# Internal Audit – Security Assessment and Authorization

Final Report

Audit, Evaluation, and Risk Branch

January 2023

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.

## On this page

# Executive summary

As cyber threats grow in sophistication and magnitude, the Canada Revenue Agency (CRA) must manage a wide range of security risks in a rapidly changing environment. A cyber attack can disrupt the availability of digital services and threaten the security of information that taxpayers and benefit recipients have submitted to the CRA. **Security assessment and authorization** is an essential process for the information technology (IT) security function to establish and maintain confidence in the security of information systems that are used or managed by the CRA, while considering the business needs for security.

This internal audit covered the current security assessment and authorization process in place within the Security Branch, which is responsible for establishing security governance at the CRA. The Security Branch is also responsible for overseeing the IT and electronic data security elements of the security program. In conjunction with process stakeholders in branches, the Security Branch assesses the security posture of all IT projects and ensures IT security-related residual risks associated with the programs, services, and operations are assessed and appropriately approved to operate.

The objective of the audit was to provide the Commissioner, CRA management, and the Board of Management with assurance that the security assessment and authorization requirements are in place and working as intended.

Overall, the internal audit team found that the security assessment and authorization process and requirements for information systems were in place for security assessments. However, the internal audit team found that improvements are needed to further strengthen corporate policy instruments, roles and responsibilities, authorization, the monitoring of performance indicators, and the development of formal procedures and tools in order to support the needs of the CRA.

## Summary of recommendations

- The Security Branch should ensure that corporate policy instruments are reviewed, updated, and communicated to reflect the creation of the Security Branch and that they are aligned with current Government of Canada policies.
- The Security Branch should develop procedures, guidelines, standards, tools, and awareness as part of its security assessment and authorization process to:
    - support process stakeholders on the completeness and effectiveness of security assessment and authorization supporting documentation for assessments and risk management activities
    - incorporate Government of Canada guidance on cloud security risk management activities into assessment and monitoring procedures
    - ensure requirements are in place to implement tools to effectively manage the security assessment and authorization process

- The Security Branch, in consultation with the Information Technology Branch (ITB), should ensure security assessment and authorization roles, responsibilities and criteria are communicated and understood by process stakeholders and integrated early during the planning for non-gated IT projects and substantially changed systems and should consider formalizing the integration of the security assessment and authorization as part of the IT work order management process.
- The Security Branch should update its current processes and procedures to ensure authorization has been obtained and documented for all applications, systems, and components prior to going into production.
- The Security Branch should develop a CRA-wide systems authorization centralized monitoring strategy to maintain authorization and to document risk-based security decisions.
- The Security Branch, in consultation with the ITB and stakeholders, should ensure inventories, tools, and supporting documentation are accurate and complete in order to prioritize the review of applications, systems, and components for authority to operate.
- The Security Branch should develop monitoring mechanisms to ensure the timely completion of safeguard implementation plans, the reporting on the compliance to the security assessment and authorization process, and the continuous effectiveness of security controls.

