Government of Canada Gouvernement du Canada

Internal Audit – Specific Cyber Security Controls

ℹ Please note that in the spirit of the Access to Information Act, some information within this document cannot be disclosed for reasons related to the vulnerability of structures or systems, including computer or communication systems.

Final Report
Audit, Evaluation, and Risk Branch
March 2023

On this page

Executive summary

From the period of April 1, 2021, to March 31, 2022, the Canada Revenue Agency (CRA) administered over $586.3 billion in revenues and pension contributions, with 91% of individual and 94% of corporation income tax returns filed digitally. The CRA was able to offer 89% of its tax services online for individuals and businesses.

The CRA has one of the largest information technology (IT) environments and repositories of personal and financial information in the Government of Canada. The CRA has been using IT since 1960 and has been able to adapt to the need of Canadians as they increasingly use and rely on digital services. The CRA has adapted to evolving while safeguarding CRA information, which is critical to achieving the CRA's priorities.

The objective of the audit was to provide the Commissioner, CRA management, and the Board of Management with assurance that the controls are in place and working as intended to safeguard the CRA's IT systems from being compromised by a digital attack.

The CRA's cyber security posture covers hundreds of key controls and this audit covered a sub-set of those controls that were deemed higher risk through a risk assessment that was conducted during the planning phase of the engagement in Q4 of 2021-2022.

The audit found that improvements are required in the following areas in order to reduce the risks of the CRA's IT systems from being compromised by a digital attack:

- [content protected]
- [content protected]

The audit did not look at all the controls included in the cyber security program and is not forming an opinion on the overall cyber security posture of the CRA. However, successfully implementing action plans to address the recommendations provided in the report will effectively support the compliance, monitoring, and reporting of the Agency Cyber Security program.

As a best practice, both the Institute of Internal Auditors and the Information Systems Audit and Control Association recommend having three lines of defences for key functions such as cybersecurity.

Summary of recommendations

- The Security Branch should establish a second line of defence for cybersecurity to evaluate and monitor the internal controls related to cyber security. The Audit, Evaluation and Risk Branch recommends that this function undertake the following activities:
  - review and update corporate policy instruments to align them with the Treasury Board Policy on Service and Digital.
  - [content protected]

    - [content protected]
    - [content protected]
    - [content protected]
- [content protected]

Management response

The Security Branch agrees with the findings in this report. The Security Branch is of the opinion, which the AERB shares, that the audit did not reveal any vulnerabilities that could leave the CRA open to immediate attack and compromise. In the Security Branch's view, however, the audit was very valuable in that it uncovered symptoms of a larger cyber governance gap at the CRA. Its action plan will close this gap while addressing the audit's individual findings.

The big picture context of the audit findings

The audit revealed six individual controls for improvement. To put this in context, the Government of Canada's cyber security risk management model comprises hundreds of such controls that work together in a layered fashion. This paradigm of –"defence in depth"- puts in place layers of different types of risk controls (technical, managerial, administrative, etc.,) to help the CRA, as per the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF): IDENTIFY threats to the organization; put in place defences to PROTECT against these threats; DETECT if the threats have penetrated its defences; RESPOND effectively if they have; and RECOVER from any incident.

[content protected]

[content protected]

Figure 1:[content protected]

A growing culture of audit in the security branch

The Security Branch has been working to build a culture of audit into its business practices. Over the past 18 months, in addition to two separate internal audits, the Security Branch conducted several self-audits against the National Institutes of Standards and Technology (NIST) Cyber Security Framework. These included a detailed audit, which Gartner scored, and the Treasury Board Secretariat annual "Cyber Security Maturity Assessment". In January 2023, the Organisation for Economic Co-operation and Development's Global Forum conducted an extensive audit of the Security Branch's information security controls. They concluded their audit without any recommendations for the CRA. Every three years the CRA engages a third-party consultant to take a comprehensive look at its overall cyber security maturity. In 2022, cyber experts at Forrester placed the CRA in the middle of the pack in terms of industry. The Security Branch will present the findings of the Forrester audit, and its action plans, to the Board of Management in June 2023. Each quarter the Security Branch also conducts a review of Shared Services Canada's vulnerability scans of the network layer for which they are responsible. The Security Branch works with SSC to remediate certain issues.

Finally, and perhaps most noteworthy of the Security Branch’s culture of audit, is the investment the branch has made in a dedicated cyber Red Team. This is a group of technical experts who try to hack into the CRA’s systems as an adversary might do. To the Security Branch’s knowledge, this team is the first of its kind in a government line department and it has successfully highlighted cyber weaknesses in CRA defences and in those of the government as a whole.

