Chapter 32
Economy—Monitoring IT Service Providers

1.0 Main Points

Information technology (IT) service providers are agencies or companies used to host, develop, and/or support IT systems and data.

For the 12-month period ended April 30, 2014, the Ministry of the Economy (Economy) had, other than for the following matters, effective processes to monitor whether its IT service providers appropriately managed and secured its IT systems and related data. Economy needs to:

- Maintain current agreements with its IT service providers
- Include appropriate provisions in agreements with IT service providers for security requirements and security reporting
- Establish written policies and procedures for taking corrective actions and reporting on problems with IT service providers

2.0 Introduction

Economy is responsible for leading and coordinating growth in Saskatchewan by working with other ministries, stakeholders, and the general public. Economy's mandate encompasses three primary lines of business: enhancing economic growth and competitiveness; regulating responsible resource development; and attracting, developing, and retaining a skilled workforce.[1]

Economy employs approximately 575 people across six divisions, and operates in Regina and other locations including Saskatoon and La Ronge.[2]

To deliver its programs and services, Economy relies on various IT systems, including systems to assign and track mineral rights, and to manage oil and gas reporting and royalties.

In 2013-14, Economy directly contracted three main IT service providers. One of these was the Information Technology Division of the Ministry of Central Services (ITD). ITD provided the majority of Economy's IT services[3,4] either directly (using its own staff) or through ITD hiring third-party IT contractors for work at Economy. In 2013-14, Economy paid ITD $10.1 million (2012-13: $6.3 million) for IT services,[5] and $2.5 million (2012-13: $1.8 million) to its other two main IT service providers.[6]

[1] Ministry of the Economy, *Plan for 2014-15*, p. 3, 4, and 5.
[2] www.economy.gov.sk.ca/structure (18 July 2014).
[3] www.cs.gov.sk.ca/ITServices (18 July 2014).
[4] The Information Technology Division of the Ministry of Central Services (Central Services) supports all ministries within the Government of Saskatchewan with the majority of their hardware and software, application development and IT security services.
[5] Ministry of Economy accounting records.
[6] Ibid.

It is vital that Economy effectively monitor its IT service providers to ensure that its IT systems and data are effectively managed and secured. If Economy does not effectively monitor its IT service providers, it may not receive good quality IT services or be aware of functional or security issues. This could result in problems with IT systems, including compromised security or errors in functioning in key IT systems. These systems contain sensitive personal and corporate (e.g., oil and gas company) information and are used to levy, collect, and record Saskatchewan's non-renewable resource revenues (i.e., 2013-14: $2.5 billion,[7] 2014-15 First Quarter forecast: $2.8 billion[8]) and related transactions for the government and other participants in the resource sector.

3.0 Audit Objective, Scope, Criteria, and Conclusion

The objective of this audit was to assess whether Economy had effective processes to monitor whether its information technology (IT) service providers appropriately managed and secured its IT systems and related data. We assessed Economy's processes for the period of May 1, 2013 to April 30, 2014.

To conduct this audit, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance*. To evaluate Economy's processes, we used criteria based on our related work, literature and consultations with management. Economy's management agreed with the criteria (see **Figure 1**).

We examined a sample of Economy's agreements, reports, and other documentation that related to Economy's IT service providers. We also examined a sample of ITD's agreements with third-party IT contractors who work at Economy. As well, we interviewed Economy staff, and reviewed meeting minutes and correspondence.

Figure 1—Audit Criteria

To have effective processes to monitor whether IT service providers appropriately manage and secure its IT systems and related data, the Ministry of the Economy should:

1. **Set effective agreements**
   - 1.1 Set out the IT services to be provided
   - 1.2 Assign responsibilities (i.e., between Economy and service providers)
   - 1.3 Specify security requirements
   - 1.4 Provide for adjustment and dispute resolution
2. **Maintain capacity for monitoring IT service providers**
   - 2.1 Identify required resources for monitoring
   - 2.2 Assign responsibilities for monitoring (i.e., within Economy)
3. **Monitor IT service delivery**
   - 3.1 Assess performance of IT service providers at key intervals (e.g., through review of reports, inspections, etc.)
   - 3.2 Verify issues and incidents are managed appropriately
4. **Take timely corrective action**
   - 4.1 Set criteria for taking action
   - 4.2 Implement timely corrective measures
   - 4.3 Report on steps taken

We concluded that, for the period of May 1, 2013 to April 30, 2014, the Ministry of the Economy had effective processes to monitor whether its information

[7] *Public Accounts 2013-14, Volume 1*. p.67.
[8] *Saskatchewan Budget Update 14-15, Steady Growth: First Quarter Financial Report,* p.4.

technology (IT) service providers appropriately managed and secured its IT systems and related data, except that the Ministry needs to:

- **Maintain current agreements with its IT service providers (i.e., that reflect current structure, responsibilities, and programs of the Ministry)**
- **Include appropriate provisions for security requirements and security reporting in agreements with IT service providers**
- **Establish written policies and procedures for taking corrective actions on and reporting problems with IT service providers**

4.0 KEY FINDINGS AND RECOMMENDATIONS

In this section, we describe our expectations (in italics) and key findings and recommendations related to the audit criteria in **Figure 1**.

