Key Policies of the

Government's Third-Party Management Framework

Note: This document contains general information for the public only. It is not intended to be relied upon as a comprehensive or definitive guide on each agency's policies and practices. The Government may, in its sole discretion, update the policies set out in this document without publishing such updates.

GOVTECH
GOVERNMENT TECHNOLOGY AGENCY OF SINGAPORE

SMART NATION & DIGITAL GOVERNMENT OFFICE

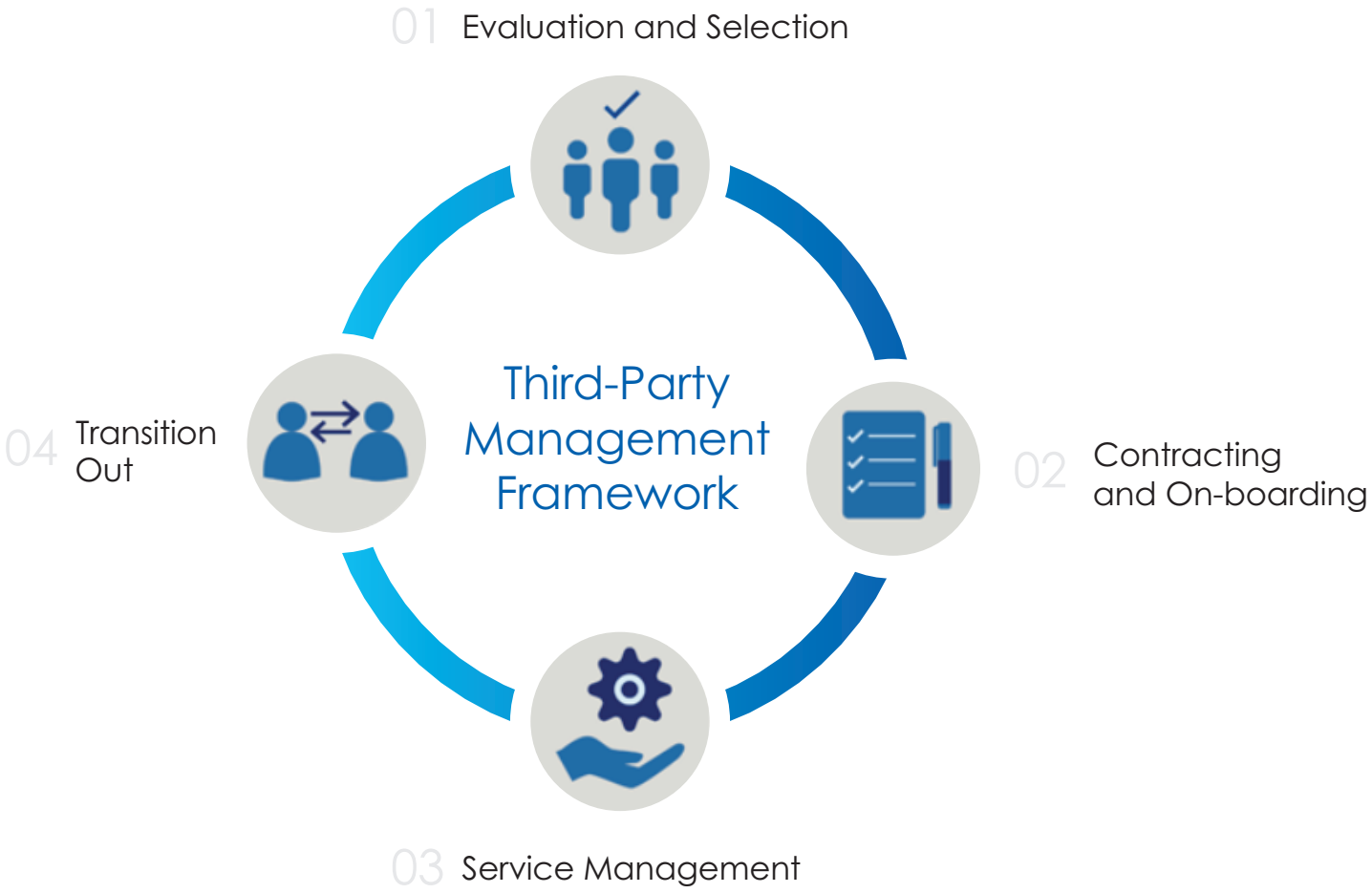
Published on 30 Apr 2020

Introduction

The Government recognises that Agencies work extensively with Third Parties to deliver services to citizens, carry out operational functions, and plan and analyse policies. When doing so, these Third Parties may handle large volumes of data from the Government. Hence, the high standards of data protection that the Government places on itself must also extend to these Third Parties.

With this in mind, the Government has introduced policies to guide Agencies in ensuring that Third Parties adequately safeguard data. These policies are organised based on the lifecycle of the relationship between the Agency and the Third Party, namely: Evaluation and Selection, Contracting and On-boarding, Service Management and Transition Out (as shown in Diagram below). When working with Third Parties, Agencies will define the data security requirements that each Third Party has to comply with based on the Government's data security policies.

Lifecycle of the Third-Party[1] Management Framework



DEFINITION

[1] Third Party is defined as a party (other than a data subject[a] or an Agency[b]) which:

(i) delivers, develops, implements, operates, provides or otherwise supplies ICT systems or services to an Agency, or

(ii) collects, stores or otherwise processes data for an Agency.

a Data subject refers to the individual or entity to which the data relates.

b Agency refers to Organs of State, Ministries, Departments and Statutory Boards.

Key Policies of the Third-Party Management Framework

Stage 1

Evaluation and Selection

01 To ensure that the Government adequately manages its security, data and project risks when engaging Third Parties, Agencies shall identify, assess, prioritise and mitigate the risks when outsourcing work to Third Parties during the evaluation and selection process.

Stage 2

Contracting and On-boarding

02 To ensure that the security, data and project risks involved in assigning work to Third Parties are addressed, Agencies shall establish contracts or other equivalent instruments with their Third Parties to govern how the Third Parties should perform the assigned work in a manner that addresses all identified risks involved.

03 To ensure that the appointed Third Parties (and their personnel) are adequately assessed, cleared and prepared for the assigned work, Agencies shall implement an on-boarding process which includes briefings on applicable data security requirements, security clearance and obtaining undertakings from Third-Party personnel, where necessary.

Stage 3

Service Management

04 Agencies shall regularly monitor and review the Third Parties' performance and compliance with applicable public sector policies and standards which are incorporated in the contracts or equivalent instruments established with the Third Parties.

05 Agencies shall perform regular checks or audits on their Third Parties throughout the period of engagement to ensure that the Third Parties carry out their assigned work in compliance with contractual obligations and applicable public sector policies and standards. More stringent requirements will be imposed on Third Parties dealing with systems and services of a higher risk.

Stage 4

Transition Out

06 To ensure business continuity and the proper transfer and disposal of data and assets back to Agencies upon the exit of the Third Parties, Agencies shall put in place and maintain up-to-date exit management plans for all Third Parties' work and services, which shall include the conduct of exit checks or audits before the Third Parties discontinue their services.