Assessment of Implementation Report

Travel Alberta

Managing the Risks of Cloud Computing

(December 2019)

Summary of Recommendations

In December 2021, we completed our assessment of implementation from our December 2019 audit of Travel Alberta's processes for managing the risks of cloud computing. We found that both recommendations have been implemented:

IMPLEMENTED Recommendation:
Develop a risk management process for cloud computing

IMPLEMENTED Recommendation:
Develop contract management processes for contracts with cloud service providers

Introduction

In 2019,[1] we audited Travel Alberta's processes to manage the risks of using cloud computing. We found board oversight over cloud computing risks, risk management processes, contracts with cloud service providers and monitoring of cloud service provider performance and compliance with service agreements could all be improved. We made recommendations to Travel Alberta to develop:

- risk management process to manage the risks of using cloud computing
- contract management processes for contracts with its cloud service providers

[1] *Report of the Auditor General of Alberta—December 2019*, page 2.

Recommendation:
Develop a risk management process for cloud computing

IMPLEMENTED

Context

Risks of cloud computing include security, privacy, service accessibility and reliance on the integrity and trustworthiness of cloud service providers.

In 2019, we found that Travel Alberta did not have a process to assess, monitor and report the risks associated with its use of cloud computing. We also found little evidence of board oversight of cloud computing risks.

Our current findings

Travel Alberta implemented our recommendation. It deployed an information technology (IT) risk management framework that includes identifying, documenting and managing cloud computing risks. We found that Travel Alberta developed a data classification policy that is consistent with the Government of Alberta's data and information security classification standard and established an appropriate cloud computing governance structure that is supported by policies and procedures.

Management ranked cloud services in tiers from one to three depending on their risk scores, with tier one the highest risk. Risk scores assigned are based on data classification, combined with the severity and likelihood of risks identified by IT department. The IT department prepares a cloud services security controls form for the service risks identified as well as detailed mitigation plans. Risk scores and mitigation plans are then logged in the IT risk register. The IT department reviews the IT risk register monthly and updates the risk scores quarterly depending on the progress of the mitigation plans. We examined evidence that this process was consistently followed.

Our discussion with the board and examination of board meeting agendas, packages, and meeting minutes provided evidence that the board asked management to:

- develop an implementation plan to improve cloud computing risk management processes
- engage an external consultant to provide advice to the board and management on best practices to develop enterprise risk management processes
- provide quarterly updates on the progress of their implementation plan
- provide updates on the communication between Travel Alberta and the Government of Alberta's Office of the Chief Information Security Officer to ensure Travel Alberta's policies are consistent with the Government of Alberta's standards
- provide periodic updates on cloud computing risks and planned mitigating actions as required by Travel Alberta's enterprise risk management policies

Recommendation:

Develop contract management processes for contracts with cloud service providers

IMPLEMENTED

Context

To manage risks arising from the use of a third-party cloud service provider, organizations need to ensure that contractual arrangements with the provider are well understood and monitored. Contracts with cloud service providers must incorporate specific business requirements identified by the organization through its IT planning and business planning processes.

In 2019, we found Travel Alberta did not identify and incorporate specific business requirements in cloud service provider contracts and did not have a process to regularly monitor cloud service providers performance and compliance with the terms of contractual agreements.

Our current findings

Travel Alberta implemented our recommendation. Policies and procedures for the acquisition of cloud services and the management of cloud services contracts were developed by management and approved by the board.

We saw documentation that the IT department carried out risk assessments before the acquisition of cloud services.

To help Travel Alberta manage and monitor its cloud service providers, management developed a cloud service vendor master list to serve as an inventory record of all cloud contracts. Travel Alberta's cloud services policy requires a performance review of cloud service providers with timelines based on the tier of cloud service (tier one—annually, tier two—at contract mid-point, and tier three—six months prior to contract end). We examined a sample of tier one and tier two contracts and found evaluations were performed within the established timelines. We also confirmed that out of the nine contracts in tier one, seven evaluations were completed and two are in progress. Of the evaluations that management completed, one resulted in a request for a contract amendment. As a result of contract reviews, management identified user controls that needed to be improved.

For the sample of contracts we examined, we found that the contract evaluation process includes an assessment of the:

- specific service level requirements that meet Travel Alberta's business needs
- security, privacy and data residency requirements that comply with Travel Alberta's corporate policies
- right to retrieve data upon termination of services
- business continuity, ownership and data transferability
- right to audit or access to service auditor reports

We found the requesting business unit, the procurement department, IT department and legal, established clear roles and responsibilities to ensure cloud service contracts are properly authorized, monitored and evaluated throughout the contract life cycle.