## Management response

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

# 1. Introduction

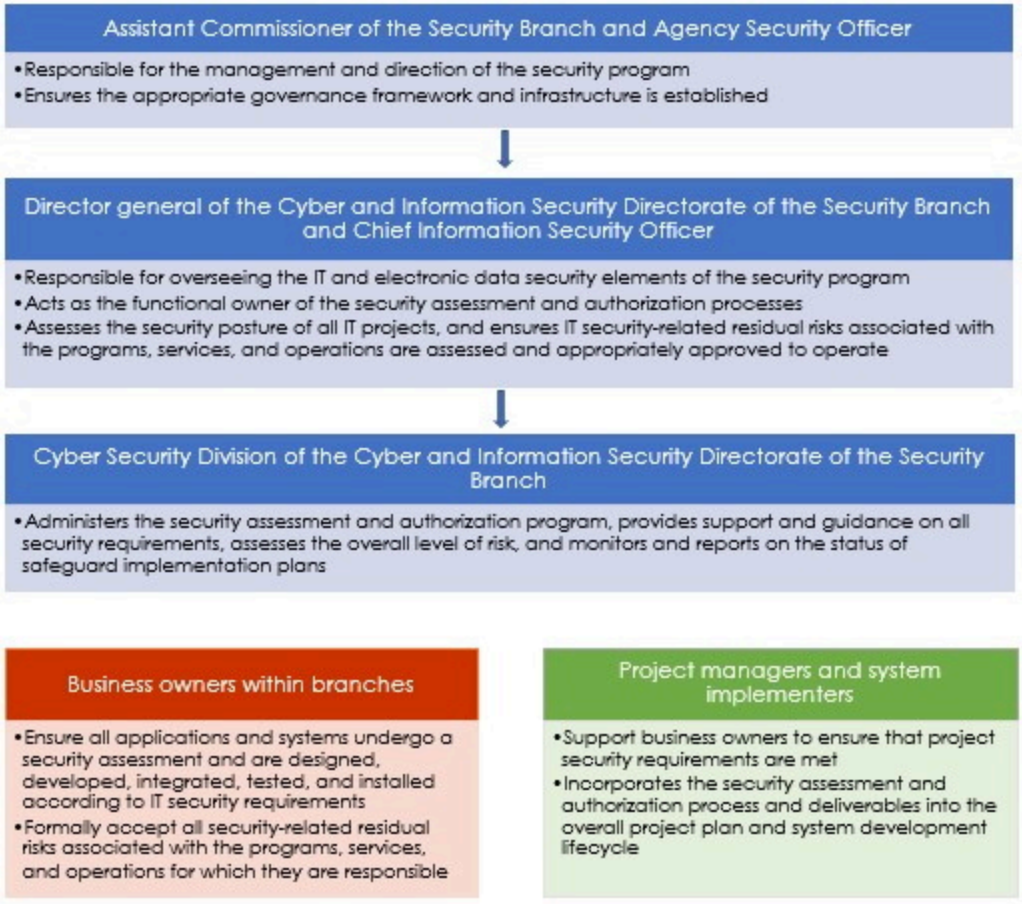
The Canada Revenue Agency (CRA) contributes to the economic and social well-being of Canadians and to the efficiency of government by delivering world-class tax and benefit administration that is responsive, effective, and trusted [1]. One of the CRA's priorities is to improve the client-centric service experience by transforming the digital services it delivers to Canadians while maintaining and building the public's trust. As Canadians increasingly use and rely on digital services, the CRA has one of the largest IT environments and repositories of personal and financial information in the Government of Canada. In fiscal year 2020 to 2021, 90.2% of income tax and benefit returns and 94.2% of corporation income tax returns were filed digitally [2].

IT security requires enterprise-wide governance and sustained effort and diligence to ensure the implementation of safeguards to preserve the confidentiality, integrity, availability, intended use, and value of electronically stored, processed, or transmitted information. An effective security risk management approach to security controls must be established, monitored, maintained, and reviewed with timely corrective measures taken when issues are identified.

As cyber threats grow in sophistication and magnitude, the CRA, in partnership with Shared Services Canada and lead security agencies, must ensure that it manages a wide range of security risks in a rapidly changing environment. A cyber attack can disrupt the availability of digital services and threaten the security of information that taxpayers and benefit recipients have submitted to the CRA. It is essential for the CRA to meet Canadians' expectations for delivering client service while maintaining trust that their information will be protected from potential data breaches and identity theft.

Security assessment and authorization is an essential process for the IT security function to establish and maintain confidence in the security of information systems that are used or managed by the CRA, while considering the business needs for security. Security assessment is the ongoing process of evaluating security practices and controls to establish the extent to which they are implemented correctly, operating as intended, and achieving the desired outcome with respect to meeting defined security requirements. Security authorization is the ongoing process for obtaining and maintaining a security risk management decision and to explicitly accept the related residual risk with the authority to operate, based on the results of the security assessment. This is done in parallel with the CRA's system development lifecycle to facilitate secure system design for the protection of information and services. In 2013, the CRA approved the initial Directive for Security Assessment and Authorization in alignment with the CRA Security Program Policy Framework, the Security Policy, the Information and Systems Security Directive.

