

**EXAMINATION OF SELECTED AUDITOR-GENERAL'S FINANCIAL AUDIT
REPORTS 2021**

Organisation: NSW Department of Customer Service

Date Received: 16 June 2022



Customer
Service

McKell Building – 2-24 Rawson Place, Sydney NSW 2000

Tel [REDACTED] | TTY 1300 301 181

ABN 81 913 830 179 | www.nsw.gov.au

Office of the Secretary

Our reference: COR-03128-2022

Your reference: D22/24889

Mr Greg Piper MP
Chair
Legislative Assembly
Public Accounts Committee

By email: pac@parliament.nsw.gov.au

Dear Mr Piper

Thank you for your letter dated 6 June 2022 about the NSW Auditor General's (AG) Financial Report on Customer Service Cluster 2021 (the Report) for Financial Year (FY) 2020-21.

The Department of Customer Service (DCS) has a proactive and positive relationship with the NSW Audit Office (AO). Actions to address NSW AO observations noted in the Report are in flight and in many instances have been addressed and closed as of May 2021.

DCS recognises the need for strong governance and internal controls across all its systems and processes. We welcome all opportunities to continually improve governance and internal controls in support of our offerings to the citizens of NSW and the NSW Public Sector.

In response to the two specific recommendations raised by the AG in the Report (as outlined in your correspondence), I offer the following submission:

- 1. Internal control exceptions in information and technology services provided by GovConnect service providers. The Auditor-General reported that in 2021, four of the eight ASAE 3402 'Assurance Reports on Controls at as Service Organisation' for GovConnect services were qualified.***

DCS, as Contract Authority for GovConnect Shared Services provision (to multiple NSW Government Agencies), terminated its contract with previous GovConnect Information Technology Outsourced (ITO) service provider (Unisys) in October 2019. The terms of the contract permitted a 'transition-out' period of up to two years.

Whilst all transitions were complete as of 30 June 2021, due to the timeline of transition activities, Auditors were unable to access records relating to several IT GovConnect controls in an acceptable format. This was a regrettable outcome of the transition process, which necessitated a qualified audit opinion for four out of eight controls. As at May 2021 all exceptions identified in the Report relating to GovConnect IT services controls have been remediated and closed.

DCS is comfortable that it does have appropriate governance controls in place to ensure the strong operation of the GovConnect environment, particularly under its Service Integration and Application Management (SIAM) model.

The SIAM model provides for a dedicated functional group (internal to DCS) to be the single point of accountability and governance for vendor management and performance for all outsourced GovConnect services, thus increasing the span of control of DCS as Service Provider.

With full responsibility for the end-to-end assurance and performance of GovConnect IT Services and controls, significant improvements have been made since the implementation of SIAM including regular reporting of control exceptions and progress against remediation through GovConnect and DCS Cluster Management Assurance processes; increased frequency of internal audits; and early notification and remedy of control exceptions, resulting in an overall reduction in control exceptions.

A post transition review of the transition from Unisys has been undertaken and learnings are being progressively implemented to drive a culture of continual improvement alongside data analytic controls.

2. *“NSW Public Sector’s cyber security resilience needs urgent attention”. The Auditor-General recommended Cyber Security NSW and NSW Government Agencies need to priorities improvements to their cyber security resilience as a matter of urgency.*

While all NSW cluster agencies remain responsible for risk management and their cyber resiliency and maturity, Cyber Security NSW assists NSW Government clusters and agencies to understand and improve their cyber security resilience and maturity. All work undertaken by Cyber Security NSW has this goal in mind.

The NSW Cyber Security Policy (the Policy) was implemented in 2019, and as a result Cyber Security NSW has a whole-of-government view of cyber security. The Policy has Mandatory requirements that focus on enhancing planning and governance, developing a cyber security culture, and strengthening resilience against attacks in addition to implementation of the “Essential Eight” - risk mitigation strategies developed by the Australian Cyber Security Centre (ACSC). To keep pace with a rapidly evolving cyber threat environment, Cyber Security NSW undertakes annual reviews of the NSW Cyber Security Policy.

The NSW Government has committed \$315 million over three years in the Digital Restart Fund (DRF) to cyber security uplift. \$180 million of this is committed to clusters, \$60 million to Cyber Security NSW and \$75 million to small agencies. Cyber Security NSW has assisted these agencies in their bids for funding allocation from the DRF. This helps to ensure there is no duplication with what we are aiming to achieve at scale across the sector. Cyber Security NSW also provides complimentary services to support clusters and agencies’ overall cyber security posture.

On 16 October 2020, the NSW Government released a Circular Cyber Security NSW directive – Cyber Security Hygiene and Practice Requirements. The Circular mandates responsibilities for all employees as well as specific responsibilities for executives, agencies and departments and mandates compulsory annual cyber security training for all NSW public servants (including contractors).

Cyber Security NSW is focussed on increasing understanding and awareness across NSW Government through education of users, specialists, high risk groups and senior executives. Live and eModule training sessions for all NSW Government employees is provided. Exercises are also conducted across the sector to practice for significant cyber security incidents or a cyber

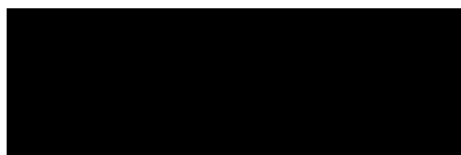
crisis. Attendance and engagement with the live training is recorded and monthly uplift statistics submitted to relevant senior executive groups.

Cyber Security NSW provides leadership and coordination across all departments and agencies to reduce the likelihood, impact and spread of cyber-attacks on NSW Government. Cyber Security NSW coordinates incidents and information across whole-of-government in accordance with the Cyber Security NSW Incident Response Plan, the State Emergency Sub-Plan for Cyber Security, and the Federal Cyber Incident Management Arrangements.

Cyber Security NSW will continue to support increased cyber resilience in the NSW Public Sector as its highest priority in consultation with clusters and agencies who are responsible for delivering on uplift initiatives.

I trust that the above provides the PAC with the necessary additional information and comfort in its examination of the AG's Financial Report on the Customer Service Cluster for Financial Year 2020-21. Should you have any further queries or seek additional information regarding this matter please do not hesitate to contact [REDACTED], Acting Chief Operating Officer Department of Customer Service at [REDACTED]

Yours sincerely



Emma Hogan
Secretary

Date: 16/06/22