CAPEXinsights
CAPITAL PROJECT DELIVERY MADE BETTER

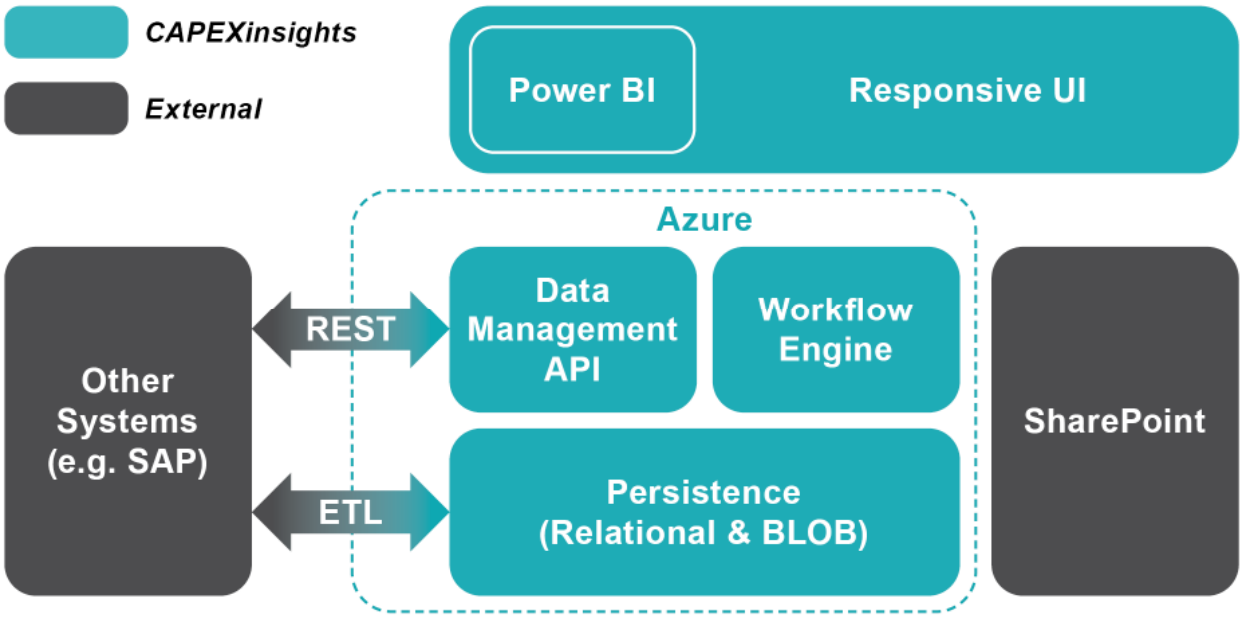
Technical Factsheet

Application Security, Privacy & Architecture

Architecture

CAPEXinsights is a user-friendly software application designed to help deliver better outcomes for your capital projects. The application utilises Microsoft Azure as a technology stack which includes; data warehouses located in Australia, Azure Security Centre Standard Tier, which has continuous assessment and Microsoft's advanced threat detection for platform-as-a-service. In addition, Beca also has the application regularly security tested by an external third-party.

Access to CAPEXinsights is authenticated via federation with the customers' own Azure Active Directory identity provider, which enables users to login with their existing corporate username and password.



Security

Our practices are aligned to ISO27000 and observe industry processes for secure software design development, testing, hosting, operations and management. CAPEXinsights leverages Microsoft Azure's comprehensive automatic backup functionality across different fault domains in the same region to provide resilient disaster recovery and business continuity failover.

We have in place a Security Incident Response Plan that is used to manage responses to incidents.

Privacy

We respect the privacy of our clients and are committed to protecting the personal data that the application collects by taking appropriate measures to maintain the accuracy and security of such information and to only permit appropriate access to it, in accordance with relevant privacy laws and regulations, including (where applicable) the EU General Data Protection Regulation (EU GDPR). This includes identification and management of personal data sub-processors.

As part of this approach, a Terms of Use of Privacy Statement are required to be endorsed by each user prior to use of the application. The Privacy Statement identifies the customer's Data Protection Officer.

Customer Data

Through Azure Data Share, we can set up regular transfers of project information from our Azure database to your Azure database. This allows your ‘citizen programmers’ to create their own.

Third Party Access

People external to the customer organisation ('third parties') can be granted access to CAPEXinsights. This can happen through one of two mechanisms:

- **Azure security groups:** Generally, a customer will be able to approve access to an Azure security group to a person or people that are external to their organisation through an Azure Web App. By consequence of this approval, they will have access to CAPEXinsights.
- **CAPEXinsights user management interface:** At the time of writing, we are currently updating CAPEXinsights so that through the user management interface, authorised people can directly modify who does and does not have access to the application or given modules within the application. This includes third parties that have been approved through the Azure security group. In addition, authorised people can add external third parties directly through the user management interface.

Note that CAPEXinsights utilises an open security model. This means that people can access any project in the project space. The benefit of an open security model is that people can learn from the delivery of other projects, and there is minimal user administration. In addition, projects can be removed from the general population by making them confidential. This is important for projects that may have significant financial impacts on an organisation, affect people, affect share price, etc. The consequence of this approach is that third parties will also have access to the general population of projects.