Internal Audit Report—Managing Information Technology Security

January 2018

Practice Review and Internal Audit

Office of the Auditor General of Canada

Bureau du vérificateur général du Canada

Ce document est également publié en français.

Cat. No. FA3-130/2017E-PDF
ISBN 978-0-660-23570-7

Table of Contents

Executive Summary

Objective

The objective of the audit was to determine whether the Office of the Auditor General of Canada (Office) had an adequate and effective framework to support information technology (IT) security.

The internal audit covered the period from 1 January 2016 to 30 November 2016. We extended the audit period to 31 March 2017 to review only the completed action plan that IT security management (management) had prepared as a result of its self-assessment. Management provided this plan to Internal Audit on 24 March 2017.

Why this internal audit matters

This internal audit is important because the Office has recognized that an effective and efficient IT security program is critical to ensuring that the Office protects the sensitive information and valuable assets that are under its stewardship. An adequate and effective **IT security framework** is key to meeting this obligation.

Conclusion

We concluded that the Office had designed an adequate framework to support the security of its IT systems. However, the Office's management of the IT security framework hindered its effectiveness. Specifically, IT security management had not systematically reviewed its policies, procedures, and guidelines, and it had not implemented many controls required by the Treasury Board's policy instruments and guidance that were relevant to IT security.

Management agrees with our recommendations. Its detailed responses follow the recommendations in this report.

We requested an action plan from management and received it on 20 July 2017.

IT security framework—All of an organization's resources, including policies, staff, processes, practices, and technologies, that assess and mitigate IT risks and attacks.

Introduction

What the internal audit focused on

1. This internal audit focused on determining whether the Office of the Auditor General of Canada (Office) had an adequate and effective framework to support information technology (IT) security.

2. A well-established IT security framework

- is consistent with relevant governmental policies and guidelines on IT security;
- has a governance structure with clear roles and responsibilities for IT security;
- has adequate reporting mechanisms for IT functions that are clear, relevant, understandable, useful, and timely;
- has management controls or technical safeguards that protect IT assets and information and ensure secure and uninterrupted service delivery; and
- has an action plan with deliverables and timelines for implementing security management controls or technical safeguards and for measuring the plan's progress.

3. This audit covered the period from 1 January 2016 to 30 November 2016. We extended the audit period to 31 March 2017 to review only the completed action plan that IT security management (management) had prepared as a result of its self-assessment. Management provided this plan to Internal Audit on 24 March 2017.

4. More details about the audit objective, systems and practices examined, and criteria are in **About the Internal Audit** at the end of this report.

Why this internal audit matters

5. This internal audit is important because the Office has recognized that an effective and efficient IT security program is critical to ensuring that the Office protects the sensitive information and valuable assets that are under its stewardship. An adequate and effective IT security framework is key to meeting this obligation.

Findings, Recommendations, and Responses

Self-assessment of information technology security

Summary of findings

6. The Office of the Auditor General of Canada (Office) had developed an adequate information technology (IT) security framework. The Office had established IT security policies, procedures, and guidelines that were mainly in line with the requirements of the Treasury Board's Policy on Government Security and the Treasury Board's Operational Security Standard: Management of Information Technology Security (MITS).

7. The Office was required to conduct annual self-assessments of its IT security programs and practices, but IT security management (management) was unable to confirm whether it had conducted such an exercise before 2016. We found that the 2016 self-assessment was thorough and resulted in a comprehensive action plan.

8. Furthermore, in terms of managing IT security, the Office partially implemented or did not implement many of the requirements in the Treasury Board's MITS standard and in the Office's Information Technology Security Policies, Procedures, and Guidelines.

The Office's self-assessment of IT security was thorough

Why this finding matters

9. This finding matters because an annual self-assessment and update of the Office's IT security program and practices are necessary to identify and mitigate evolving risks.