Key audit recommendation: establish a governance, risk and compliance capacity in the security branch

Notwithstanding the above, the current internal audit and coincidentally, the Forrester third- party audit suggested the need for the Security Branch to further improve its continuous assurance work. To this end, internal audit recommended the creation of a Governance, Risk and Compliance capacity within the branch to evaluate and monitor the internal controls related to cyber security.

The Security Branch agrees with this recommendation and sees a formal GRC capacity as a "second line of cyber defence" under the well-known "Three Lines of Defence" (or 3LoD) governance model. The first line of the CRA's cyber defence will continue to be the operational management in the Security Branch's Cyber and Information Security Directorate (CISD). The directorate will continue to have ownership, responsibility and accountability for directly assessing, controlling and mitigating cyber and information security risks.

A new second line of defence will be established by March 2024 and will comprise a Governance, Risk and Compliance (or "Assurance") team. It will oversee cyber policies, frameworks, tools and techniques to facilitate CISD's management of cyber risks. It will also examine how effectively the CRA measures cyber risk and whether the controls in place are working as intended. Finally, it will facilitate the flow of cyber risk information laterally and horizontally in the CRA and across other key government partners (e.g. Shared Services Canada, Canada Border Services Agency, the Canada Centre for Cyber Security, Employment and Social Development Canada, and others).

The third line of defence will, of course, continue to be the internal audit function within the Audit, Evaluation, and Risk Branch. The branch will ensure that the first two lines are operating effectively and advise how they can be improved.

In summary, the Security Branch agrees with the recommendations in this internal audit report and will address them in the context of a new Governance, Risk and Compliance function in the branch. The Security Branch has developed related action plans, and the Audit, Evaluation, and Risk Branch has determined that they appear reasonable to address the recommendations.

1. Introduction

The Canada Revenue Agency (CRA) has one of the largest information technology (IT) environments and repositories of personal and financial information in the Government of Canada. As Canadians increasingly use and rely on digital services, safeguarding the CRA's information is critical to achieving the CRA's priorities.

From the period of April 1, 2021, to March 31, 2022, 89% of the CRA's tax services were available online for individuals and businesses. The CRA administered over $586.3 billion in revenues and pension contributions, with 91% of individual and 94% of corporation income tax returns filed digitally. The CRA issued over $36 billion in federal and provincial benefits [1].

On March 11, 2020, the World Health Organization characterized COVID-19 as a pandemic. The CRA played a leading role in Canada's COVID-19 Economic Response Plan, taking unprecedented action to help Canadians and businesses facing hardship, while ensuring that any privacy implication was reviewed and mitigated [2].

The CRA administered the distribution of over $200 billion through 11 benefit programs, with another $19.4 million being administered in two remaining active benefit programs. More than 20.7 million Canadians received pandemic-related benefits in 2020 [3]. Offering digital services presents an opportunity to quickly deliver programs and benefits, but it also highlights the importance of having a robust cyber security framework to ensure that security risks are appropriately mitigated.

In late 2020, the CRA began steps to integrate all security functions under one branch. As of April 2022, the Agency Security Officer took on an increased role of providing oversight on all of the CRA's security obligations.

The CRA depends on a multi-layered cyber security architecture that includes protection of its outer perimeter by Shared Services Canada (SSC) and the Canadian Centre for Cyber Security, who are the main providers of the infrastructure security safeguards at the network and physical layer. As a third party, SSC is supplying services, which the CRA is mandated to use. In order to properly manage this interaction, the relationship with SSC is managed as a supply chain risk.

[content protected]

To further safeguard the electronic data stored by the CRA and to protect Canadians' personal information from being compromised, Budget 2021 proposed to provide $332 million over five years to the CRA, starting in fiscal year 2021 to 2022, and $51.2 million in ongoing funding to invest in new technologies and tools that match the growing sophistication of cyber threats, and to ensure the CRA's workforce has the specialized skills to proactively monitor threats and better safeguard Canadian data [4]. The CRA has an in-depth defence approach to security and does not rely on any single solution. It provides complementary safeguards associated with the endpoints and in the application and data layers.

2. Focus of the audit

This internal audit was included in the Board of Management (Board) approved 2021-2022 Risk-Based Assurance and Advisory Plan. The Assignment Planning Memorandum was approved by the Commissioner on June 14, 2022.

