Agriculture

3

Main points

The Ministry of Agriculture (Ministry) regulates pesticides. The Ministry has made some progress towards addressing our 2007 recommendations related to its processes for regulating pesticides, but more work remains. To better monitor and enforce compliance with pesticide control laws, it needs to finish its risk assessment and develop a strategy to address its risks.

The Milk Control Board (Board) regulates the production, supply, pricing, and sale of milk in Saskatchewan. The Board did not set adequate policies for the timely preparation and review of bank reconciliations and journal entries. As a result, management did not independently review or approve monthly bank reconciliations and journal entries on a timely basis.

For Saskatchewan Crop Insurance Corporation (SCIC), we concluded that it had adequate processes for security awareness except that SCIC needs to:

- document in its policies its requirement for a formal security awareness program, specifying who is responsible for the program
- document its plan for delivery of its security awareness program and carry out the plan
- monitor the effectiveness of its security awareness program

Introduction

The purpose of the Ministry of Agriculture (Ministry) is to enable a prosperous market-driven agricultural industry through a supportive legislative framework, policies, and programs and services.[1]

Special purpose funds and Crown agencies

At December 31, 2009, the Ministry was responsible for the following special purpose funds and Crown agencies (agencies). Each one has a March 31 year-end unless otherwise noted.

Agricultural Credit Corporation of Saskatchewan
Agricultural Implements Board
Agri-Food Council
Beef Development Board
Cattle Marketing Deductions Fund
Crop Reinsurance Fund of Saskatchewan
Horned Cattle Fund
Individual Cattle Feeder Loan Guarantee Provincial Assurance Fund
Livestock Services Revolving Fund
Milk Control Board (December 31)
Pastures Revolving Fund
Prairie Agricultural Machinery Institute
Saskatchewan Agricultural Stabilization Fund
Saskatchewan Crop Insurance Corporation
Thomson Meats Ltd. (December 31)
Pension Plan for the Employees of Thomson Meats Ltd. (December 31)

This chapter contains the results of our audits of the agencies with December 31 year ends (other than Thomson Meats Ltd.), the status of recommendations from our 2007 audit about the Ministry's processes for pesticide regulation, and our audit of Saskatchewan Crop Insurance Corporation's processes to keep its staff informed about and understanding information technology security issues (security awareness).

[1] Government of Saskatchewan, Ministry of Agriculture, Plan for 2010-11, p.2.

Our 2009 Report – Volume 3 reports the results of our audit of the Ministry and its special purpose funds and agencies with years ended March 31, 2009. We have not yet completed the 2009 audits of Thomson Meats Ltd. and its pension plan. We expect to report the results of these audits in our next report.

Milk Control Board

The mandate of the Milk Control Board (Board) is to regulate the production, supply, pricing, and sale of milk. Working with producers, processors, and consumers, the Board is to provide producers with the opportunity to obtain a fair return while providing consumers with an adequate supply of high quality dairy products at reasonable prices.

In 2009, the Board had revenues of $175.8 million including $173.3 million from milk sold to processors, expenses of $175.9 million including $174.6 million from milk purchased from producers, and a net loss of $0.1 million. At December 31, 2009, it held net financial assets of $0.9 million.

In our opinion, for the year ended December 31, 2009:

- ♦ **the Board had adequate rules and procedures to safeguard public resources except for the matter noted in this chapter**
- ♦ **the Board complied with authorities governing its services relating to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing**
- ♦ **the Board's financial statements are reliable**

Adequate policies for bank reconciliations and journal entries needed

Management did not independently review or approve monthly bank reconciliations and journal entries on a timely basis.

Regular reconciliation and review of recorded bank balances to the bank's records provides an important check that all charges to the bank accounts are proper, all money due is received, and deposits are made to the correct bank account. It also provides a check on the accuracy and reliability of the Board's accounting records. Furthermore, timely bank reconciliations help detect errors or misuse of money quickly.

The preparation and review of journal entries helps ensure that adjustments to recorded account balances are correct and authorized.

The Board has written policies for the preparation and review of bank reconciliations and journal entries. However, these policies do not specify when this work must be done.

Management did not approve bank reconciliations for February 2009 to May 2009 until August 2009. Also, management did not approve journal entries for the month of April 2009.

Without adequate policies governing the preparation and approval of bank reconciliations and journal entries, there is an increased risk that management may not promptly detect errors or fraud in the Board's bank accounts and accounting records.