What we examined

10. At the start of our internal audit, IT security management informed us that it was undertaking a self-assessment of security controls. Management and Internal Audit agreed on the following:

- Management would develop a self-assessment work plan to test key IT security controls, analyze the results, and develop an action plan.
- Internal Audit would review management's work and provide comments and recommendations.

11. Our first step was to discuss with management the methodology that it would use for the self-assessment. We assessed whether the methodology would provide the assurance that Office management needed. We considered the Treasury Board's requirements for the self-assessment and its guidelines for the proposed controls to be tested.

12. We reviewed all of the tests that IT security management designed and performed, and we performed a sample of the tests ourselves. We reviewed management's conclusions on all of the tests.

13. Our findings discuss the following topic:

- Management's approach to self-assessment

Findings

14. **Management's approach to self-assessment.** The MITS standard states that "departments must conduct an annual assessment of their IT security program and practices to monitor compliance with government and departmental security policies and standards. . . ." There was no evidence that the Office had conducted a self-assessment of its IT security program and practices until fall 2016. Therefore, the Office was not in compliance with this requirement in the MITS standard.

15. Management decided that it would conduct the fall 2016 self-assessment on selected systems. This decision was due to time constraints and limited resources, and consistent with Communications Security Establishment Canada's IT Security Risk Management: A Lifecycle Approach (ITSG-33) guidelines.

16. Management used the suggested security controls and control enhancements in the ITSG-33 guidelines. These guidelines list over 900 possible controls for an organization to select from. Management determined controls to be tested on the basis of a tailored approach in line with its risk environment.

17. We reviewed management's decision to perform a self-assessment of only a selection of the Office's systems. We understood that because of limited resources, it was difficult to conduct a full self-assessment of all of the Office's IT systems. Management informed us that, consistent with the spirit of the ITSG-33 guidelines, it would assess other systems on a systematic, rotational basis. It is our view that this is a reasonable approach.

18. For each control test it performed, management documented its work in one or more test scripts, which summarized the scope of work, procedures, results, and conclusions.

19. We did the following:

- We verified that management performed all tests outlined its tailored approach.
- We reviewed all scripts to verify that management performed tests according to the ITSG-33 requirements and that there was evidence to support management's conclusions for each test.
- We verified that all of the scripts went through a proper quality review process.
- We randomly selected 25 scripts and performed the tests ourselves to see if we arrived at the same conclusions as management.

20. We found no discrepancies in the work that management performed. It is our view that management's approach allowed for a thorough self-assessment of a selection of the Office's systems.

The Office's IT security framework was adequate, but weaknesses in implementing its IT policies and practices hindered its effectiveness

Why this finding matters

21. As required by the Treasury Board, it is important that the Office establish clear governance and follow the Treasury Board's policy instruments and guidance that are relevant to IT security to ensure that the information and IT assets under the Office's control are secure.

What we examined

22. We examined the results of the self-assessment of the Office's IT security. In particular, we looked at the Office's IT security framework and whether it was well established, well implemented, and consistent with relevant governmental policies and standards on IT security.

23. We reviewed the Office's governance structure and assessed whether it followed the Treasury Board's policy instruments and guidance that were relevant to IT security. We looked at whether the Office had a reporting process that was clear, relevant, understandable, useful, and timely in reporting IT security incidents to external parties (for example, Shared Services Canada).

24. Our findings discuss the following topics:

- Results of the self-assessment
- Office IT security framework
- Governance
- Implementation of the IT security framework

Findings

25. **Results of the self-assessment.** After completing its self-assessment, IT security management concluded that the Office had many weaknesses related to IT security risk management. We agreed with this conclusion; the following findings detail these weaknesses.

26. **Office IT security framework.** The Office's IT security framework generally aligned with the Treasury Board's policy instruments and guidance that were relevant to IT security. Some mandatory elements were missing in the Office's policy coverage compared with these policy instruments and guidance. The Office's policy did not include the following requirements:

- an annual self-assessment,
- a proper description of the roles and responsibilities of the Office's Chief Information Officer, and
- a description of the IT Security Coordinator's reporting relationship to the Chief Information Officer.

