Demystifying Software as a Service

What is Software as a Service?

Software as a Service (SaaS) is a software distribution model where applications are purchased or hosted by a cloud service provider, and then made available for customers to use over the internet.[1] Examples include email services like Gmail and collaborative applications like Miro or Airtable. The Government of Canada implemented Microsoft 365, which is another example. If it's web-based, stores data, and requires an account (even a free one), it's likely SaaS.

Why are we talking about SaaS?

Public servants want to be agile in a rapidly changing technological environment, but we also need to avoid mistakes. **It's important to know the limits and the rules before signing up for SaaS**. Because SaaS is often ready to use as soon as you get your login and password, you might not realize that you first need authorization and approvals. All existing IT-related government policies also apply to SaaS.

What are the risks of not following protocol?

Before signing up for SaaS, you should advise and involve key IT colleagues. Not doing so involves certain risks, including:

- Poor assessments
- Flawed implementation
- Extra costs
- Potential business continuity and data security issues

Budgeting:

Departments must pay cloud subscription costs from parliamentary-approved operational funding

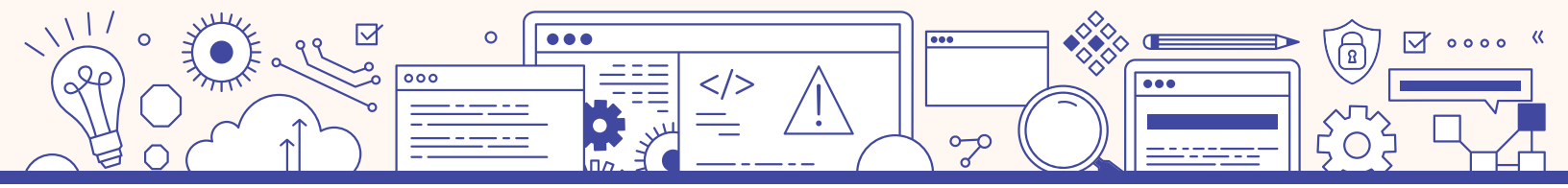
Government departments should only use time-limited, discretionary funding to implement and improve cloud activities, not to sustain subscription costs. Cloud subscription costs continue until a program or service migrates to another technology. There is a risk of disrupting business continuity if a department uses discretionary funding to pay for cloud subscriptions.

1 Canadian Centre for Cyber Security

Job aid: DDN2-J19

Canada School of Public Service | École de la fonction publique du Canada

Canada



Contract planning:

Contracts with cloud providers should reflect the entire life cycle of services needed

Business continuity can also be disrupted if departments create contracts of insufficient length and value to support a long-term relationship with the cloud provider.

Security:

The account or the data stored in SaaS could be compromised

What if the data is breached (and the organization may never know). Or someone uses the untracked SaaS data for purposes other than what was intended. The following issues need to be addressed before you sign up for SaaS:

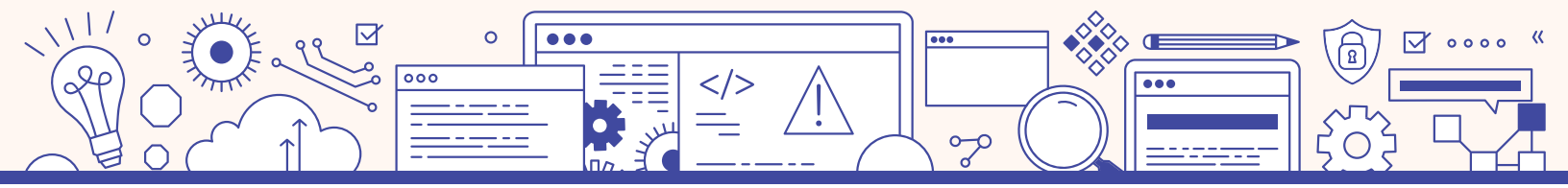
- What level of protection does your data require? Will the SaaS be used for personal information? If so, you need a statement of sensitivity (SoS).
- Who's accessing the data? Who's sharing it? What happens if there's a breach?
- Could bad actors or malicious employees steal government data? Will the government be able to view audit logs in the case of an insider threat?
- How will you ensure that infected files aren't brought back to your organization?

Departmental chief information officers (CIOs) apply the GC Cloud Tiered Assurance Model to the approval process to ensure security compliance.

Data:

All public servants have a responsibility to be good data stewards

Privacy. There is an approval and assessment process any time government data is placed in an online service, particularly if the data is protected. Your department may have different approval thresholds for different types of SaaS. For example, approval might be faster for read-only subscriptions than for requests for services that store government data. Consider what can happen when privacy is breached: RCMP's use of Clearview AI's facial recognition technology violated Privacy Act, investigation concludes.



