And indeed, *almost all major government systems are hosted in UK or EU data centres of the big providers*, meaning day-to-day operations don't ship British citizens' data overseas. The UK government thus feels it has achieved a level of data sovereignty without needing a fully nationalised cloud. This contrasts with Canada, which still articulates data sovereignty as a concern – for example, Canada's directive outright says all sensitive data must reside in Canada, and it invests in projects to guarantee that (such as exploring a government-owned Secret-level cloud or edge for defence)[110]. The UK's approach is arguably more flexible and market-driven, trusting that robust encryption, legal agreements, and diverse cloud choices can manage sovereignty risks. In 2023, the UK even **urged departments to use "higher-level cloud services" and not cling to in-house systems out of misplaced sovereignty fears**, releasing nine new cloud guidance principles (as discussed) to dispel myths and encourage more public cloud use for efficiency[111].

In summary, the **UK's cloud governance (its "GGCL") is characterised by**:

- **Policy commitment from the top** – Cloud First has been Cabinet Office policy for 10+ years, strongly backed by central government. This sustained mandate has driven cultural change in procurement.
- **Centrally provided enablers** – from G-Cloud procurement frameworks to Crown Hosting and common MoUs, making it easier and cheaper for agencies to go cloud than to do status quo.
- **Standards and guidance over regulation** – The UK sets out clear security/privacy expectations via NCSC and ICO guidance, but gives departments discretion on how to

[108] https://www.gov.uk/guidance/government-cloud-first-policy

[109] https://www.gov.uk/guidance/government-cloud-first-policy

[110] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/_layouts/15/Doc.aspx?sourcedoc=%7B90A2B40F-7842-4C2F-A0A2-318B5CFA566F%7D&file=From%20Concept%20to%20Care%20Health%20Te%202.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[111] https://www.theregister.com/2024/12/03/uk_gov_cloud_services/

meet them (with central review). It has not needed to pass specific “cloud laws” because existing data protection law and security policy were seen as sufficient. (Similarly, Canada leverages existing Privacy Act, etc., but Canada did issue a specific Cloud Adoption Strategy and Guardrails for departments.)

- **Emphasis on multicloud and competition** – The UK public sector consciously uses multiple providers (AWS, Azure, Google all have significant share in different departments, plus niche SaaS). This mitigates vendor lock-in and encourages innovation. Canada as of mid-2020s still has a heavier tilt to one or two vendors (a large portion of Protected B workloads went to Azure in early years via SSC, with AWS catching up; Google is less present in Canadian government so far). But Canada too recognises this risk and has started to encourage multi-cloud strategies.
- **Continuous evolution** – In 2025, the UK is already looking at the next stage: optimizing cloud usage (cost control, advanced services like AI and big data in the cloud) and ensuring the workforce is cloud-savvy[112]. The cloud conversation is shifting from “should we move to cloud?” to *“how do we best leverage cloud for digital innovation?”*. Canada is entering that phase a bit later, as it reaches a tipping point of cloud adoption.
- **International cooperation** – The UK works with allies (including Canada) on aligning cloud security standards and sharing best practices, as evidenced by joint statements and the UK-Canada cooperation on AI compute MOU. Both countries participate in global cloud security and procurement discussions (e.g. through the Digital Nations forum and technology partnerships). In essence, they face common challenges (jurisdictional issues with foreign providers, balancing innovation vs sovereignty, tackling legacy IT), and increasingly address them in a coordinated way.

Ultimately, the **UK’s cloud-centric approach** has enabled rapid digital government improvements – many public services in Britain run on scalable, modern cloud platforms that handled COVID-19 surges and online demand far better than legacy systems. The policy frameworks ensure this is done securely and cost-effectively, without (in the government’s view) compromising national control over data. The Canadian GGCL reader can take away that while contexts differ, the core principles – **cloud by default, secure and compliant by design, use of common platforms, ongoing optimisation** – are very much shared between the UK and Canada. The UK experience underscores the importance of strong central leadership and enabling functions (like G-Cloud) to make cloud adoption easier than the old ways, an insight Canada has reflected in its own recent cloud procurement and governance refinements.

[112] https://technology.blog.gov.uk/2025/02/18/governments-cloud-first-policy-is-12/