27. Internal Audit noted that other than the policy review that was part of the self-assessment, the Office had not performed a systematic review of each element of the IT security policy. As a result, governance of IT security had not been updated in the Office's policy.

28. Management informed Internal Audit that the Office will adopt any relevant new Treasury Board policy or directive that is issued. Management also informed us that the Office would create procedures, standards, and guidelines as appropriate.

29. **Governance.** Internal Audit looked more deeply into governance issues. We reviewed the work descriptions of IT security staff where relevant, and we found that the three job descriptions were either outdated, did not align with the MITS standard, or did not align with staff members' current responsibilities. One description was non-existent.

30. We found a lack of oversight in the following areas:

- IT Change Management Board—An individual from IT security was appointed chair of the meetings. This individual did not attend about one third of the meetings during our audit period. No one from IT security was delegated to replace this individual during the individual's absence. Furthermore, the terms of reference for the board were outdated.
- Virtual Security Team Committee—We found no terms of reference for this committee and few records of decision. In our view, there was a lack of evidence that the committee provided sufficient oversight to ensure that information related to IT security priorities, plans, and performance was reviewed regularly and that advice on issues was provided in a timely manner.

31. We also found that the Office's automated tools that send alerts to monitor IT security events needed to be improved.

32. With respect to communication, we found that the Office had not formally informed its staff of the nominations of a new Departmental Security Officer and a new Chief Information Officer or of the creation of a new Deputy Departmental Security Officer position. During our audit, the Office also appointed a new coordinator for its Business Continuity Plan. Management informed us that it wanted to communicate these nominations following its IT security self-assessment, once it was in a better position to create an efficient IT security governance framework.

33. The Treasury Board's MITS standard requires senior management to approve departmental IT security policies, standards, and directives. We did not find evidence that Office management had approved the Office's IT security policies.

34. **Implementation of the IT security framework.** The Office partially implemented or had not implemented many of the requirements in its policies and procedures.

35. According to the findings of the self-assessment, 31 percent of the Office's IT security processes met the requirements. For the remaining 69 percent, the controls partially met, mostly met, or did not meet the requirements.

36. Internal Audit obtained audit assurance to support IT security management's conclusion that the test results demonstrated that the Office's selected systems were not safeguarded to an acceptable risk level.

37. Given that management's conclusion on the self-assessment was for selected systems only, Internal Audit also wanted to know if it could conclude on the effectiveness of the Office's IT security framework as a whole. Consequently, Internal Audit also looked to see if the same conclusion applied to other systems. We found that many of the same observations also applied to other systems. Management also reported that most of the controls it tested applied to more than just selected systems and that its action plan incorporated solutions that included all of the Office's systems and applications.

38. In 2015, the Office's Comptroller's Service team also assessed the effectiveness of the system of internal control over financial reporting. Some of the team's observations were similar to management's observations in its self-assessment of selected systems. The team made recommendations based on its observations, and management responded with an action plan. The team's observations supported the view that the problems identified in selected systems were not unique to these systems. These observations reinforced the need for the Office to perform a self-assessment of all of its IT systems.

39. ***Departmental Security Plan.*** Federal organizations are required to develop a Departmental Security Plan that outlines objectives, goals, strategies, priorities, and timelines for improving security. The plan must also provide details on decisions for managing security risks.

40. According to the Directive on Departmental Security Management, the Departmental Security Officer is responsible for updating the Departmental Security Plan on the basis of the results of performance measurement, evaluation, and risk assessments. We found that, although the Office had periodically updated its IT security risks, it had not updated its Departmental Security Plan to reflect these risks since 20 December 2013. The Deputy Departmental Security Officer informed us that the Office intended to issue a new Departmental Security Plan in the 2017–18 fiscal year.