4.1 Effective Agreements Required

To effectively monitor a service provider, an appropriate agreement must be in place. We expected to see such agreements in place between Economy and all of its IT service providers, and also between those IT service providers and contractors they hired to work at Economy. We expected that agreements would set out the services to be provided, assign responsibilities, specify security requirements, and provide for adjustment and dispute resolution.

We found problems with Economy's agreements with two of its three main IT service providers.

First, Economy did not have an up-to-date agreement with ITD. The agreement had not been updated since 2011 even though numerous changes had occurred at Economy, including the amalgamations of parts of different ministries into Economy. As a result, the agreement did not reflect Economy's current structure, programs, services, or IT environment. Economy and ITD have developed a draft agreement to reflect the current programs, services and IT environment; however, the agreement has not yet been signed by either party.

Second, Economy did not have a current agreement with one of its other main IT service providers. This IT service provider hosts[9] and operates Economy's IT system for assigning and tracking mineral rights. In 2008, Economy signed a development agreement with this IT service provider for development of this IT system. This IT system went into operation in 2012. Since that time, Economy has experienced issues with this system's functionality. Economy is working with this IT service provider to resolve the issues. Pending resolution, Economy has withheld payments and not signed an agreement for the IT services it currently receives from this IT service provider.

Without up-to-date agreements, there is greater risk the parties will not have a clear understanding of what IT systems the service providers are responsible for, what

[9] "Hosting" is where the IT system servers and data are located at the service provider.

services the service providers are expected to provide, the levels of service and reports that Economy is to receive, and the cost to Economy to utilize the service providers. The absence of an agreement with the IT service provider hosting Economy's system and related data increases risks regarding the security and availability of that IT system and mineral rights data.

1. **We recommend that the Ministry of the Economy maintain agreements with its IT service providers that reflect the current structure, responsibilities, and programs of the Ministry.**

We also found that Economy's IT agreements with two of the main IT service providers did not contain appropriate security requirements. For example, these agreements did not set out controls Economy expects these providers to use to protect Economy's systems and data against viruses or malicious software. Without appropriate security requirements in agreements, Economy's systems and data may not be properly protected, for example, against cyberattacks.[10] The agreements also do not specify the processes to follow to report a security breach to Economy. Therefore, if a security breach were to occur, Economy may not be informed in a timely way.

In addition, Economy's agreements with all three of its main IT service providers need to strengthen requirements for security reporting. For example, none of the agreements included adequate requirements for reporting security breaches to Economy. Nor do the agreements require ongoing reporting to provide Economy with assurance that security controls are effectively protecting Economy systems and data. Without adequate security reporting, Economy will not have adequate information to determine whether its data and systems are sufficiently protected.

2. **We recommend that the Ministry of the Economy include appropriate provisions for security requirements and security reporting in agreements with IT service providers.**

As noted earlier, ITD provides certain IT services to Economy directly and other IT services by hiring third-party IT contractors to work at Economy. We found that the agreements ITD signed with these contractors for the delivery of services to Economy sufficiently outlined the expectations of the contractors, the roles and responsibilities of each party involved, and security requirements.

4.2 Sufficient Capacity Exists for Monitoring IT Service Providers

To appropriately monitor IT service providers, we expected Economy to assign the responsibility for monitoring to employees within Economy who are in positions to

[10] Cyberattacks include the unintended or unauthorized access, use, manipulation or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or share that information. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf, p. 3 (16 July 2014).

monitor the IT service providers. As well, we expected these supervising employees to have adequate resources and information to fulfill their monitoring role.

Economy uses multiple employees to monitor IT service providers. These employees (supervising employees) are responsible for managing a particular IT service or system and monitoring the receipt of expected IT services. We found that these supervising employees were aware of their role and responsibilities, and were in positions that enabled effective monitoring. For example, supervising employees were directors of the units for which the IT service providers hosted systems.

However, as discussed in **Section 4.1**, Economy's agreements with its IT service providers did not set out appropriate IT security requirements including security reporting. Because of this, Economy did not have sufficient information to monitor whether these service providers appropriately secured its systems and data. See recommendation in **Section 4.1**.

