Cyber Security Arrangements

6 May 2022

jerseyauditoffice.je

R.71/2022

JERSEY AUDIT OFFICE

Contents

Summary

Introduction

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

2. 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'.

3. In late 2019, to continue the work towards its key aim, the Government commenced a Government-wide Cyber Security Programme (CSP), with the bulk of the work to be delivered in two, 12-month tranches. Tranche one, that did not extend to OT systems, was originally scheduled for completion by March 2021. However, the COVID-19 pandemic and associated public health measures and restrictions have inevitably led to some programme delays.

4. The two tranches encompass several workstreams each comprising projects aimed at delivering a series of agreed requirements (see Exhibit 1).

Exhibit 1: Terminology used

Term	Meaning
Programme	The overall schedule of work for cyber security, to be delivered over a period of multiple years.
Tranche	A phase of the programme. In this case the cyber security programme has been separated into two tranches.
Workstreams	Distinct areas of delivery agreed to form the scope of the tranche. These relate to different cyber security or project management specialties. In tranche one there were six workstreams, one for project management and five related to delivery of specific cyber security outcomes.
Projects	Individual work packages which together make up a workstream of the programme.
Requirements	Discrete requirements which each project needs to deliver in order to deliver on overall programme objectives.

Source: Jersey Audit Office analysis

5. Tranche one of the CSP comprised six distinct workstreams each made up of several projects. The workstreams were:

- programme management
- Managed Service Security Provider (MSSP)
- governance improvement
- Identity and Access Management (IAM)
- asset management; and
- people security.

6. These workstreams and associated 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.

7. To secure delivery of a programme of this size and complexity effective programme and project management are essential. This review has therefore focussed not only on evaluating delivery of the CSP against the agreed roadmap but also on the reasons for delays and gaps in delivery and the effectiveness of the programme and project management arrangements in place.

8. Articles 11 and 20 of the Comptroller and Auditor General (Jersey) Law 2014 make provision for me to prepare reports arising from my work and forward them to the Greffier of the States to be laid before the States Assembly. Paragraph 64 of the Code of Audit Practice (November 2020) provides that in determining the content and timing of public reporting I should have regard to potential prejudice to the interests of the States of Jersey or other parties arising from public reporting.

9. Having regard to this provision and the subject matter of this report, I have elected to issue a shorter report than usual, excluding my detailed findings but including the recommendations arising from my work. I am, however, providing relevant officers with a supplementary report that provides more details of my findings to assist them in responding to the recommendations that I have included in this report.

Key findings

10. The key findings from my review are as follows:

- an objectively assessed improvement in cyber security maturity has been delivered through tranche one of the CSP

- completion of tranche one was delayed by approximately six months. Although more than 80% of 'must have' deliverables were delivered in tranche one, some were deferred to tranche two and others were removed from the scope of the CSP. Decisions to defer work or remove it from the scope of the CSP were not documented consistently

- in addition to the inevitable impact of the COVID-19 pandemic, other factors impacted on delivery of tranche one, including shortages in internal resources, the inexperience of some key stakeholders and weaknesses in management of interfaces and dependencies

- there were many strengths in the governance model that was implemented to manage delivery of the CSP, including comprehensive tracking at workstream level and strong communication with business units on technical delivery; and

- tracking of benefits at the corporate level was limited, making it difficult to assess the impact of the programme on the Government's overall cyber security. Further benefit tracking and programme level reporting would make it easier for external and senior stakeholders to understand the improvements that are being delivered as a result of the CSP.

Conclusions

11. Tranche one of the CSP has been delivered in a challenging environment, as the COVID-19 pandemic changed operational priorities and stretched resources across the Government of Jersey.

12. Cyber security maturity has increased across all operational areas covered by the tranche one workstreams.

13. However, delays to the CSP cannot solely be attributed to the effects of the COVID-19 pandemic and the associated restrictions and changes to operational priorities.

14. The success of large transformation projects is reliant on effective prioritisation, communication and engagement. The CSP has implemented communication pathways with business units across Government. However, the prioritisation of transformation programmes and projects and of the interdependencies between concurrent transformation programmes and projects could be further improved. In particular there should be increased communication at the leadership level and more effective planning and prioritisation processes.

