<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>3</td>
</tr>
<tr>
<td>Definitions</td>
<td>4</td>
</tr>
<tr>
<td>Assessing jurisdictional risk</td>
<td>5</td>
</tr>
<tr>
<td>Commonly-used jurisdictions</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive summary

Purpose
This guidance has been produced by the Government Chief Information Officer to help New Zealand public sector agencies manage jurisdictional risks for public cloud services. It should be used by agencies as an input into their risk assessments of public cloud services. Additional guidance on risk assessments is available from: ict.govt.nz

Background
In July 2016, Cabinet confirmed new measures to accelerate the adoption of public cloud services across government. These measures were a response to the reduced costs and improved resilience and security of these services compared with other technology delivery models. These services also have the ability to drive digital transformation within agencies.

Jurisdictional risks
In the context of public cloud services, jurisdictional risks occur where data is subject to the laws of the country where cloud services providers store, process, or transmit data. ‘Data sovereignty’ is often used interchangeably with ‘jurisdictional risks’.

Assessment frameworks
This guidance contains frameworks for assessing jurisdictional risks in relation to both jurisdictions and cloud services providers. Agencies are encouraged to use these frameworks to inform their risk assessments of public cloud services.

After completing their risk assessments, agencies may decide that their appetite to use a public cloud service is limited to specific cloud services providers, specific jurisdictions, and specific data sets.

Jurisdictional assessments
This guidance assesses the following eight jurisdictions: United States, Netherlands, Germany, Singapore, United Kingdom, Ireland, Australia, and Canada. These are the most commonly-used jurisdictions and were identified from an analysis of public cloud services that agencies intend to use.

Agencies may use public cloud services hosted in jurisdictions outside of these eight jurisdictions. However, they should use the assessment framework from this guidance to inform their risk assessments.

Basis of assessments
The assessments in this guidance are based on open source information. These assessments were made in June 2017 and will be reviewed periodically or if significant changes occur that warrant a review.

Release of guidance
Note that this version of this guidance omits the jurisdictional assessments (pages 9-29). The full version is available to agencies via: ict.govt.nz

UNCLASSIFIED
Definitions

Jurisdictional risks

In the context of public cloud services, jurisdictional risks occur where data is subject to the laws of the country where cloud services providers store, process, or transmit data. ‘Data sovereignty’ is often used interchangeably with ‘jurisdictional risks’.

Jurisdictional risks may lead to situations which are disadvantageous to New Zealand’s national interests or inconsistent with New Zealand’s laws as it is not possible to fully contract out of the legal framework of another country. For this reason it is important that agencies engage with cloud providers to ensure they know in which country their data is transmitted, processed, or stored (a concept sometimes referred to as data residency) and are aware of the laws of the country to which their data will be subject.

Extra-territorial reach

Extra-territorial reach is where a government lawfully endeavours to access data from a cloud services provider outside its territory. While this is a complex and evolving area of international law, recent court rulings suggest that there are significant limitations on the exercise of extra-territorial reach.

Data surveillance

This guidance is concerned with lawful access to data by other governments. It does not address the risks of data surveillance (espionage) or data theft by other governments or actors. The risks posed by data surveillance are out of scope of this advice.
Assessing jurisdictional risks

Case-by-case risk assessments

Agencies are required by Cabinet to undertake case-by-case risk assessments before using public cloud services. These risk assessments include an assessment of jurisdictional risks.

Consider jurisdictions and providers

As jurisdictional risks are impacted by which jurisdictions and cloud service providers are used, assessments of jurisdictional risks should include both of the following considerations:

• how governments lawfully access data which is stored, processed, or transmitted in their territory
• how cloud services providers respond to requests by other governments for access to the data they store, process or transmit.

After completing their risk assessments, agencies may decide that their appetite to use a public cloud service is limited to specific cloud services providers, specific jurisdictions, and specific data sets.
Assessing jurisdictions

Rationale
Agency risk assessments of public cloud services should be informed by an assessment of how governments lawfully access data which is stored, processed, or transmitted in their territory.

Implications
After completing their risk assessments, agencies may decide that some jurisdictions are only appropriate for some types of data.

Assessment framework
It is recommended that agencies assess jurisdictions using all of the following three criteria:

• **Lawful access** — An assessment of the laws that regulate a government’s lawful access to data.

• **Legal institutions** — An assessment of the robustness of legal institutions that oversee a government’s lawful requests for access to data.

• **Privacy frameworks** — An assessment of the protections available to personally identifiable information.
Assessing cloud services providers

Rationale

In addition to assessing jurisdictions, agency risk assessments of public cloud services should be informed by an assessment of how cloud services providers respond to requests by other governments for access to the data they store, process or transmit.

Implications

After completing their risk assessments, agencies may decide that some public cloud services are only appropriate for some types of data.

Assessment framework

It is recommended that agencies assess cloud services providers using all of the following five criteria:

• **Location** – An assessment of whether the provider identifies the location of where customer data is stored and backed-up.

• **Informed** – An assessment of whether the cloud provider informs its customers in the event of lawful requests to access customer data.

• **Disclosure** – An assessment of whether the provider only discloses customer data when required by a warrant.

• **Reviewed** – An assessment of whether the provider dedicates resources to reviewing lawful requests to access customer data.

• **Deletion** – An assessment of whether the provider deletes customer data after the termination of contract.

Best practice service terms

A best practice cloud service provider will:

• Commit in its service terms to never disclose customer data except as directed by the customer or required by the law (noting any potential exceptions, such as imminent threat to life, and the processes that must be followed in these cases).

• Set out a process for responding to government requests that includes:
  – always attempting to redirect the requesting agency to contact the customer
  – if possible, seeking to narrow the scope of government demands
  – always contacting the user when information is released (unless legally prevented from doing so)
  – disclosing only that information which is specified in the legal order.

• Have a dedicated team for reviewing government demands for user data.

• Report publicly on the frequency of data requests by country and the results of data requests (particularly for commercial services).

• Allow the customer to determine where their content will be stored, and specify the circumstances when it may be moved to another jurisdiction.
Commonly-used jurisdictions

For practical reasons, such as latency, it is anticipated that New Zealand public sector agencies will want to use public cloud services hosted in jurisdictions that are in close geographical proximity to New Zealand: Australia, Singapore, and the United States.

Based on the demand for public cloud services from the October 2016 survey of CIOs, it is possible that agencies will also use several other jurisdictions: Netherlands, Germany, United Kingdom, Ireland, and Canada.

Other jurisdictions

These eight jurisdictions are not an approved list of jurisdictions. Agencies may use public cloud services hosted in other jurisdictions. However, where agencies do so, it is recommended that they use the criteria outlined above to inform their risk assessment.

Analysis and assessment of jurisdictions

Using a range of open source material, each of these eight jurisdictions are analysed in terms of the three criteria from the assessment framework for jurisdictions: lawful access, legal institutions, and privacy frameworks.

An overall assessment of this analysis is also provided for each of these eight jurisdictions. It is recommended that agencies use this overall assessment as an input into their assessment of jurisdictional risk and this should, in turn, form part of their case-by-case assessment of public cloud services.

Please note that the country-by-country analysis is not included in the UNCLASSIFIED version of this guidance.