1. **We recommend that the Milk Control Board set adequate policies for the timely preparation and approval of bank reconciliations and journal entries.**

Pesticide regulation—a follow-up

Introduction

The Ministry of Agriculture (Ministry) is responsible for regulating the sale, use, storage, transportation, and disposal of registered pesticides in both agricultural and non-agricultural settings.

Chapter 3 of our 2008 Report – Volume 3 includes the status of recommendations from our 2007 audit of the Ministry's processes for pesticide regulation. It reports that at September 30, 2008, the Ministry has made progress towards addressing the two recommendations but more work remains. We continued to recommend that the Ministry:

1. formally analyze the risks that licensees and exempt persons are not following pesticide control laws

2. document its strategy to address identified risks associated with monitoring and enforcing compliance with pesticide control laws

The Standing Committee on Public Accounts agreed with our recommendations on June 16, 2008.

At March 31, 2010, the Ministry has made progress towards addressing these recommendations but more work remains. The following section explains what we expected (in italics) and highlights progress the Ministry has made towards implementing them.

Risk identification and analysis

As noted in our 2007 audit, without an overall risk analysis to guide its activities, the Ministry's inspection activities may not focus on areas with higher risks. The Ministry needs to analyze the risks associated with monitoring and enforcing compliance with pesticide control laws, prioritize those risks, and document the strategy to address those risks. Its analysis should address each of the major categories regulated (i.e., sales, use, storage, transportation, and disposal). For each category, the Ministry needs to identify the risks related to the particular products, locations, and circumstances involving pesticides that pose a threat to human health and the environment (i.e., land, air, and water).

Since our 2008 follow-up, the Ministry provided staff with training on identifying risks, analyzing risk, and using assessments to design suitable action plans. The Ministry used this training to start a risk identification process that focused on pesticide legislation and regulations. Its process helped to identify some risks, the probability of their occurrence, and the severity of their impact. The Ministry also started to note some potential actions to mitigate areas of risk. However, the Ministry had not completed its risk identification and analysis.

The Ministry told us it has plans to continue to develop an overall risk analysis to guide its activities.

Saskatchewan Crop Insurance Corporation—security awareness processes

Introduction

The Saskatchewan Crop Insurance Corporation (SCIC) is a Crown corporation established under *The Crop Insurance Act*. SCIC administers a crop insurance program for crop losses due to weather-related and other natural perils.

SCIC makes significant use of information systems to deliver its programs and services and carry out its mandate. It uses information systems to calculate premium rates and track premiums owed. Field adjusters use computers to record claims. SCIC uses its computer system to calculate and pay out claims to producers. SCIC has over 400 staff at 21 customer service centres throughout the province and at head office.[2] SCIC has plans to increase its staff as it begins operating the federal-provincial agricultural stabilization program (AgriStability) effective January 1, 2010.

SCIC needs to ensure its information systems are secure. If security is not adequate, SCIC risks:

- unauthorized disclosure of confidential producer information
- basing its decisions and operations on incorrect data
- not collecting the correct amount of premiums from the producers
- incorrectly calculating and paying for claims

SCIC needs to ensure that all of its employees keep its information secure. We audited whether SCIC has adequate processes for security awareness.

Security awareness

Security awareness means being well informed about security issues, understanding security responsibilities, and acting accordingly.[3] The key

[2] 2008-09 Annual Report Saskatchewan Crop Insurance Corporation, p.6.
[3] Wulgaert, p.9.

to security awareness is being security conscious and as a result, changing behaviour to appropriately protect information.[4]

Security awareness is an important part of information security. Agencies must keep their information secure, including their information technology (IT) systems and data. This means ensuring the confidentiality, integrity, and availability of information. To do this, agencies must set out and follow adequate security policies and procedures. If users are not aware of the policies and procedures that they need to follow, it is more difficult for an agency to protect its information.[5] Even sophisticated security measures can be rendered less effective if there is inadequate security awareness.

A security awareness program can be a cost-effective method of improving an agency's information security. Improved security awareness can reduce future costs such as recovery of lost data and notification and litigation costs when information has been inappropriately disclosed.

Security awareness activities need to be a continuous process.[6] Without on-going activities, users may forget or be less able to take adequate measures to protect an agency's information. Repeated reminders of security awareness issues can improve a user's capacity to remember security principles. Agencies that have continuous security awareness activities are more likely to have employees that are "security conscious" as they carry out their responsibilities. This decreases the risk that information will be lost, stolen, or inappropriately disclosed.

We describe good processes for security awareness more fully at the end of this chapter.

Audit objective, criteria, and conclusion

The objective of this audit was to assess whether SCIC had adequate processes for security awareness for the twelve-month period ended February 28, 2010.