In fiscal year 2021 to 2022, the CRA created the Security Branch, bringing the functional security programs together to ensure a coordinated approach to continue protecting its people, information, and assets, and to ensure security risks are managed proactively and continuously. IT security and security assessment and authorization are shared responsibilities within the CRA, as detailed below.




▼ Text version of Figure 1

Figure 1 above illustrates the reporting relationships between the senior management positions and the division in the Security Branch who are responsible for IT Security and Security Assessments. It also shows the responsibilities of key stakeholders involved in the process such as Business Owners within branches and Project managers and system implementers.

Branch business owners ensure that all applications and systems undergo a security assessment and are designed, developed, integrated, tested, and installed according to IT security requirements. They are also responsible for formally accepting all security-related residual risks associated with the programs, services, and operations for which they are responsible.

Project managers and system implementers support business owners to ensure that project security requirements are met and incorporate the security assessment and authorization process and deliverables into the overall project plan and system development lifecycle.

The Cyber Security Division of the Cyber and Information Security Directorate of the Security Branch administers the security assessment and authorization program, provides support and guidance on all security requirements, assesses the overall level of risk, and monitors and reports on the status of safeguard implementation plans.

Director general of the Cyber and Information Security Directorate of the Security Branch and Chief Information Security Officer is responsible for overseeing the IT and electronic data security elements of the security program, and acts as the functional owner of the security assessment and authorization processes. He is also responsible for assessing the security posture of all IT projects, and ensures IT security-related residual risks associated with the programs, services, and operations are assessed and appropriately approved to operate.

The Director General of the Cyber and Information Security Directorate reports to the Assistant Commissioner of the Security Branch and Agency Security Officer who is responsible for the management and direction of the security program ensures that the appropriate governance framework and infrastructure is established.

As the CRA continues to look at the delivery of new digital services and emerging technologies, it is essential that IT security is integrated at the earliest stages of new programs and initiatives and in the design of secure and reliable information systems.

# 2. Focus of the audit

This internal audit is included in the most recent Board of Management (Board) approved Risk-Based Assurance and Advisory Plan 2021-2022. The Assignment Planning Memorandum was approved by the Commissioner on January 26, 2022.

## 2.1. Importance

Privacy breaches and cyber attacks that threaten sensitive data and assets can have grave consequences for organizations ranging from financial loss to reputational harm. Security assessment and authorization is an essential practice that ensures security is integrated early to new programs and risks are identified and appropriately managed for the CRA's systems, components, and applications. This audit is linked to enterprise risks identified in the CRA's Corporate Risk Profile on the protection of taxpayer information and cybersecurity.

## 2.2. Objective

The objective of the audit was to provide the Commissioner, CRA management, and the Board with assurance that the security assessment and authorization requirements were in place and working as intended.

## 2.3. Scope

The audit covered the CRA's production systems, components, applications, supporting processes, and activities as of December 31, 2021.

The audit team conducted interviews within Headquarters with the Security Branch, the ITB, the Assessment, Benefit, and Service Branch, the Appeals Branch, the Collections and Verification Branch, and the Compliance

Programs Branch.

Infrastructure assets, such as mainframes, servers, networks, and cloud infrastructure under the management of Shared Services Canada were outside the scope of this audit.

## 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 December 2021 to May 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.

## 3.1. Compliance

### 3.1.1 Corporate policy instruments are in place and communicated; however, given the recent re-organization of the Finance and Administration Branch and the creation of the Security Branch, they are not current or aligned with Government of Canada policies.

The Security Branch has reviewed, published, and communicated corporate security policy instruments relevant to security assessment and authorization.

At the time of examination, corporate policy instruments were not current due to the establishment of the Security Branch and were also not aligned to current Government of Canada policies. In particular, corporate policies instruments did not reflect the expanded responsibilities of the new Agency Security Officer and referenced outdated Government of Canada policies. In addition, the Directive on Security Assessment and Authorization was not updated to reflect the Security Branch as the functional owner. This could lead to unclear governance and accountabilities to ensuring IT security risks are appropriately managed for CRA programs, services and operations and the protection of people, information, and assets. The internal audit team reviewed plans for draft corporate policies instruments to be updated by the Security Branch which was not in place at the time the audit was concluded.

