



Overview

A large federal government body was facing challenges from ageing infrastructure and expiring hardware and software contracts. Refreshing the environment was vital to the continued hosting of a strategic and critical application. Diaxon was asked to lead the development of detailed server and network designs to inform and enable the subsequent build phase.

Diaxon delivers server and network detailed designs for a federal government body

The Challenge

Our client is a large federal government body that was undergoing a period of data centre transformation and rationalisation, driven by ageing infrastructure and expiring hardware and software contracts. The environment hosted a strategic and critical application that needed to be refreshed, calling for the development of detailed server and network infrastructure designs. These would be used by the infrastructure teams to support the build phase of the organisation's file transfer platform refresh project.

An important component of the project would be an analysis of the current environment with an intent to eliminate or reduce technology obsolescence, remove end-of-support hardware and software, simplify infrastructure through consolidations, and move to a next generation security architecture requiring a transformation into multiple functional layers. The environment would need to be highly available with protection against numerous potential component or site failures, while providing secure connections internally and externally.

The organisation needed help from a company with extensive experience in complex change programmes for Protected, secure, and regulatory environments. The provider would need to have security cleared resources and a proven engagement methodology working with federal government agencies.

The Solution

After a formal tender process, Diaxon was selected based on its proven methodology with similar projects in critical application environments that were complex, secure and Protected. Giving the client confidence and illustrating their transformation journey were vital. Security cleared resources and prior experience with the client also made Diaxon the ideal choice.

The engagement began with an evaluation of the current environment, identifying what was working and the issues being experienced.



Diaxion

Right fit IT strategy and high
calibre delivery for tangible
business outcomes.
Helping organisations achieve
IT Modernisation through
People, Process and
Technology.

Diaxion's methodology was used to define the scope and scale, and specify all technical and operational dependencies. The discovery also included a thorough review of technical documentation to formulate a picture of the topology and the design decisions for the current environment.

With a current baseline in place and guided by design principles of security, availability, simplification, and customer experience, Diaxion defined the target state and the initial requirements to feed into the new server and network detailed design documents. Diaxion took a collaborative and dynamic approach by actively seeking input from stakeholders at all stages of the design process. This ensured that risks and issues were identified, mitigated and signed off quickly to facilitate efficient delivery of the project.

The detailed design considered implementation of the target state and incorporated interim migration states and rollback capability. The analysis and target state definition also took the business strategy and drivers into account, ensuring that the design aligned with organisational strategy, needs and expectations. Diaxion also assessed the gathered information against policy alignment, enterprise architecture, operational and physical considerations.

When all stakeholders agreed to the outcomes, the conclusions of the workshops and the documentation to date, the detailed design documentation process began. If subsequent adjustments were required, a review process was initiated to ensure rapid incorporation into the final deliverables.

The Outcome

The detailed design documents provided our client with a comprehensive architectural blueprint to inform and enable the server and network build phase. The documents outlined the scope, assumptions, reference documents, solution architecture, physical design, logical design, security, integration, and management requirements.

The documentation became the new standard and enabled easier filtering and viewing of hundreds of defined objects. It was also used as a structured dataset for firewall policy generation to enhance consistency, reduce time to delivery, and aid any subsequent configuration or design changes.

The client was able to identify changes required and move onto migration planning of the critical service with confidence that the network and server designs met the robust compliance and performance requirements.