



Audit of Business Continuity Management

June 26, 2026

Internal Audit Branch
Internal Audit and Evaluation Sector



Department of Justice
Canada

Ministère de la Justice
Canada

Canada

Table of contents

Executive summary	1
1 Statement of conformance	2
2 Acknowledgement	2
3 Background	2
4 Findings, recommendations and management response and action plan	4
4.1 Continuity planning and strategies	5
4.2 Governance and capacity	9
4.3 Coordination and communication	13
4.4 Justice Canada's BCM Exercise Program	15
5 Audit opinion and conclusion	17
Appendix A: About the audit	18
Appendix B: List of acronyms and abbreviations	20

Executive summary

Purpose of the audit

This audit examined the adequacy of the Department of Justice Canada's business continuity management (BCM) to ensure the continued availability of its critical services and resources to support the functioning of government during a disruption.

Key findings

What worked well

- Justice Canada had a Business Continuity Management (BCM) Program that was continuously maintained and improved, as reflected in the Program's maturity level within the BCM life cycle.
- Governance structures were in place to support BCM.
- The Department had established coordination and communication mechanisms to support BCM.
- Justice Canada's three-year BCM Exercise Program helped improve business continuity planning.

Opportunities for improvement

- Continuity strategies within Business Continuity Plans (BCPs) were not fully developed, limiting the information required to support the update of the Strategic Business Continuity Plan (SBCP).
- Operational challenges limited the consistent implementation of key elements of the BCM life cycle.
- Coordination and communication mechanisms were not fully consistent and leveraged to support an integrated BCM approach.
- The Department could strengthen its ability to effectively respond to disruptions by leveraging lessons learned from other organizational resilience disciplines.
- Inconsistent and infrequent testing at the operational level limited the Department's preparedness and resilience in the event of a disruption.

Audit opinion and conclusion

The Department of Justice Canada had a BCM Program that supports and enables its continued capacity to provide its critical and sub-critical services. This includes those services or activities that directly enable or support the delivery of these critical services to Canadians and other government departments in the case of a disruption.

At the time of this audit, the Department was in the process of updating its BCM Program with a strong, foundational framework in place to enable its continued development and enhancement.

To further improve the Program, the Department should leverage lessons learned from other organizational resilience disciplines to strengthen its ability to effectively respond to and learn from disruptions; it should clarify oversight and accountability mechanisms and help ensure BCM practices and processes are completed in accordance with the BCM Framework; and it should adopt a more coordinated approach to sharing information and documenting decisions during disruptions.

Management response

Management agrees with the audit findings, accepts the recommendations included in this report and has developed a management action plan to address them. The management action plan is integrated in this report.

1 Statement of conformance

In my professional judgment as Chief Audit and Evaluation Executive, the audit conforms to the Global Internal Audit Standards, as supported by the results of the Quality Assurance and Improvement Program.

Submitted by:

Tricia Goulbourne
Chief Audit and Evaluation Executive
Department of Justice Canada

Date

2 Acknowledgement

The Chief Audit and Evaluation Executive would like to thank the audit team and those individuals who contributed to this engagement and particularly, employees who provided insights and comments as part of this audit.

3 Background

Business Continuity Management (BCM) helps organizations identify their critical and sub-critical services and functions and provides a framework for building resilience and capacity for an effective response to emerging threats or to recover from disruptions. Events and disruptions refer to occurrences with actual or potential impact to an

organization's business operations. Events or disruptions may be anticipated or occur suddenly.

In the Government of Canada (GC), BCM is governed by key legislation, policies and directives:

- The [Federal Policy for Emergency Management](#) (FPEM) pursuant to the [Emergency Management Act](#), outlines responsibilities for federal institutions concerning emergency preparedness, which includes BCM.
- Treasury Board Secretariat (TBS) defines policy requirements for the GC's eight security controls, which includes BCM, via the [Policy on Government Security](#) (PGS) and [Directive on Security Management](#) (DSM), pursuant to the [Financial Administration Act](#).

As per the Policy on Government Security, Public Safety (PS) has produced the Business Continuity Management Guide (Guide) that adapts industry best practices to reflect a GC context and supports federal organizations in implementing the mandatory BCM procedures as outlined in the Directive on Security Management (DSM).