## Recommendation 1

**The Security Branch should ensure that corporate policy instruments are reviewed, updated, and communicated to reflect the creation of the Security Branch and that they are aligned with current Government of Canada policies.**

Action Plan 1

The Security Branch will work with stakeholders to update the Directive on Security Assessment and Authorization to reflect the creation of the Security Branch and to ensure the directive is aligned to the current Government of Canada policies.

The target completion date for this action plan is October 2023.

## 3.1.2 Stakeholder roles and responsibilities are defined and communicated; however, opportunities exist to ensure they are understood by all stakeholders involved in the security assessment and authorization process.

Roles and responsibilities regarding the management of security assessment and authorization within the CRA are clearly defined and published within corporate policy instruments.

However, the internal audit team identified opportunities to ensure roles and responsibilities were understood. Interviews with stakeholders noted that they were not always aware of or did not clearly understand the security assessment and authorization process, more specifically for monitoring, and particularly stakeholders who were not recently involved with conducting a security assessment and authorization or who were new to their respective role. A number of factors were indicated as causes for a lack of understanding by inexperienced stakeholders, including turnover in key stakeholder roles, lack of security assessment and authorization training, and limited communication and outreach to stakeholders. This situation could lead to inconsistent compliance with legislative and policy requirements and the potential loss of protected and classified information.

## See recommendation 1 and 3.

## 3.1.3 Security assessments for information systems are in place; however, opportunities exist to improve formalized procedures, guidelines, standards, awareness and tools to effectively manage the security assessment and authorization process.

Security assessments ensure that systems are designed, developed, configured, and implemented with a proper security posture, and they provide the basis for trust in CRA systems by a variety of users, including staff, clients, partners, and taxpayers. CRA corporate policy instruments state that the Security Branch must document an approved security assessment and authorization process that provides adequate security assurance of CRA systems and software to allow informed authorization decisions.

The internal audit team noted that a high-level security assessment and authorization process was documented and available. Details of the security assessment and authorization process were documented in various locations, including on the CRA's intranet and internal wiki pages, workflow diagrams, and various templates. Based on a sample of 10 security assessments completed between fiscal year 2020 to 2021, documentation was generally in place to support security assessment reports and were completed by a security assessor. The security assessment reports included identified risks and recommendations to correct deficiencies. These reports were appropriately approved by the director of the Cyber Security Division, within the Security Branch. At the time of examination, the Security Branch was revising the security assessment and authorization process as part of a process improvement exercise and an initiative to review and implement a commercial-off-the-shelf solution to support the security processes.

The internal audit team identified that the security assessment and authorization process lacked formalized and centralized procedures and guidelines. This could be improved to ensure completeness and appropriate sign-offs on supporting documentation and vulnerability scans, development of consistent templates for assessment and risk calculation,

and incorporation of Government of Canada (GC) guidance on cloud security risk management activities into assessment and monitoring procedures.

The internal audit team also identified that tools, such as [content redacted] and reporting spreadsheets, were in place; however, these locally developed solutions do not meet the needs of the security assessment and authorization process around tracking, risk monitoring and reporting functionality.

In addition, stakeholder awareness of the security assessment and authorization process is based on prior experience, and new stakeholders and project managers faced difficulties in understanding the security assessment and authorization process due to a lack of training. Addressing security in the early stages of IT projects and throughout the information system's lifecycle is vital to ensuring that security is integrated into the design, that security objectives are met, and that planning and resources are optimized. Although the security assessment and authorization process was integrated into the project management process, specifically the ITB Project Gate Assessment framework for major IT projects, small IT projects or system enhancements are not always required to follow the framework. There was also a lack of clarity from stakeholders on the guidelines and triggers to proactively engage the Security Branch early in the planning process and understanding the definition of a substantial change as part of the criteria for re-assessment. As a result, small IT projects or system enhancements were not always integrated into security assessment and authorization considerations early, which could lead to undependable service operations, delays in implementing new services, insufficient resource allocation, and security vulnerabilities without proper security risk considerations.