Data accessibility. Organizational data must be accessible for searching, analytics or access to information and privacy (ATIP) requests. Specifically:

- How will you prevent data sprawl to ensure that your data is integrated into other systems and available to users in the Government of Canada?
- How will you manage access to the data given that there are separate accounts and credentials for every SaaS? What happens when the employee with the SaaS account leaves the organization, taking data access with them?
- Are you following data retention, deletion, archiving, backup and ATIP policies?
- What's your withdrawal plan? What happens to the data if you stop paying the subscription or if the company disappears?

Legal:

SaaS updates can unexpectedly contravene government policy

SaaS changes are sometimes made without the involvement or knowledge of clients. For example, a SaaS provider might switch from one cloud service provider to another or from one geographic location to another without consulting users. Such a strategy may be convenient, but it's also problematic. All users must exercise vigilance to ensure that SaaS updates don't contravene government policies related to privacy and legal issues, usability and accessibility, and data residency, among others.

Value:

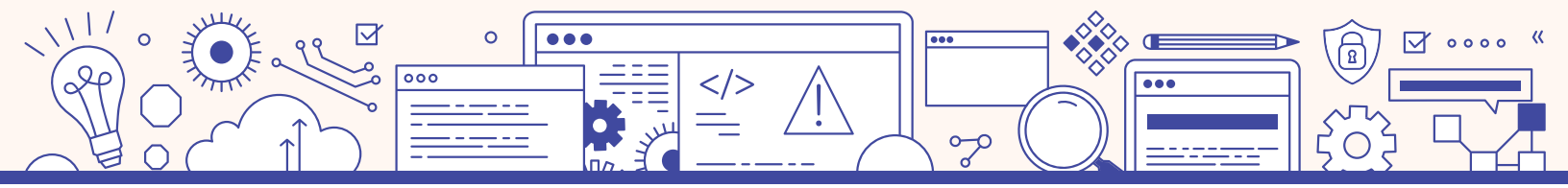
SaaS needs to make good business sense

The following are possible scenarios that would undermine the value of the investment in SaaS:

A similar service already exists, creating unnecessary duplication. Does the government ecosystem already have what your team needs? How can you coordinate approved SaaS to realize economies of scale?

You realize after you've paid for your SaaS subscription that it has specific technical requirements. It might be more complex than you realize. For example, the SaaS may need to integrate with the government's enterprise services for purposes of identity and access, security and data backup, among other issues. Had you informed your departmental enterprise architecture team of your plans, they might have spotted these issues for you.

Updated SaaS no longer meets your expectations around capabilities, performance or cost. Losing control of the costs of SaaS is a considerable risk.



How do I get approval for and obtain SaaS?

Talk to your CIO about the process in place for your organization so you're ready, as a manager, to respond to your team's SaaS requests. Obtaining approvals may take some time (likely weeks); many approval processes will include your CIO's cyber security team, Shared Services Canada (SSC), Public Services and Procurement Canada (PSPC), and the Communications Security Establishment (CSE). This may seem like a long (even intimidating) list; don't worry! Your IT team will navigate this process on your behalf.

The following conditions, though beneficial, are **not** enough to fully mitigate any risk:

- The SaaS is hosted on a government-approved cloud provider
- Data is hosted in Canada
- The SaaS has third-party security certifications
- Another government organization is using it

A comprehensive yet responsive approval process helps to ensure the vendor meets all the technical, security, procurement and information requirements for government IT applications.

Tip: When researching and procuring SaaS, a good place to start is the GC Cloud Brokering Service.

A final note

The Treasury Board of Canada Secretariat's (TBS) Directive on the Management of Procurement, Appendix B, B.1.1.4, states that, for low-risk and low-dollar-value goods and services contracts, PSPC, SSC and departmental procurement teams may accept standard commercial terms and conditions. These include subscriptions, software, mobile applications, cloud services, and open-source software. This should make procuring SaaS easier. Work with your CIO and procurement team to ensure everyone is applying the most updated policies and directives when procuring SaaS. Need a kick-start? Read the blog How a new directive makes it easier to procure software in the GC for inspiration.

Related products

Discover GC Cloud (DDN104)

GC Cloud for Managers and Executives Learning Path (DDN1-PA1)

GC Cloud for Managers and Executives: Planning for GC Cloud (DDN211)

GC Cloud for Managers and Executives: Supporting the Procurement of GC Cloud (DDN212)

GC Cloud for Managers and Executives: Enabling the Deployment of GC Cloud (DDN213)