[4] Ibid.
[5] Herold, p.xxix.
[6] Wulgaert, p.4.

To conduct this audit, we followed *The Standards for Assurance Engagements* published by The Canadian Institute of Chartered Accountants. To evaluate SCIC's processes, we used criteria based on the work of other auditors and current literature listed in the selected references. SCIC's management agreed with the criteria (see Exhibit 1).

Exhibit 1 – Audit criteria

To have adequate processes for security awareness, an agency should:

1. demonstrate management commitment to security awareness
2. implement adequate security policies that incorporate a security awareness program
3. inform users of their responsibilities through a formal security awareness program
4. periodically review the effectiveness of its security awareness program

We concluded that, for the twelve-month period ended February 28, 2010, Saskatchewan Crop Insurance Corporation's processes for security awareness were adequate except Saskatchewan Crop Insurance Corporation needs to:

- ♦ **document in its policies its requirement for a formal security awareness program and specify who is responsible for the program**
- ♦ **document its plan for delivery of its security awareness program and carry out the plan**
- ♦ **monitor the effectiveness of its security awareness program**

Key findings and recommendations

In this section, we describe our expectations (in italics) and key findings for each criterion.

Demonstrate management commitment to security awareness

To demonstrate management commitment to security awareness, we expect that agency management will:

- *communicate responsibility for security awareness to all employees*
- *set an example by participating in security awareness activities*
- *approve human resources and a budget sufficient to carry out security awareness activities*

SCIC management demonstrated its commitment towards security awareness. SCIC hired a contractor to analyze the overall information security level at SCIC. SCIC formed a security and privacy oversight committee. The committee is composed of members representing all major departments at SCIC. Its objective is to oversee all aspects of security and privacy management within SCIC. SCIC has also hired a full-time privacy security commissioner. During the audit period, SCIC developed a Privacy and Security Manual. The manual states that the policies and guidelines apply to all employees, consultants, and other organizations sharing information belonging to SCIC. During the audit period, executive management discussed privacy and security issues at executive management committee meetings.

Although there was no separate budget for security awareness activities, SCIC held several security awareness sessions during the audit period at various locations throughout the province. Senior management also attended the security awareness sessions.

Security policies incorporate security awareness program

We expect that agency security policies will include the requirement for a security awareness program. The policy should require that the security awareness program:

- *include all employees and relevant contractors*
- *be an on-going program to ensure that security issues are regularly discussed*
- *be reviewed for effectiveness on a regular basis*

SCIC has a privacy and security policy. However, the policy only discusses security awareness for new employees. The policy does not set out a requirement for an on-going security awareness program.

The privacy and security policy states that managers and business leaders are responsible for ensuring that employees comply with policies. However, the policy does not specify who is responsible for security awareness activities at SCIC. The job description for the Privacy Security Commissioner does not specifically address security awareness for SCIC.

2. We recommend that Saskatchewan Crop Insurance Corporation include in its privacy and security policies a requirement for a formal security awareness program.

3. We recommend that Saskatchewan Crop Insurance Corporation document who is responsible to ensure that security awareness activities are regularly carried out.

Inform users of their information security responsibilities through the formal security awareness program

We expect that agencies will implement a formal security awareness program. This would include:

- *a documented plan that specifies clear objectives, target dates, and the strategy to build security awareness*
- *ensuring the plan is based on an assessment of the agency's security awareness needs*
- *ensuring the program covers all employees, all key topic areas and uses a variety of methods to deliver the security awareness message*
- *tailoring the program to meet the needs of the employees that are receiving the security awareness information*
- *having key branches and departments of the agency provide input into the program*

SCIC does not have a formal plan to deliver security awareness to all employees and contractors.

During the audit period, security awareness training was delivered to business leaders (management and supervisors) within SCIC. This training covered all topic areas and was in appropriate detail for the intended audience. SCIC also sent reminders to employees regarding security and privacy issues. Also, SCIC employees are required to read a summary of the security and privacy policies and acknowledge in writing that they have read them. SCIC plans to provide security awareness training to all its staff during 2010-11.

4. We recommend that Saskatchewan Crop Insurance Corporation document its plan for delivery of its security awareness program and carry out the plan.

Periodically review the effectiveness of the security awareness program

We expect agencies to monitor the effectiveness of their security awareness program, including:

- *setting out how it will measure the effectiveness of its security awareness program*
- *performing periodic research to identify trends in security awareness issues*
- *adjusting its security awareness program based on its assessment of effectiveness and its research*

SCIC has not set out plans to monitor the effectiveness of its security awareness program. SCIC told us that it informally discussed security awareness sessions with its employees and made changes.