## Recommendation 2

**The Security Branch should develop procedures, guidelines, standards, tools, and awareness as part of its security assessment and authorization process to:**

- **support process stakeholders on the completeness and effectiveness of security assessment and authorization supporting documentation for assessments and risk management activities**
- **incorporate Government of Canada guidance on cloud security risk management activities into assessment and monitoring procedures**
- **ensure requirements are in place to implement tools to effectively manage the security assessment and authorization process**

Action Plan 2

Early 2022, the Security Branch initiated a review of its internal workflows and processes to identify items for improvement. The security assessment and authorization improvement goal was to improve consistency, reusability, and repeatability of the process. In addition, a strong push was done toward increasing efficiency and agility with the intent to improve the quality of the assessment, and enable the organization to improve the integration of cybersecurity early in the development lifecycle (design-in security). The Security Branch will review and develop consistent and formalized security assessment and authorization process, detailed procedures, guidelines, tools, and awareness training material for the internal security assessment and authorization workflows. In addition, the Security Branch will support stakeholders with managing effectively the security assessment and authorization supporting documentation for assessments and risk management activities; as well as incorporate Government of Canada guidance on cloud security activities into assessment and monitoring procedures.

The Security Branch will ensure requirements are in place to continue implementation of supporting tools to effectively manage the security assessment and authorization process.

The target completion date for this action plan is December 2023.

## Recommendation 3

**The Security Branch, in consultation with the ITB, should ensure security assessment and authorization roles, responsibilities and criteria are communicated and understood by process stakeholders and integrated early during the planning for non-gated IT projects and substantially changed systems and should consider formalizing the integration of the security assessment and authorization as part of the IT work order management process.**

Action Plan 3

The Security Branch will work with the stakeholders to update the Directive on Security Assessment and Authorization to reflect changes to the roles and responsibilities based on the creation of the Security Branch. As part of this process, the stakeholders are consulted for awareness and feedback on changes. Once the updates are completed and approved, the Security Branch will work with the appropriate teams to publish an Agency News item on InfoZone to communicate the changes.

The target completion date for this action plan is March 2023.

The Security Assessment and Authorization Improvement Project marked a turning point, where continuous improvements, self-evaluation, and adjustments have become the norm. As part of this initiative, the security assessment and authorization intake process was reviewed, a security assessment and authorization tiers methodology was implemented,

underlying workflows were reviewed, and security assessment and authorization templates used for day-to-day operations were streamlined and updated.

Security Patterns were created to have a “design-in” approach rather than reactive to the security assessment. As the changes are being implemented, gradual improvement is expected to be revealed in current outstanding security assessment and authorization projects.

The number of security assessment and authorization requests are increasing exponentially, therefore the Security Branch will increase its coordination presence via its security assessment and authorization intake process to ensure its security deliverables are completed on target dates. This measure will ensure stakeholders understand well the security assessment and authorization roles and responsibilities within gated and non-gated projects and bring additional awareness of the security assessment and authorization process improvements to ITB. Furthermore, this will open discussions on better integration of the security assessment and authorization process components within the IT work order management process.

The target completion date for this action plan is December 2023.

## 3.1.4 Authorities to operate for information systems in the production environment is not always current, documented, appropriately approved, and consistently maintained throughout the operational lifecycle.

Authorization, or authority to operate, is a critical ongoing step in the security assessment and authorization process. It is the official decision and formal acceptance of the risks documented in the security assessment

report by a designated authority to approve an information system for operational use in the production environment throughout the operational lifecycle.

The internal audit team found that the authority to operate for information systems in production was not always current, documented, or appropriately approved. In a review of 10 completed security assessments in calendar year 2020 to 2021, the internal audit team found five cases where authorization was either not appropriately retained or not signed off by the respective business owners as required by policy. The internal audit team also noted an occurrence where authorization was not signed prior to production dates as required by CRA policy.

