New Zealand Government

BRIEFING FOR EMPLOYEES AND CONTRACTORS

Accelerating Public Cloud

Right-sizing risk assessments

December 2017

Cloud first policy

This policy requires agencies to adopt public cloud services in preference to traditional IT systems.

A risk assessment is required

Agencies are required to adopt public cloud services on a case-by-case basis following a risk assessment and implementation of applicable security controls. For office productivity services, additional security controls are required.

The risk assessment process is a series of questions that help gauge the risks associated with a public cloud service and identify any controls that are required to ensure the risk of adopting the service is acceptable. Some of these questions can be answered by suppliers.

You decide how to assess risk

Each agency must understand the business context of its use of public cloud services. Agencies decide how they want to run their risk assessment process. The Government Chief Digital Officer (GCDO) has tools and guidance available to help with this.

The time and effort spent on the risk assessment should be proportional to the level of risk. In practice, this means carrying out an initial assessment focused on the sensitivity of the information and the criticality of the service. If the initial assessment concludes that risks are acceptable, then a detailed risk assessment will not usually be required in order to use the service.

Where significant risks are present, then a more-detailed risk assessment will typically be needed to address a range of security, jurisdiction, privacy and contractual issues. Where possible, agencies should reuse guidance produced by the GCDO or other agencies.

Approval can be delegated

As it is impractical for Chief Executives to approve all risk assessments, each agency should ensure that approvals are delegated to an appropriate level, in line with the agency's risk framework. For example, a low risk service could be signed off by a business unit manager.

The GCDO does not endorse agency sign-offs. Instead, agencies are required to submit their risk assessments to the GCDO for reporting purposes and to enable agencies to share and re-use them.

Tools and resources

The GCDO provides a range of services that assist agencies to use cloud services securely, including:

- Security and Related Services (SRS) panel – An all of government panel of suppliers is available to provide ICT security professional services to help agencies with in-depth risk assessments.
- Telecommunications-as-a-Service (TaaS) panel – An all of government panel of suppliers is available to provide a range of managed security services that can be used to mitigate some of the risks of using cloud services.
- Public cloud marketplace - The GCDO is developing a way to give agencies access to a catalogue of public cloud services which will help agencies understand the security position and commercial terms and conditions of these services.

There are more tools and guidance available on ict.govt.nz and in the New Zealand Information Security Manual.

The following scenarios illustrate different ways agencies can use the risk assessment process

Scenario 1

Using an online booking service to organise an event

Do an initial risk assessment by thinking about the information that will be stored in the service (for example is there any personal information? What could happen if the information was lost or made public?)

Check the marketplace or your agency’s list of approved cloud services to see if your preferred tool (or an equivalent tool) is already approved for use.

Check your agency’s policies to find out who is able to accept risk. For low risk usage or services already in use by your agency, you or your manager may be able to accept the risk. Ideally, you should be able to complete this kind of risk assessment on the spot or at least within a day.

Use basic risk mitigations, such as: reviewing terms and conditions of use, assigning a business owner who is accountable for the use of the service, making sure you know how to add and remove staff access, knowing what information can and cannot be stored in the service, and having a plan for retaining access to information once you stop using the service or if the service is discontinued.

Scenario 2

Using a public cloud service to analyse data

Do an initial risk assessment by thinking about the information that will be analysed (for example is there any personal information?)

Check the marketplace or your agency’s list of approved cloud services to see if your preferred tool (or an equivalent tool) is already approved for use.

Check your agency’s polices to find out who is able to accept risk. For further guidance, talk to your IT team or relevant advisors.

For some scenarios, you may need specialist advice from the SRS panel to complete the risk assessment, including undertaking a privacy impact assessment (PIA) and any security certification and accreditation activities. You may also use some of the managed security services from the TaaS panel to implement additional security controls.

Learn more

Find the latest public cloud guidance and tools on ict.govt.nz, or talk to your Department of Internal Affairs relationship manager. This briefing is part of the programme led by the Department of Internal Affairs to accelerate the adoption of public cloud services.