Objectives and scope of the review

15. This review has evaluated:

- the progress of the CSP against the roadmap which was defined at the commencement of tranche one
- 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 reasons for any delays and gaps in delivery, with identification of potential actions to reduce the risk of recurrence
- the governance of the CSP, including the programme and project management arrangements in place; and
- the overall effectiveness of the CSP in achieving the objectives of tranche one.

16. This review has only evaluated the progress of the activities that have been defined as forming tranche one of the CSP. Any tranche two activities are outside the scope of this review.

17. The review has not considered cyber security arrangements in arm's-length organisations.

18. The review approach is explained in detail in Appendix One.

19. Articles 11 and 20 of the Comptroller and Auditor General (Jersey) Law 2014 make provision for me to prepare reports arising from my work and forward them to the Greffier of the States to be laid before the States Assembly.

20. Paragraph 64 of the Code of Audit Practice (November 2020) provides that in determining the content and timing of public reporting I should have regard to potential prejudice to the interests of the States of Jersey or other parties arising from public reporting. Having regard to this provision and the subject matter of this report, I have elected to issue a shorter report than usual, excluding my detailed analysis but including the recommendations arising from my work.

21. I am, however, providing relevant officers with a supplementary report that provides more details of my findings to assist them in responding to the recommendations that I have included in this report.

Recommendations

R1 Secure documented formal senior approval of any changes to high-level programme targets.

R2 For major programmes, adopt a set of success measures that can be used to evaluate the impact of a programme in a clear and straightforward way.

R3 For major programmes, set overall milestones for delivery at programme level and monitor against those milestones.

R4 For those workstreams and projects where the focus is on consultancy rather than technology implementation, set milestones for delivery and monitor delivery against those milestones.

R5 Undertake a formal documented risk assessment before agreeing deferrals or changes to project deliverables.

R6 Formally document all deferrals and changes to project deliverables.

R7 Formally document at a programme level where deferrals and descoping have been referred to Ministerial level.

R8 Make best use of scarce internal staff resources in future technology programmes through:

- confirming availability during the planning phase; and
- engaging with other programme leads to identify activities in common.

R9 In planning future technology programmes, assess the risks and opportunities associated with simultaneous delivery of multiple programmes.

R10 Deliver structured training to risk owners to develop their understanding of and confidence in their role.

R11 Develop formal mechanisms for co-ordination between programmes regarding the prioritisation and co-ordination of tasks.

R12 Designate internal owners for each workstream in major programmes.

R13 Identify individuals to deputise as alternates at key programme meetings when designated individuals are not available.

R14 In Outline Business Cases document linkages to wider organisational strategies and initiatives.

R15 Ensure that all workstream planning activities in major programmes are fully documented.

R16 Routinely hold workshops with programme stakeholders to identify and prioritise requirements for major programmes.

R17 Develop and roll out appropriate induction training for external project managers.

R18 Introduce structured briefings for stakeholders at the commencement of their involvement in a programme so that they have a clear understanding of their role.

R19 For major programmes, routinely evaluate benefits realised and delivery of Outline Business Case tasks at programme level.

Appendix One

Audit Approach

The review included the following key elements:

- review of relevant documentation provided by the Government of Jersey; and
- interviews with key officers within the Government of Jersey.

The documentation reviewed included:

- Government of Jersey Cyber Assessment Report 2019
- Government of Jersey Cyber Security Programme: Outline Business Case
- Security Working Group – Terms of Reference v2
- Supplier Familiarisation Pack - Cyber Security Programme
- Asset Management - Team Structure
- Terms and Conditions of Contract: Service Agreement for Managed IT Security Services
- Detailed Requirements List for each workstream
- Stage-Gate Checklist for each workstream
- Closure packs/reports
- Project Initiation Document for each workstream
- RAID log for each workstream
- Stage-Gate review slides
- Cyber Security Programme Business Change Introduction

The following officers were interviewed or provided written input:

- The Chief Operating Officer
- The Chief Information Security Officer
- CSP Programme Manager
- The Business Change Lead

The fieldwork was carried out by the Wembley Partners Limited on behalf of the Comptroller and Auditor General.

LYNN PAMMENT
Comptroller and Auditor General
Jersey Audit Office, de Carteret House, 7 Castle Street, St Helier, Jersey JE2 3BT
T: +44 1534 716800 E: enquiries@jerseyauditoffice.je W: www.jerseyauditoffice.je