41. ***Threat and risk assessments.*** Threat and risk assessments help organizations to evaluate changes that could affect security. The Treasury Board's MITS standard recommends that for all IT systems, a threat and risk assessment should be performed throughout each system's life cycle (initiation, design and development, implementation, operation, and disposal). Because technologies and threats are always changing, departments and agencies must review security risks regularly and adjust security requirements as needed.

42. For many of its systems, the Office did not regularly update its threat and risk assessments. Management has since implemented a plan to address this issue.

43. ***Business Continuity Plan.*** In January 2014, the Office finalized its Business Continuity Plan. This plan ensures that the Office maintains critical operations so that it has structures and processes in place to recover services after an unplanned business interruption. Routinely testing and revising this plan is a good way to see if it works as designed to ensure minimal or no interruption to critical IT services and assets.

44. To ensure that the Business Continuity Plan works as designed, the Office performed some tests such as two **tabletop exercises**. However, the Office had not tested its **disaster recovery site**. Subsequent to the internal audit, the disaster recovery site was tested.

45. ***External reporting.*** The Treasury Board's Policy on Government Security states that when significant issues concerning policy compliance and security incidents arise, departments must report them to the appropriate agency (for example, the Treasury Board of Canada Secretariat or Shared Services Canada). IT security management developed and documented a process for reporting on IT security incidents. The original process document is dated 1 January 2013. Over the years, management made many changes to the document; the last revision was on 10 September 2015. We found that the document was clear, relevant, and understandable. However, it was still a draft, and it did not reflect the current governance structure for IT security at the Office. This limited the document's usefulness. Management informed us that it was reviewing the document. Management also informed us that there were no significant security breaches.

46. ***Contracts.*** Before issuing a contract, departments must determine if IT security is relevant to the contractor's provision of goods or services. If so, departments must account for IT security requirements at every stage of the contracting process. At the Office, the IT Security Coordinator is responsible for completing IT security checks before a contract is finalized. We were informed that until May 2016, the contracting process did not automatically include verifying IT security requirements.

47. ***Security risks from social engineering attacks.*** In all IT security systems, there are risks associated with people. Attackers often use the vulnerability of people to access secure data. **Social engineering exercises** are an excellent way to assess staff members' reactions to possible IT security attacks from social engineering. We found that the Office had not conducted social engineering exercises since 2011 to determine how its staff members would respond to outside attacks. Management is analyzing the best way to perform such exercises.

Tabletop exercise—A simulated, paper-based exercise that tests organizations' response capabilities.

Disaster recovery site—A facility an organization can use to recover and restore its technology infrastructure and operations when its primary data centre becomes unavailable.
Source: TechTarget, Inc.

Social engineering exercises—Exercises that test staff members' responses to an IT attack, where an outsider acquires sensitive information or inappropriate access by building trust relationships with or tricking insiders or employees.

Recommendations

48. Management should monitor its implementation of the Treasury Board's policy instruments and guidance that are relevant to information technology (IT) security once they are issued and, if needed, take corrective action in a timely manner.

Management's response. *Agreed. As part of the IT security self-assessment action plan of the Office of the Auditor General of Canada (Office), the IT security team has identified and will take all corrective actions that need to be implemented to ensure compliance with the Treasury Board's policy instruments and guidance that are relevant to IT security once they are issued.*

49. Management should annually assess its IT security procedures, standards, and guidelines to ensure that they are up to date and in line with the Treasury Board's policy instruments and guidance that are relevant to IT security once they are issued. This assessment should include monitoring compliance with requirements.

Management's response. *Agreed. As part of the IT security self-assessment action plan, new procedures, standards, and guidelines are being developed. A process is also being developed to ensure that the Office's IT security policies, procedures, and guidelines are reviewed annually to ensure that they are up to date and compliant with the Treasury Board policy instruments and guidance that are relevant to IT security.*

50. Management should

- define, document, update, and approve the roles and responsibilities for all positions that support IT security, including backup support for key positions; and
- always communicate its IT security governance framework promptly to all staff once management approves changes to the framework.

