



DOIA 1617-1339

29 June 2017

Shane Gibson

fyi-request-5813-3b21a668@requests.fyi.org.nz

Dear Mr Gibson

Thank you for your email of 3 May 2017 to the Ministry of Business, Innovation and Employment (the Ministry) containing an Official Information Act 1982 request for the following information:

- *Does your organisation currently use the Atlassian Confluence Cloud service? (<https://www.atlassian.com/software/confluence>)*
- *Has a formal cloud assessment being undertaken and approved for the use of this service?*

Yes, a handful of staff at the Ministry use, or have used, the Atlassian Confluence Cloud service to upload a minor amount of non-confidential data for testing Confluence, or to contribute to an international forum through an online questionnaire, for their respective roles. However, the Ministry does not administer or maintain Confluence services.

Turning to the second part of your request, the Atlassian Confluence Cloud service has not been formally approved for use at the Ministry, however, we have utilised a CASB¹ Risk Assessment function to provide us with a high-level Risk Assessment of the service. A CASB Risk Assessment provides us with an assessment covering 50 attributes of a cloud service. These cover legal, service, business, data and user/device risks.

The CASB Risk Assessment deemed the Atlassian Confluence Cloud service to be low risk. If, in the future, the Ministry decides to use the Confluence Cloud service to deliver the Ministry's services, it will be subject to the various government ICT and Cloud governance and assurance requirements. For example, the NZ Government Protective Security Requirements and Section 4 of the New Zealand Information Security Manual (System Certification and Accreditation Process).

Yours sincerely

Jon Matthews
Manager ICT Security & Risk

¹ **CASB Definition**

According to Gartner, a cloud access security broker (CASB) is an on-premises or cloud-based security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. Organizations are increasingly turning to CASB to address cloud service risks, enforce security policies, and comply with regulations, even when cloud services are beyond their perimeter and out of their direct control.