The internal audit team also reviewed existing production enterprise applications and could not determine if a security assessment and authorization was in place or retained for all applications, systems, components, and supporting infrastructure. Specifically, the internal audit team found information management and data integrity issues with tools in the Solutions Application Catalogue inventory, the [content redacted], and periodic review spreadsheets. The internal audit team also found that not all enterprise applications could be readily traced back to a signed authority to operate or to an older threat and risk assessment due to a lack of management oversight and a lack of an appropriately managed centralized repository. Some business or support areas were also not aware or did not retain supporting documentation of the current security assessments or authorization.

In addition, the internal audit team noted that the Security Branch documents the high-level step for ongoing monitoring and the need to maintain authorization as threats and risks to the information systems and business environment continue to evolve over time. The internal audit team found that there was a lack of formalized monitoring procedures for

stakeholders. Also, not all stakeholders perform consistent monitoring to maintain authorization throughout the information system's operational lifecycle. Based on a review of the Application Portfolio Management survey in 2021, a number of respondents did not consistently review or were unaware of the adequacy of the security assessment and authorization or older threat and risk assessment to meet business needs.

Through interviews, the internal audit team noted that various IT security activities were performed, including several application areas with security assessment updates related to releases and major IT projects, specific local activities, or particular controls that included the management of security risks and vulnerabilities; however, these activities were not documented or reported as part of a consistent and formalized security assessment and authorization approach. The internal audit team noted that some application areas were not always engaged by the Security Branch or aware of specific monitoring requirements and noted the lack of guidance and ability to centrally report and document results of the completed review to maintain authorization throughout the information system's operational lifecycle.

The lack of an appropriate process for obtaining and maintaining authorization could result in outdated security assessments and changes and risks that might not be proactively managed, leading to the potential for new security vulnerabilities and a disruption in critical services for taxpayers.

## Recommendation 4

**The Security Branch should update its current processes and procedures to ensure authorization has been obtained and documented for all applications, systems, and components prior to going into production.**

Action Plan 4

Early 2022, the Security Branch initiated a review of its internal workflows and processes to identify items for improvement. As part of this initiative, the authority to operate tracking, processes, and associated residual risks to the organization was in scope.

While the Security Branch can only ensure that an authority to operate is provided after a system security assessment, some gaps were identified during the intake process relevant to the templates used and authority to operate processes. As a result, the Security Branch identified there was insufficient security assessment and authorization awareness and proper project integration of security assessment and authorization deliverables within the project planning; therefore, it may have resulted the system being put in production without formal authorization as they did not channel through the security assessment and authorization intake process. Changes were implemented in June 2022. More will be completed with respect to the security assessment and authorization process awareness and project integrations. This awareness will be done via training offering for all branches, and awareness material that will be available on InfoZone/Wiki pages, or other internal publications. In addition, work will be done in cooperation with ITB do identify applications and systems that do not have a valid security assessment, while in operation.

The Security Branch to approve and implement the Cyber Security Risk Council.

The target completion date for this action plan is March 2023.

## Recommendation 5

**The Security Branch should develop a CRA-wide systems authorization centralized monitoring strategy to maintain authorization and to document risk-based security decisions.**

Action Plan 5

Early 2022, the Security Branch initiated a review of its internal workflows and processes to identify items for improvement. As part of this initiative, the authority to operate tracking, processes, and associated residual risks to the organization was in scope.

While the Security Branch can only ensure that an authority to operate is provided after a system assessment, some gaps were identified during the intake process relevant to the templates used and authority to operate processes. As a result, the Security Branch identified there was insufficient security assessment and authorization awareness and proper project integration of security assessment and authorization deliverables within the project planning; therefore, it may have resulted the system being put in production without formal authorization as they did not channel through the security assessment and authorization intake process. Changes were implemented in June 2022.

In order to have an overview of the system authorization, CRA will require a CRA-wide systems authorization centralized monitoring strategy that will require the use of multiple “stream” of information from ITB and the Security Branch to provide an accurate picture of the system authorization state within the organization. Initially, discussions with the ITB will be required to integrate their workflows with the Security Branch processes to ensure that views of all system in production, or being developed, is available.

Secondly, the Security Branch will require a strong corporate tool to support the integration of the data (e.g. Governance, Risk and Compliance tool), to be able to track, review, and identify systems that either don't have a proper authorization, or is required to be reviewed.