Management's response. *Agreed. Roles and responsibilities for all positions that support IT security have now been prepared, defined, documented, updated, and approved by management. Management communicated the new IT security governance framework to all staff on 30 June 2017 and will continue to communicate with staff when governance changes arise.*

Management addressed identified risks

Why this finding matters

51. Having effective IT security controls is essential for ensuring that the Office can protect its assets and sensitive information. Because of the weaknesses presented in our previous findings, it is important that IT security management implement its action plan as designed to improve controls to address known risks.

What we examined

52. We looked at whether the Office had an internal reporting process that was clear, relevant, understandable, useful, and timely for reporting on IT security.

53. We reviewed management's action plan in response to the observations in the self-assessment. We assessed whether the actions aligned with the observations and whether management planned to perform them on a timely basis.

54. Our findings discuss the following topics:

- Risk assessment and internal reporting
- Action plan

Findings

55. **Risk assessment and internal reporting.** We looked at the risk register of the Office's Information Systems and Technology services for fall 2015 and 2016. The IT security risks identified in fall 2015 were in place for most of our audit period. We also examined the risks identified in fall 2016, since they were part of our audit period.

56. In fall 2015, management assessed IT security as having a high **inherent risk**. However, management determined that it had the controls in place to reduce this risk to an acceptable **residual risk**. On the basis of the preliminary results of the self-assessment, management observed that, in many cases, the controls seemed to be ineffective. As a result, management revised the risk assessment results for 2016. IT security still had a high inherent risk, but because some controls were ineffective, management raised the residual risk for IT security to high.

57. We found that IT security management promptly informed Office management of the changes in the residual risk for IT security. In addition, IT security management promptly briefed Office management on the initial results of the self-assessment. In fall 2016, the Deputy Departmental Security Officer certified to Office management that IT security was currently not at an acceptable level for the Office. In January 2017, the Deputy Departmental Security Officer also briefed members of the Office's Audit Committee on the results of the self-assessment.

58. Office management decided to include IT security as a significant risk in the 2016 corporate risk register. The Office made IT security part of its 2017–18 strategic priorities and committed to monitoring IT security.

Inherent risk—The risk prior to taking into account existing controls and any existing risk responses.

Residual risk—The risk after taking into consideration the risk mitigation measures and controls that are in place.

59. Each year, IT security management reports to Office management on security incidents or instances of non-compliance with IT security policies. There were no IT security incidents reported during the period covered by our internal audit. IT security management used the same process to internally report IT security incidents that it used for external reporting (see paragraph 45). As we already noted, this process document was a draft and had not been updated. The Departmental Security Officer informed us that he would promptly inform Office management if there was a significant IT security breach.

60. We also noted that IT security management provided relevant, understandable, and clear information on IT security to Office staff in a timely manner when IT security could affect their day-to-day work.

61. **Action plan.** For all the deficiencies identified in its self-assessment, IT security management established an action plan, including who was responsible for its implementation and a target date for remediation. IT security management also presented this action plan to Office management.

62. We reviewed management's action plan. On the basis of our review, we believe that implementing the action plan will address the weaknesses that management identified in its self-assessment. Because of these weaknesses, it is important that management implement the plan as designed. We will follow up on management's action plan.

Conclusion

63. We concluded that the Office of the Auditor General of Canada (Office) had designed an adequate framework to support the security of its information technology (IT) systems. However, the Office's management of the IT security framework hindered its effectiveness. Specifically, IT security management had not systematically reviewed its policies, procedures, and guidelines, and it had not implemented many controls required by the Treasury Board's policy instruments and guidance that were relevant to IT security.

About the Internal Audit

The Practice Review and Internal Audit team of the Office of the Auditor General of Canada (Office) provides the Auditor General with independent and objective information, advice, and assurance. The team's efforts add value to the Office by improving audit practices and Office operations and by encouraging learning and continuous improvement.

The internal audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada, which conform to the Institute of Internal Auditors Standards. The Office plans to conduct a practice inspection by 31 March 2018.

