FORESIGHT

GRC Case Study

Blending a consultative approach with professional expertise to deliver security assurance services

Summary

A leading Australian government department ("the Department") required security specialists to conduct a myriad of system security assurance services, including security risk assessments and system security plan development. The scale, complexity, and timeframe of this program of work required an innovative and agile response from Foresight's expert team. A consultative approach was adopted throughout each delivery cycle, commencing with a discovery workshop for each in-scope system to fast-track the delivery timeline. The client noted the assessments undertaken exceeded their expectations. Foresight was and continues to be seen as a trusted advisor.

Our client's challenge

As a government body with international presence, the Department operates within a dynamic and demanding cybersecurity threat landscape. The Department also developed a "cloud-first" strategy to leverage more services from cloud service providers and shift away from deprecated on-premise solutions. In line with its commitment to improving its security posture, the Department developed a formal system accreditation framework. The framework was to be applied to all of the Department's information assets, including highly critical systems which could directly impact national security. The key challenges faced by the Department related to the volume, complexity and diversity of the systems, and the pressing timeframe within which the assessment and accreditation process was to be completed.

In response to these challenges, the Department commissioned a program of work and established a panel inviting third-party security specialists. Foresight has been a member of the panel since the commencement of the program and has established a strong and trusted relationship with the Department.

Scope of engagement

The scope of the program entailed security assessment and advisory services for a range of systems within the Department's operating environment, as well as systems proposed for implementation. The Department conveyed the scope and requirements for each system to the prospective third-party consultancies, which were managed as individual engagements.

The nature of the work requested typically requires a comprehensive review of documentation and system architecture, stakeholder engagement and risk analysis. Over an 18-month period, Foresight assisted the Department to complete several engagements, including security risk assessments, the provision of security advisory, and the development of Security Risk Management Plans (SRMPs), System Security Plans (SSPs), Statements of Applicability (SoA), security policies and frameworks.

How Foresight helped?

Foresight adopted a consultative approach with the Department throughout the journey. Foresight commenced each engagement with a discovery and scoping workshop with the Department's subject matter experts to gain an understanding of the system context, architecture, scope, and associated requirements. This approach helped form a trusting and open relationship with the Department and enabled Foresight to deliver services efficiently and effectively. Foresight was also able to work as a team to meet the requirements of the Department, leveraging experienced consultants to support GRC work on a range of cloud, on-premise, hybrid, managed-service and other types of engagements. Foresight consultants also sought advice from other experienced consultants within Foresight to understand technologies better and develop robust deliverables for the Department.

By comprehensively reviewing system documentation and actively engaging with key client stakeholders, the Foresight team developed an in-depth understanding of the Department's system accreditation framework and associated processes. Coupled with Foresight's experience in cybersecurity and risk management standards and frameworks, this understanding contributed towards delivering practical risk-based outcomes which added value.

The outcome

Foresight demonstrated an excellent track record in completing the requested services within expected (and often narrow) timeframes. The work required by the Department also required consultants to think on their feet and be responsive to stakeholder needs, and it was noted by the Department that Foresight was able to deliver where other vendors could not. This was illustrated by the additional engagements won by Foresight under this program of work.

Moreover, the Department was highly impressed with the quality of the deliverables, and the professionalism and dedication of the Foresight team particularly during COVID-19. Foresight achieved high quality deliverables by leveraging an internal peer-review process, and products were discussed and workshopped with Department stakeholders prior to submission. During the early phase of the pandemic, Foresight continued to provide services onsite to meet the Department's timeline.

The Department noted the Foresight team has provided risk workshops and technical risk analysis to their security teams and business owners, a level of service that was not supplied by other vendors. The Department also conveyed the technical assessments exceeded their expectations. As such, Foresight is not only viewed as a third-party vendor, but a trusted advisor to the client organisation.

foresight.security

FORESIGHT