This data will then be channelled via the Cybersecurity Risk Council quarterly for informational purpose and decision making. The Security Branch to approve and implement the Cyber Security Risk Council.

The target completion date for this overall action plan is March 2024, while some components will be competed by March 2023.

## Recommendation 6

**The Security Branch, in consultation with the ITB and stakeholders, should ensure inventories, tools, and supporting documentation are accurate and complete in order to prioritize the review of applications, systems, and components for authority to operate.**

Action Plan 6

While the Security Branch can only ensure that an Authority to Operate is provided after a system assessment, some gaps were identified during the Intake Process relevant to the templates used and Authority to Operate processes. As a result, the Security Branch identified there was insufficient security assessment and authorization awareness and proper project integration of security assessment and authorization deliverables within the project planning; therefore, it may have resulted in the system being put in production without formal authorization as they did not channel through the security assessment and authorization Intake Process. Changes were implemented in June 2022. More will be completed with respect to the security assessment and authorization process awareness and project integrations.

The Security Branch will continue to work with ITB to improve the available data enabling the accurate inventory of systems that are in operation, with their authorization status.

Until the Agency implements a CRA-wide systems authorization centralized monitoring strategy and an accurate inventory/representation of the system authorization is available, the Security Branch will review its internal process. This review will include investigating the feasibility of manually identifying high-importance systems within the agency. This would require a more frequent cycle of authorization review, review the system authorization validity, and provide the resulting information to the Cybersecurity Risk Council quarterly for informational purpose and decision making.

The target completion date for this action plan is March 2023.

## 3.2. Monitoring and reporting

### 3.2.1 Monitoring activities and oversight reporting mechanisms for security assessment and authorization are defined and performed, but further improvements are needed for key performance indicators and monitoring procedures.

Monitoring and reporting is key to inform designated organization officials of the current state of the CRA’s security posture. CRA corporate policy instruments state that an effective risk-based approach of security controls must be established, monitored, maintained, and reviewed, with corrective measures promptly taken when issues are identified. These requirements include defining responsibilities to monitor and report on decisions

regarding residual risk to the CRA, the status of all safeguard implementation plans, and compliance and continued effectiveness of security controls through periodic audits and reviews.

The internal audit team noted that monitoring responsibilities and activities for security assessment and authorization were defined at a high level and were included in corporate policy instruments. The internal audit team also observed that the Security Branch performs periodic oversight reporting on IT security for the ITB and the Board of Management. Specific key performance indicators are defined and the status and progress of risks and safeguard implementation plans are based on recommendations from security assessments and are reported.

However, the internal audit team found that there was a lack of monitoring baselines or procedures defined to ensure all risks were identified and safeguard implementation plans were completed in a timely manner to ensure residual risks in production are addressed and escalated when they do not meet prescribed timelines or require further consideration. The internal audit team also determined that not all risks being monitored were traced back to appropriate risk inventories, specifically inherited risks from supporting systems, platforms, and infrastructure, including those risks relating to cloud service providers. Also, at the time of the audit, there was no function or procedures in place to conduct reviews or audits that would ensure the security assessment and authorization process is being followed or to ensure the continued effectiveness of security controls for all applications, components, and systems as required by security requirements.

The Security Branch is planning on developing the Cyber Security Risk Council governance body to manage decisions on enterprise security risks, which was not in place at the time the audit was concluded.

Gaps in monitoring activities for managing risks and ensuring compliance could lead to an adverse impact on the confidentiality, integrity, and availability of protected information.

## Recommendation 7

**The Security Branch should develop monitoring mechanisms to ensure the timely completion of safeguard implementation plans, the reporting on the compliance to the security assessment and authorization process, and the continuous effectiveness of security controls.**

Action Plan 7

The Security Branch has designed a “Cyber Security Risk Council”, which has not yet been formally approved. The Security Branch will be responsible to provide the risk data upstream and coordinate risks mitigations with the system owners, with the intent to mitigate the risks in a timely matter, before it reaches the Cyber Security Risk Council.

The Security Branch will review and implement key performance indicators and workflows for the Cyber Security Risk Council to report on the timely completion of safeguard implementation, compliance to the security assessment and authorization process, and effectiveness of security controls.