As part of our regular audit process, we obtained management's confirmation that the audit report is factually accurate.

Audit objective

This internal audit focused on whether the Office of the Auditor General of Canada had an adequate and effective framework to support information technology (IT) security.

Systems and practices examined, and criteria

At the beginning of this internal audit, we presented the Office's Audit Committee with an audit plan summary that identified the systems and practices, and related criteria, that we considered essential for examining how the Office manages IT security.

The following table outlines the systems and practices, as well as the criteria that we used for our internal audit.

We selected the criteria for this internal audit on the basis of the Treasury Board's policy instruments and guidance that were relevant to IT security and on our professional standards and knowledge of the subject matter.

Management reviewed and accepted the suitability of the criteria used in the internal audit.

Criteria

Criteria	Sources
To determine whether the Office of the Auditor General of Canada (Office) had an adequate and effective framework to support information technology (IT) security, we used the following criteria:	
The Office's IT security framework is well established and consistent with relevant governmental policies and guidelines on IT security.	• Policy on Government Security, Treasury Board
The Office has a governance structure with clear roles and responsibilities for IT security: • Accountabilities, delegations, reporting relationships, and roles and responsibilities are defined, documented, and communicated to relevant persons. • Those charged with governance have clearly communicated mandates, are actively involved, and oversee management processes. • The oversight body meets regularly and reviews information related to IT security priorities and plans, provides advice on issues, reviews the performance of the IT security function, and communicates its decisions to the organization in a timely manner.	• Policy on Government Security, Treasury Board
The Office's IT function has adequate reporting mechanisms that are clear, relevant, understandable, useful, and timely.	• Policy on Government Security, Treasury Board
The Office has IT security management controls or technical safeguards that protect IT assets and information and ensure secure and uninterrupted service delivery.	• Operational Security Standard: Management of Information Technology Security (MITS), Treasury Board
The Office has an action plan with deliverables and timelines for implementing its security management controls or technical safeguards and measuring the plan's progress.	

Period covered by the internal audit

The internal audit covered the systems and practices that were in place between 1 January 2016 and 30 November 2016. We extended the audit period to 31 March 2017 to review only the completed action plan that IT security management had provided on 24 March 2017.

Audit team

Chief Audit Executive: Louise Bertrand
Director: Marc Gauthier

List of Recommendations

The following table lists the recommendations and responses found in this report. The paragraph number preceding the recommendation indicates the location of the recommendation in the report.

Recommendation	Response
48. Management should monitor its implementation of the Treasury Board's policy instruments and guidance that are relevant to information technology (IT) security once they are issued and, if needed, take corrective action in a timely manner.	**Management's response.** Agreed. As part of the IT security self-assessment action plan of the Office of the Auditor General of Canada (Office), the IT security team has identified and will take all corrective actions that need to be implemented to ensure compliance with the Treasury Board's policy instruments and guidance that are relevant to IT security once they are issued.
49. Management should annually assess its IT security procedures, standards, and guidelines to ensure that they are up to date and in line with the Treasury Board's policy instruments and guidance that are relevant to IT security once they are issued. This assessment should include monitoring compliance with requirements.	**Management's response.** Agreed. As part of the IT security self-assessment action plan, new procedures, standards, and guidelines are being developed. A process is also being developed to ensure that the Office's IT security policies, procedures, and guidelines are reviewed annually to ensure that they are up to date and compliant with the Treasury Board policy instruments and guidance that are relevant to IT security.
50. Management should • define, document, update, and approve the roles and responsibilities for all positions that support IT security, including backup support for key positions; and • always communicate its IT security governance framework promptly to all staff once management approves changes to the framework.	**Management's response.** Agreed. Roles and responsibilities for all positions that support IT security have now been prepared, defined, documented, updated, and approved by management. Management communicated the new IT security governance framework to all staff on 30 June 2017 and will continue to communicate with staff when governance changes arise.