



Australian Government
**Department of Employment
and Workplace Relations**

RFFR Accreditation Report

TPES system - Bridge



With the exception of the Commonwealth Coat of Arms, the Department's logo, any material protected by a trade mark and where otherwise noted all material presented in this document is provided under a [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) (<https://creativecommons.org/licenses/by/4.0/>) licence.

The details of the relevant licence conditions are available on the Creative Commons website (accessible using the links provided) as is the full legal code for the [CC BY 4.0 International](https://creativecommons.org/licenses/by/4.0/legalcode) (<https://creativecommons.org/licenses/by/4.0/legalcode>)

The document must be attributed as the RFFR Accreditation Report for Bridge SaaS Limited's Bridge.

Contents

Purpose	4
Background	4
RFFR Accreditation	4
Shared Responsibilities	4

Purpose

This document is to assist the Department's employment and skills service Providers (Providers) in understanding the scope and conditions of the RFFR Accreditation status issued to the Third Party Employment and Skills (TPES) system Bridge.

Background

Bridge SaaS Limited provides Software-as-a-Service (SaaS) based Customer Relationship Management (CRM) and workflow solutions to employment, care and support industries. The system developed by Bridge SaaS Limited is called Bridge.

Bridge SaaS Limited was certified under ISO27001: 2013 on 12 May 2023 by the certifying body Global Compliance Certification Pty Ltd (GCC).

RFFR Accreditation

The Department issued RFFR Accreditation to the TPES system Bridge on 12 July 2023 as a result of a risk-based assessment. Features in scope of the assessment included:

- Client case management,
- Communications platform (email, SMS)
- Outcome tracking and claim management,
- Ongoing support,
- Job application management and job matching,
- Job Seeker Classification Instrument (JSCI) import,
- Job plan import,
- Organisation (Employer, Supplier, Activity Host) management,
- Vacancy management,
- Task management,
- Finance management,
- Appointment management,
- Advanced user management, and
- Data visualisation and analytics.

Shared Responsibilities

The Bridge system is developed and maintained in house by Bridge SaaS Limited. It is currently hosted in Vault Cloud via the service subscription of Critical Infrastructure Cloud (CIC) service. Vault Cloud is a CSP who provides Infrastructure-as-a-Service (IaaS). In addition to CIC, Vault Cloud also offers Government Cloud (GC) service which is not consumed by Bridge SaaS Limited. Both CIC and GC have

been IRAP assessed for the security of the cloud, whereby only the Vault Cloud GC service is listed under the Digital Transformation Agency (DTA)'s Hosting Certification Framework¹.

Bridge SaaS Limited is responsible for the security in the cloud while Vault is responsible for the security of the cloud. The RFFR assessment was focused on Bridge SaaS Limited's responsibilities.

When consuming the TPES system Bridge, Providers have shared responsibilities for the security in the system including below.

- Providers are responsible for adhering to their contractual obligations in managing the security while using the TPES system Bridge. This includes achieving RFFR Accreditation within required timeframe and maintain the Accreditation through annual surveillance assessments. The consumption of Bridge should be included in scope of the relevant Providers' Information Security Management System (ISMS) and required security assessments using a risk-based approach.
- Providers are responsible for managing the authorisation to Bridge SaaS Limited to access and process commonwealth records on their behalf via the TPES system Bridge, in adherence to the terms and conditions of relevant government systems such as eSAM and MyGovID.
- Providers are responsible for risk assessing the TPES system Bridge in line with the Provider organisations' security requirements before consuming the system. Providers are encouraged to reach out to the Department and Bridge SaaS Limited to seek additional assistance when required.
- When using the TPES system Bridge, Providers are responsible for the applicable controls in below Guidelines from the Australian Government Information Security Manual (ISM):
 - Guidelines for Cyber Security Roles,
 - Guidelines for Cyber Security Incidents,
 - Guidelines for Procurement and Outsourcing,
 - Guidelines for Personnel Security,
 - Guidelines for Enterprise Mobility,
 - Guidelines for System Hardening,
 - Guidelines for System Management,
 - Guidelines for Email, and
 - Guidelines for Data Transfer.

Yours sincerely



Adam Shain
Acting First Assistant Secretary,
Digital Solutions Division

12 July 2023

¹ <https://www.hostingcertification.gov.au/certified-service-providers>