2.1. Importance

This audit is important because privacy breaches and cyber attacks that threaten sensitive data and assets can have grave consequences for organizations ranging from financial loss to reputational harm. As one of the largest holders of information in the Government of Canada, the protection of personal and taxpayer information is crucial to upholding the public's trust in the CRA. An effective cyber security posture is the culmination of security practices, staff training, and layered controls that must continually adapt to evolving persistent threats. This internal audit is linked to enterprise risks identified in the CRA's Corporate Risk Profile on the protection of taxpayer information and cyber security.

2.2. Objective

The audit objective was to provide the Commissioner, CRA management, and the Board with assurance that the controls are in place and working as intended to safeguard the CRA's IT systems from being compromised by a digital attack.

2.3. Scope

The audit covered the CRA's production systems, components, applications, supporting processes, and activities as of December 1, 2021. The scope of the audit was driven by the result of a risk assessment and also took into consideration work performed by other advisory and assurance providers to avoid duplication. Examples of audit tests conducted by the audit team included procedures to test:

- [content protected]
- [content protected]
- [content protected]
- [content protected]
- [content protected]

[content protected]

The scope excluded the following:

- management of infrastructure assets, such as mainframes, servers, networks, and cloud infrastructure under the management of Shared Services Canada
- areas where the internal controls would be changing with the initiation of new projects or initiatives
- networks and devices certified for information classified as Protected C or higher
- areas that were under review by other internal or external engagements, including:
  - the Credential Stuffing attack of August 2020 as the Office of the Privacy Commissioner of Canada began an investigation in October 2020; the investigation was still ongoing at the end of the examination phase in August 2022

  - the maturity of the Agency's IT security practices as the Security Branch engaged an external contractor to assess the current state and provide recommendations for improvement, specifically around the CRA Cyber Business Resiliency program

The period covered in this audit is from December 1, 2021, to August 31, 2022.

2.4. Audit criteria and methodology

The audit criteria and methodology can be found in Appendix A.

The examination phase of the audit took place from May 2022 to August 2022.

The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing, as supported by the results of the quality assurance and improvement program.

3. Findings, recommendations, and action plans

The recommendations presented in this report address issues of high significance or mandatory requirements.

The Security Branch and the Information Technology Branch agree with the recommendations in this report and have developed related action plans. The Audit, Evaluation, and Risk Branch has determined that they appear reasonable to address the recommendations.

3.1. Compliance

3.1.1. CRA policies, directives, standards, and procedures related to cyber security are defined, current, and communicated to stakeholders, but changes are required to align them with the Treasury Board Policy on Service and Digital.

The audit expected that CRA policies, directives, standards, and procedures related to cyber security would be defined, current, and communicated to stakeholders. They were also expected to be aligned with the Treasury Board Policy on Service and Digital.

In April 2022, the Security Branch was formed, a transition that is part of the evolution of security at the CRA, where the Agency Security Officer has taken on an increased role and provides oversight on all of the CRA's security obligations. In late 2020, the CRA began steps to integrate all security functions under the Agency Security Officer, who holds the rank of assistant commissioner, sits on all senior committees, and is responsible for leading all CRA security functions in collaboration with other senior officials in accordance with the Directive on Security Management. As of September 2021, the Agency Security Officer became fully accountable for all eight security controls listed in the Policy on Government Security as well as cyber security.

At the time of examination, the corporate policy instruments were being updated to reflect the organization changes and responsibilities generated by the creation of the Security Branch and the resulting transfer of responsibilities. The corporate policy instruments relating to cyber security are in place and communicated on the Security Branch InfoZone pages.

Some corporate policy instruments need to be updated to include the following new elements introduced by the Treasury Board Policy on Service and Digital that came into effect on April 1, 2020:

- Canadian data residency requirement
- authorization of devices connecting to CRA infrastructure

The CRA also has stricter controls in certain areas as it prohibits employees, consultants, and contractors from working outside of Canada for personal reasons (unless authorization is given by the commissioner) whereas the Treasury Board policies offer no guidance in this regard.

Recommendation 1

The Security Branch should establish a second line of defence for cybersecurity to evaluate and monitor the internal controls related to cyber security. The Audit, Evaluation, and Risk Branch recommends that this function undertake the following activities:

1.1. review and update corporate policy instruments to align them with the Treasury Board Policy on Service and Digital.
1.2. [content protected]
1.3. [content protected]
1.4. [content protected]
1.5. [content protected]

Action Plan 1.1

The internal audit correctly pointed out that CRA corporate policy instruments are not aligned to the Treasury Board Policy on Service and Digital and its accompanying directives. That said, the Security Branch wishes to emphasize that the CRA's practices are in fact aligned with the Policy on Service and Digital.