The target completion date for this action plan is March 2023.

# 4. Conclusion

Overall, the internal audit team found that the security assessment and authorization process and requirements for information systems were in place for security assessments. However, the internal audit team found that

improvements are needed to further strengthen corporate policy instruments, roles and responsibilities, authorization, the monitoring of performance indicators, and the development of formal procedures and tools in order to support the needs of the CRA.

# 5. Acknowledgement

In closing, we would like to acknowledge and thank the Security Branch, the ITB, the Assessment, Benefit, and Service Branch, the Appeals Branch, the Collections and Verification Branch, and the Compliance Programs 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, the following lines of enquiry were identified:

| Lines of enquiry | Criteria |
|---|---|

| Lines of enquiry | Criteria |
|---|---|
| **Compliance** | CRA policies, directives, standards, and procedures related to security assessment and authorization are in place, current, communicated to stakeholders, and align with those of the Government of Canada. |
| | Roles and responsibilities related to security assessment and authorization are defined, communicated, and understood by stakeholders. |
| | Systems, components, and applications are managed, assessed, and authorized with formal acceptance of risks by stakeholders in compliance with the CRA's policy instruments related to security assessment and authorization. |
| **Monitoring and reporting** | Security assessment and authorization performance indicators are defined and reported with ongoing compliance updates to management. |
| | Oversight reporting mechanisms for security assessment and authorization are in place and are working as intended. |

# Methodology

The methodology for examination included the following:

- review and analyze corporate policy instruments and supporting documentation related to security assessment and authorization
- conduct interviews and walkthroughs with the Security Branch and the ITB management and staff as well as selected branch business owners
- test for compliance of controls through documentation reviews

- review and analyze data from supporting security applications and tools
- review and analyze performance indicators and monitoring reports in place related to security assessment and authorization

# Appendix B: Glossary

| Term | Definition |
|---|---|
| Authority to operate | A formal declaration by a designated approving authority that authorizes operation of a system or service moving into production and explicitly accepts the risks to CRA operations. The authority to operate signature certifies that the system has met all security requirements to become operational. |
| Availability | The ability for the right people to access the right information or systems when needed. Availability is applied to information assets, software, and hardware (infrastructure and its components). Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise. |
| 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. |
| Confidentiality | The ability to protect sensitive information from being accessed by unauthorized people. |

| Term | Definition |
| --- | --- |
| Cyber attack | The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device. |
| Cyber threat | Risk an information system or application receives from related or connected systems or components that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. |
| Inherited risk | Risk an information system or application receives from related or connected systems or components that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. |
| 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. Integrity also applies to business processes, software application logic, hardware, and personnel. |
| Residual risk | The level of risk remaining after security measures have been applied. |

| 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. |
| Safeguard implementation plan | The process used to track the implementation of recommendations that have been identified within a security evaluation to achieve the targeted level of residual risk. |
| Solutions Application Catalogue | The authoritative list of CRA enterprise applications that captures a variety of characteristics, such as application name, acronym, description, business, technology, and other portfolio attributes. |
| Security assessment | The ongoing process of evaluating security practices and controls, for new and existing IT systems and applications, to establish the extent to which they are implemented correctly, operating as intended, and achieving the desired outcome with respect to meeting defined security requirements. |
| Security authorization | The ongoing process for obtaining and maintaining a security risk management decision and to explicitly accept the related residual risk with the authority to operate, based on the results of the security assessment. |

| Term | Definition |
| --- | --- |
| 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 redacted] | [content redacted] |
| Security Risk Management | A fundamental principle where security is incorporated into the continuous updating of knowledge, understanding, assessment, and mitigation of threats and risks, both internal and external, to protect employees, information, assets, and revenues. |
| Threat and risk assessment | The process of identifying system assets and how these assets can be compromised, of assessing the level of risk that threats pose to assets, and of recommending security measures to mitigate threats. |
| 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. |

# Footnotes

1 CRA Mission, vision, and values – Canada.ca

2 CRA 2020-2021 Departmental Results Report – Canada.ca

**Date modified:**
2023-09-11