Review of
Data Centre Security

July 2018

INTERNAL AUDIT
AND ADVISORY SERVICES

BRITISH COLUMBIA | Ministry of Finance

Project No.: 18−05 CITZ

Review of Data Centre Security

Internal Audit & Advisory Services
Ministry of Finance

Fieldwork completed: April 2018

Introduction

The Office of the Chief Information Officer (OCIO) enables the Government of British Columbia (the Province) and the broader public sector to access technology solutions, including hosting infrastructure and services.

In 2009, the Province entered into a 15-year Master Service Agreement with ESIT Advanced Solutions Inc. (ESIT) for the provision of data centre services. The agreement also covers a 12-year term for managed-hosting services, including security administration and compliance activities.

To meet the Province's requirement of having its core data centre in British Columbia, ESIT contracted Q9 Networks Inc. (Q9) to build a data centre in the Province's interior region. A secondary data centre facility in Alberta is also used to support the Master Service Agreement. These facilities were designed to ensure high levels of reliability and availability. They became available to the Province in April 2011 and the fall of 2009 respectively.

Expected benefits of the data centre consolidation include: savings in energy costs, replacement of aging infrastructure, and relocation of data to facilities away from major earthquake fault lines and flood zones. Furthermore, geographic diversity provides enhanced disaster recovery capabilities between the two data centres.

The Province and broader public sector entities can subscribe to a secure environment with an allotment of power, space, and specific services within the two facilities managed by ESIT and Q9. Reliability and security of the data centre infrastructure and IT assets are crucial requirements to ensure the confidentiality, integrity, and availability of the Province's records and information, and is core to the delivery of the Province's critical services.

Review Summary

Internal Audit & Advisory Services reviewed the physical and environmental security of the third-party managed data centre facilities as well as the data security and security incident management. An internal management report with detailed recommendations was issued to the OCIO. Due to the sensitivity of the review's scope, the detailed management report will not be publicly released.

The review evaluated and made recommendations, where appropriate, on the OCIO's and service provider's security processes (including practices to date), with a focus on reviewing the following areas:

- **Physical and Environmental Security Management**: Existing processes to ensure access to the data centre facilities and the related IT infrastructure is protected from environmental threats;
- **Data Security Management**: Existing processes to ensure the Province's information assets housed at the data centres are safeguarded from compromise; and
- **Security Incident Management**: Existing processes to ensure continuity of data centre operations and the stability of its systems while managing incidents or disruptions.

As part of this engagement, Internal Audit & Advisory Services reviewed the work completed through third-party reports including: System and Organization Controls reviews, engineering reviews, and an IT general controls review. No additional testing was completed on the controls identified in these reports. In addition, an on-site visit to the Province's primary data centre was performed.

Conclusion

The OCIO and ESIT have established procedures and controls to ensure that the Province's IT infrastructure and data located in the data centre facilities are secured from physical, environmental, and logical threats. While many of these controls are appropriate, there are still opportunities to improve on specific areas.

Upon completion of our review work, this review identified 10 recommendations related to the following:

- Four recommendations related to enhancing the physical security of the third-party data centres used by the Province;
- Two recommendations to strengthen the Province's processes to manage and monitor its data security;
- Three recommendations to better monitor the service delivery by the Province's service provider;
- One recommendation to further improve the Province's security incident management process.

The OCIO and ESIT have started to develop action plans to address these recommendations.

Internal Audit & Advisory Services would like to thank the management and staff of the Office of the Chief Information Officer as well as ESIT Advanced Solutions Inc. and Q9 Networks Inc. who participated in and contributed to this review, for their cooperation and assistance.

Stephen Ward, CPA, CA, CIA
Executive Director
Internal Audit & Advisory Services
Ministry of Finance