The Policy on Service and Digital replaced eight separate Treasury Board policies, and updating the CRA's corporate policy instruments will be an extensive administrative exercise requiring significant time for intra-Agency consultations and approvals on approximately 18 separate corporate policy instruments. The December 2024 date aligns with the Security Branch's original policy cycle review plans, which means it will not have to consult its stakeholders twice, causing them unnecessary work.

Target completion date to update the corporate policy instruments to align with the Policy on Service and Digital: December 2024.

3.1.2 [content protected]

[content protected]

Recommendation 1

The Security Branch should establish a second line of defence for cybersecurity to evaluate and monitor the internal controls related to cyber security. The Audit, Evaluation, and Risk Branch recommends that this function undertake the following activities:

1.1. review and update corporate policy instruments to align them with the Treasury Board Policy on Service and Digital.
1.2. [content protected]
1.3. [content protected]
1.4. [content protected]
1.5. [content protected]

Action Plan 1.2

[content protected]

3.1.3 [content protected]

[content protected]

Recommendation 1

The Security Branch should establish a second line of defence for cybersecurity to evaluate and monitor the internal controls related to cyber security. The Audit, Evaluation, and Risk Branch recommends that this function undertake the following activities:

1.1. review and update corporate policy instruments to align them with the Treasury Board Policy on Service and Digital.
1.2. [content protected]
1.3. [content protected]
1.4. [content protected]
1.5. [content protected]

Action Plan 1.3

[content protected]

3.1.4 [content protected]

[content protected]

Recommendation 1

The Security Branch should establish a second line of defence for cybersecurity to evaluate and monitor the internal controls related to cyber security. The Audit, Evaluation, and Risk Branch recommends that this function undertake the following activities:

1.1. review and update corporate policy instruments to align them with the Treasury Board Policy on Service and Digital.
1.2. [content protected]

1.3. [content protected]
1.4. [content protected]
1.5. [content protected]

Action Plan 1.4

[content protected]

3.1.5 [content protected]

[content protected]

Recommendation 1

The Security Branch should establish a second line of defence for cybersecurity to evaluate and monitor the internal controls related to cyber security. The Audit, Evaluation, and Risk Branch recommends recommend that this function undertake the following activities:

1.1. review and update corporate policy instruments to align them with the Treasury Board Policy on Service and Digital.
1.2. [content protected]
1.3. [content protected]
1.4. [content protected]
1.5. [content protected]

Action Plan 1.5

[content protected]

3.1.6 [content protected]

[content protected]

Recommendation 2

[content protected]

Action Plan 2

[content protected]

3.2. Monitoring and reporting

3.2.1 The Cyber Security Dashboard is evolving to ensure adequate cyber security information is provided to senior management and the Board.

The audit reviewed and assessed various iterations of the Cyber Security Dashboard presented to the Board of Management since the first quarter of 2021-2022.

During that same period, there were also other cyber security related reports whose metrics were not part of the dashboards and that were prepared and presented to CRA senior management and the Board.

The Cyber Security Dashboard has been evolving since the beginning of the internal audit through consultation with Board members on the adequacy of the dashboard elements.

The Cyber Security Dashboard is normally presented as a consent item at the quarterly meetings of the Board of Management. When a cyber security incident of interest occurs (such as the Log4j vulnerability), the Security Branch, the Information Technology Branch, and the Finance and Administration Branch are present to answer questions and to provide additional information.

A multitude of leading and lagging indicators are available but selecting the appropriate indicators to adequately state the CRA's overall cyber security posture is currently a work in progress. The audit assessed the accuracy and completeness of the information being provided in the dashboard and determined that the Security Branch was validating the data behind the indicators.

The content and the format of the Cyber Security Dashboard presented to CRA senior management and the Board for monitoring and oversight have been revised over the years to include more relevant performance key indicators aligned with the National Institute of Standards and Technology cyber security framework functions.

[content protected]

4. Conclusion

The audit found that the CRA did not have a second line of defence dedicated to cybersecurity. Setting up this function will allow the Security Branch to address improvements required in the following areas in order to reduce the risks of the CRA's IT systems from being compromised by a digital attack: [content protected] Successfully implementing action plans to address the recommendations provided in the report will effectively support the compliance, monitoring, and reporting of the Agency Cyber Security program.

