Cyber Security Arrangements

Project Specification

Background

In 2017, the Government of Jersey published its first island-wide Cyber Security Strategy for public consultation with the aim of making the island a "safe place to live and do business in both the physical and digital worlds". The strategy addressed five key pillars: Government, Critical National Infrastructure, Business, Legislation and International Engagement and Citizens.

The Government of Jersey provides critical operations and services to citizens and businesses across the Island and all of its services depend on the security and availability of Information Technology (IT) and Operational Technology (OT) systems.

In 2020, to continue the work towards its key aim, the Government of Jersey commenced a Government-wide cyber security transformation programme, to be delivered in two, 12 month tranches. Work commenced on the programme in March 2020, with Tranche 1 originally scheduled for completion by March 2021. However, the global COVID-19 pandemic and associated public health measures and restrictions have inevitably led to some programme delays.

Tranche 1 of the programme is comprised of six distinct projects:

- Programme Management
- Managed Service Security Provider (MSSP)
- Governance Improvement
- Identity and Access Management
- Asset Management; and
- People Security.

These projects are designed to allow the Government to manage secure access to critical systems, proactively detect security incidents and manage the security of assets used within the network.

The Functions of the Comptroller and Auditor General (C&AG)

Article 11 of the Comptroller and Auditor General (Jersey) Law 2014 requires the C&AG to:

- provide the States with independent assurance that the public finances of Jersey are being regulated, controlled, supervised and accounted for in accordance with the Public Finances (Jersey) Law 2005

- consider and report to the States on:

    o the effectiveness of internal controls of the States, States funded bodies and funds

    o the economy, efficiency and effectiveness in the way the States, States funded bodies and funds use their resources; and

    o the general corporate governance arrangements of the States, States funded bodies and funds; and

- make recommendations to bring about improvement where improvement is needed.

Objectives of this follow-up review

The review will evaluate:

- the progress of the cyber security programme against the roadmap which was defined at the commencement of Tranche 1

- any significant gaps between the roadmap and work carried out to this point, with an assessment of the actions planned and being undertaken to address such gaps

- the overall effectiveness of the cyber security programme in achieving the objectives of Tranche 1.

Scope

This review will evaluate the progress of the activities that have been defined as forming Tranche 1 of the Cybersecurity Programme for the Government of Jersey. Any Tranche 2 activities are outside the scope of this review.

The review will not consider cyber security arrangements in arms-length organisations.

The objectives and/or scope of the review may be amended in the course of the review in the light of emerging findings or other matters arising.

Approach

The review will commence with an initial documentation request and the identification of the relevant key officers and stakeholders to be engaged.

The findings of the document review will be followed up by interviews with key officers and potentially with other stakeholders.

The methodology of the work conducted will align with current public health guidance from the Government of Jersey.

The detailed work will be undertaken by affiliates engaged by the C&AG.

Fieldwork is planned to commence September 2021.