5. We recommend that Saskatchewan Crop Insurance Corporation monitor the effectiveness of its security awareness program.

Good processes for security awareness

In this section we describe more fully good processes for security awareness.

Demonstrate management commitment to security awareness

Adequate security awareness starts with senior management setting the tone for the agency. Senior management needs to provide adequate resources in terms of personnel and funding for security awareness activities. It should communicate to all employees the importance of security and security awareness. Senior management needs to assign responsibility for security and security awareness to someone senior in the agency. This assignment should ensure that someone takes the lead in security awareness and that security awareness activities take place. Also, senior management needs to lead by example by participating in security awareness activities. Senior management should ensure that the agency has appropriate security awareness policies (discussed further under the next heading). It needs to approve these policies and monitor compliance.

Security policies incorporate security awareness program

Security policies need to specify requirements for an on-going security awareness program. A formal program should cover all staff and relevant contractors. It should provide for on-going activities. There should be regular reviews of the effectiveness of the security awareness activities. The policies should specify who is accountable to ensure security awareness activities take place.

Inform users of their information security responsibilities through the formal security awareness program

Agencies should make sure users are aware of security policies. A formal security awareness program would be based on a plan that documents an assessment of the agency's security awareness needs. Based on those needs, the plan should document a security awareness strategy, set target dates, and set objectives.

The plan and the process to carry out the plan should:

- Cover all employees and relevant contractors
- Focus on all key areas or divisions of the agency

- Make users aware of all key topic areas based on the risks that the agency faces
- Use a variety of techniques to deliver the security awareness messages
- Provide training for both new and existing employees within the agency

The individual assigned responsibility for security awareness should ensure that the key elements in the security awareness plan are carried out.

To help ensure a successful security awareness program, the plan and the security awareness activities should reflect input from a number of areas within the agency.[7] For example, human resources should be involved to ensure that all new employees receive awareness training as soon as practical. Human resources would be able to assist in ensuring that the agency provides security awareness activities to all employees. Also, an agency's IT help desk would be able to provide input into key areas in which users would benefit from additional awareness training.

A security awareness program that involves several delivery techniques is likely to be more effective in increasing the security awareness level of employees. Repetition of the security awareness message in different ways helps employees to keep security in mind as they carry out their responsibilities.

An effective security awareness program ensures that awareness activities are tailored to the needs of the users. Based on the assessed risks, different parts of an agency may need focused training in different areas. For example, a branch that has significant interaction with the public and their personal information would need to be more aware of issues related to confidentiality of personal information (as compared to a network administrator that is not required to access personal information as part of his or her responsibilities).

Security awareness training should be delivered by individuals with appropriate knowledge and experience. Their delivery will be more effective as they will be better able to address participant questions.

[7] Wulgaert, p.31.

Periodically review the effectiveness of the security awareness program

A key to a successful security awareness program is to regularly assess the effectiveness of the program and make changes to improve the program.

To monitor the effectiveness of a program, an agency needs to set targets, measure the achievement of those targets, and report results to senior management. Without this, an agency will not know if its security awareness activities are effective. The risk is that the program does not improve the overall security posture of the agency. Measuring effectiveness could include:

- Tracking the change in the number of security incidents
- Checking employee knowledge of security policies
- Setting mock incidents that would identify whether employees are following the security policies

The agency should use the information gathered to make improvements to the security awareness program. This should be done on a regular basis.

Selected references

European Network and Information Security Agency. (2006). *A Users' Guide: How to raise Information Security Awareness*. http://www.iwar.org.uk/comsec/resources/ENISA/infosec-awareness.pdf. (20 Apr 2010)

Herold, R. (2005). *Managing an Information Security and Privacy Awareness and Training Program*. Boca Raton, FL: Auerbach Publications.

Information Systems Audit and Control Association. (2005). *Critical Elements of Information Security Program Success*. Rolling Meadows, IL: Author. http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/CritElemInfoSec.pdf. (20 Apr 2010)

Saskatchewan Ministry of Justice and Attorney General. (2009). *Information Management Handbook*. http://www.justice.gov.sk.ca/InformationManagementHandbook. (7 April 2010)

Wilson, M. and Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program*. Gaithersburg, MD: National Institute of Standards and Technology Special Publication, U.S Department of Commerce. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf. (20 Apr 2010)

Wulgaert, T. (2005). *Security Awareness - Best Practices to Secure Your Enterprise*. Rolling Meadows, IL: Information Systems Audit and Control Association.