5. Acknowledgement

In closing, we would like to acknowledge and thank the Security Branch, the Information Technology Branch, the Finance and Administration Branch, and the Legislative Policy and Regulatory Affairs Branch for the time dedicated and the information provided during the course of this engagement.

6. Appendices

Appendix A: Audit criteria and methodology

Based on the Audit, Evaluation, and Risk Branch's risk assessment and the evolution of security at the CRA, the following lines of enquiry were identified:

Lines of enquiry	**Criteria**	**Sub-criteria**
1. Compliance	**1.1** CRA policies, directives, standards, and procedures related to cyber security are defined, current, communicated to stakeholders, and align with those of the Government of Canada.	**1.1.1** Corporate policy instruments are defined.
		1.1.2 Corporate policy instruments are current.
		1.1.3 Corporate policy instruments are communicated.

Lines of enquiry	Criteria	Sub-criteria
		1.1.4 Corporate policy instruments align with the Government of Canada’s policies and guidance.
	1.2 Roles and responsibilities related to cyber security are defined, communicated, and understood by stakeholders.	[content protected]
	1.3 Systems and controls that ensure compliance with policies and procedures are working as intended.	[content protected]
2. Monitoring and reporting	**2.1** Cyber security performance indicators provide accurate and relevant information to support decision making.	**2.1.1** Cyber security monitoring activities are defined, in place, and reported in a timely manner.
		2.1.2 The objectives and key performance indicators provide sufficient information to accurately reflect the true state of cyber security.

Methodology

The methodology for examination included, but was not limited to, the following:

- reviewing and analyzing corporate policy instruments and supporting documentation related to cyber security
- conducting interviews with Security Branch and Information Technology Branch management and staff as well as selected branch business owners
- reviewing control outcomes and documentation
- reviewing and analyzing data from supporting security applications and tools
- reviewing IT incident reports and related documents
- reviewing and analyzing performance indicators and monitoring reports for accuracy and consistency

Appendix B: Glossary

Term	Definition
[content protected]	[content protected]
[content protected]	[content protected]
[content protected]	[content protected]

Term	Definition
Cloud computing	The use of remote servers hosted on the Internet. Cloud computing allows users to access a shared pool of computing resources (such as networks, servers, applications, or services) on demand and from anywhere. Users access these resources via a computer network instead of storing and maintaining all resources on their local computer.
Cloud vendor	An organization that sells computing infrastructure, software as a service, or storage.
Confidentiality	The ability to protect sensitive information from being accessed by unauthorized people.
[content protected]	[content protected]
Cyber attack	The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.
Cyber Security Dashboard	A dashboard for executive cyber security metrics ensures that leadership teams can monitor security and vulnerabilities of company infrastructure and applications.
Cyber threat	A threat actor, using the Internet, who takes advantage of a known vulnerability in a product for the purposes of exploiting a network and the information the network carries.

Term	Definition
[content protected]	[content protected]
[content protected]	[content protected]
[content protected]	[content protected]
[content protected]	[content protected]
Integrity	The ability to protect information from being modified or deleted unintentionally or when it’s not supposed to be. Integrity helps determine that information is what it claims to be. [content protected]
Local Application Repository	A national repository of information for all local solutions developed internally within the CRA.
Log	A chronological record of actions, performances, computer/network usage, and events that occur in a computer system, such as problems, errors, or information on current operations.
[content protected]	[content protected]
[content protected]	[content protected]
[content protected]	[content protected]

Term	Definition
Safeguard	Protective measure prescribed to meet the security requirements (that is, confidentiality, integrity, and availability) specified for an information system. Safeguards can include security features, management constraints, personnel security, and security of physical structures, areas, and devices.
Security control	A management, operational, or technical high-level security requirement needed for an information system to protect the confidentiality, integrity, and availability of its IT assets. Security controls can be applied using a variety of security solutions, including security products, security policies, security practices, and security procedures.
[content protected]	[content protected]
[content protected]	[content protected]
[content protected]	[content protected]
Supply chain	Refers to the processes required to design, manufacture, and distribute equipment or other commodities, including IT hardware and software. The stages of this complex process often involve different entities.
[content protected]	[content protected]

Term	Definition
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited to adversely affect an organization’s assets or operations.

[1] 2021-2022 Departmental Results Report

[2] 2019-2020 Departmental Results Report

[3] 2021 Census, Analytical products

[4] Budget 2021, Protecting Taxpayer Information

Date modified:
2023-12-12