As noted earlier, Economy used third-party contractors hired by ITD (IT contractors) primarily to work on its new IT system for oil and gas business processes.[11] These contractors helped develop the new system, program new requirements into the already functioning parts of the system, and maintain the system. During the audit period, approximately 40 IT contractors worked with Economy on this system. Consistent with its main IT service providers, Economy assigned certain employees to monitor the work of these IT contractors. We found those employees were adequately informed of their monitoring role and carried out their monitoring responsibilities. They had access to appropriate information and resources to carry out their monitoring responsibilities.

4.3 More Effective Monitoring of IT Service Delivery and IT Security Needed

To effectively monitor IT service providers that provide hosting services, we expected Economy to receive reports related to system performance and security. As well, we expected Economy to review reports and communicate with its IT service providers to discuss updates, issues, or changes.

Economy used a variety of methods to monitor IT service delivery. These methods included participation on committees with related stakeholders, review of reports from IT service providers, and direct communication with IT service providers and IT contractors. We found that Economy regularly met with representatives from all three of its main IT service providers, and participated on committees that help monitor them. We found senior management at Economy received and reviewed reports on the performance of each of its three main IT service providers (except, as noted earlier in **Section 4.1**, Economy did not require, and therefore did not receive, appropriate information on IT security). Not receiving adequate information on security increases the risk that IT systems and data will not be properly secured and insufficiencies in security will go undetected. This in turn increases the risk that systems and data may be accessed or changed without authorization or not be available when needed (see recommendation in **Section 4.1**).

[11] The new system is called the Integrated Resource Information System (IRIS). The project to develop the IRIS system is called the Process Renewal and Infrastructure Management Enhancement (PRIME) project. Our Office examined project management for development of PRIME and reported the results in our *2011 Report – Volume 2*, Chapter 6.

Where Economy identified issues and incidents related to IT services, we found that it adequately followed up with the related IT service providers. For IT services delivered through ITD, Economy used ITD's service desk to address problems. If Economy was of the view that ITD did not handle problems in a timely or adequate manner, it escalated the problem by contacting appropriate individuals at ITD until the problem was resolved to its satisfaction. For IT services delivered through other service providers, we found that Economy either met with or communicated regularly with those IT service providers to address issues or incidents.

For the third-party contractors hired by ITD to work at Economy (IT contractors), Economy's supervising employees held weekly meetings with them to review their progress on tasks. As well, the supervising employees produced a monthly performance report which reflected the amount of work tasked to and completed by the contractors.

If problems arose with an IT contractor's performance, Economy directly contacted the company through which ITD had hired the contractor to provide services to Economy. Where that company was not able to work with the contractor to resolve Economy's issues with the contractor's performance, Economy worked with the company and ITD to replace the contractor. Economy evaluated the impact of the problems on its staffing.

4.4 Policies and Procedures Required for Taking Timely Corrective Action

Employees monitoring IT service providers need to take corrective action when issues occur. We expected that Economy would establish criteria in written policies and procedures for taking action to address problems with its IT service providers. We expected the supervising employees to follow the Ministry's policies when taking action and to report on corrective actions to appropriate levels within the Ministry (i.e., to senior management).

Economy's supervising employees identified problems with IT service providers through service reports and through its contacts with system users (both employees within Economy and external users of Economy's IT applications). Supervising employees demonstrated a clear understanding of corrective measures to take, and took corrective measures in a timely manner. For example, Economy contacted all three of its main service providers at various times and when resolving problems, escalated the problems to more senior levels as necessary. With respect to reporting, supervising employees kept relevant senior managers within Economy informed via emails and participation in meetings regarding corrective actions taken.

However, Economy did not have written policies or procedures to guide employees on actions to take on problems identified with IT service providers and IT contractors, and to guide related reporting. Without written policies and procedures, there is an increased risk that supervising employees may take inconsistent or inadequate action to address IT service problems, and that there may be resulting inefficiencies or errors in the IT services provided that could affect the cost, timely delivery, and operating effectiveness of IT systems.

3. **We recommend that the Ministry of the Economy establish written policies and procedures for employees regarding taking corrective actions on and reporting problems with IT service providers.**

5.0 Selected References

Canadian Institute of Chartered Accountants (CICA). (2009). *Trust Services Principles, Criteria, and Illustrations*. Toronto: Author.

International Organization for Standardization. (2005). ISO/IEC 270002:2005(E). *Information Technology – Code of Practice of Information Security Management; 2nd Edition*. Geneva: Author.

IT Governance Institute. (2012). *COBIT 5*. Rolling Meadows, IL: Author.