For the Department of Justice Canada (Justice Canada or the Department), the Consolidated Business Continuity Plan (CBCP) (now known as the Strategic Business Continuity Plan [SBCP]) was first developed in 2015 and last updated in 2016. To align with the guidance provided by PS and refresh its BCM Program, the Department released a Business Continuity Management Framework (2023). This Framework outlined the governance and key components of the Department's business continuity planning to assist those involved with the development, implementation and maintenance of its BCPs. Through this effort, the Department also identified its critical and sub-critical services and related enabling functions.

Critical and/or Sub-Critical Services	Related Enabling Functions
• Provision of Family Orders and Agreements Enforcement Assistance Act Program • Legal Services to the Minister of Justice and Attorney General of Canada, Deputy Minister of Justice, and other federal government Ministers • International Mutual Legal Assistance Requests and Extradition Matters • Judicial Verifications that support judicial appointments and the secure operation of courts and tribunals	• Information Technology • Communication Services • Accounting Operations

Activation of the Department's Business Continuity Plans (BCPs), according to the Consolidated Business Continuity Plan, is for any significant incident that could cause a disruption of critical services. Examples of significant incidents include physical or cyber security risks; risks to Justice human resources, infrastructure or information assets; an emergency resulting in the activation of two or more continuity plans, possibly including relocation of resources to pre-planned alternate sites, recovery or replacement of assets.

To ensure strong coordination in the development, implementation, and maintenance of a BCM program, federal organizations should establish or identify a governing body to oversee the organization's BCM program within their governance structure. Justice Canada's BCM governance consists of the Strategic Emergency Management Committee (SEMC) and the National Business Continuity Management Committee (NBCMC).

The Safety, Security and Emergency Management Division (SSEMD) is a division under the Corporate Services Branch, led by the Chief Security Officer, within the Department's Management Sector. It serves as the centre of subject-matter expertise for BCM. SSEMD is accountable for the implementation of the Department's BCM Program including the coordination of exercising and testing of the BCPs. Justice Canada's senior managers and BCM representatives also play an important role in BCM, but contributions are made at all levels.

The Business Continuity Management Coordinators (BCM Coordinators), including their designated alternates are crucial to the success of the Department's BCM Program. BCM Coordinators are appointed by the Senior Manager of their Branch/Sector/Portfolio/Directorate and are responsible for defining, documenting, and maintaining business continuity practices and processes for their respective Branch, Portfolio, Sector or Directorate, and for collaborating with partners and involved parties including supply chain entities. BCM Coordinators focus on the application of BCM at the operational level.

As part of Justice Canada's efforts to refresh its Business Continuity Management Program (BCM Program), the Department has adopted the new tools and templates provided by PS for its Business Impact Analysis (BIA) and BCPs. At the time of the audit, the BIAs were completed and had been updated using the new template for all critical and sub-critical services. The Department plans to update its SBCEP following the update to the operational BCPs (i.e., BCPs by Branch, Portfolio, Sector, Directorate responsible for critical and/or sub-critical services) which will adopt a new template aligned with guidance from PS.

4 Findings, recommendations and management response and action plan

This section provides the findings and recommendations resulting from the audit work carried out. The audit was conducted based on the lines of enquiry and audit criteria identified during the planning phase, which are presented in [Appendix A](#) of this report.

4.1 Continuity planning and strategies

Justice Canada had a Business Continuity Management Program that was continuously maintained and improved. However, the Department could strengthen its ability to effectively respond to and learn from disruptions, by further developing continuity strategies, updating its overall Strategic Business Continuity Plan and leveraging lessons learned from other organizational resilience disciplines.

Justice Canada had a formally established Business Continuity Management Program that was continually maintained and improved.

The BCM life cycle, as described in PS' Business Continuity Management Program Guide 2023 (Guide), "provides a framework for building organizational resilience by planning and adapting responses capabilities that safeguards its critical activities". The life cycle contains six elements that are comprised of broad steps to ensure that the BCM Program meets policy requirements and best practices. The six elements are *Manage, Analyze, Plan, Educate, Validate* and *Improve*, with each element containing its own steps and best practices.

At the time of the audit, Justice Canada's BCM Program was in the *Improve* (Maintenance and Improvement) phase of the BCM life cycle. It had a BCM Framework in place, which aligned with the guidance provided by PS, and continued to take steps to refresh its BCM Program by adopting new tools and templates.

Continuity strategies within Business Continuity Plans were not fully developed, limiting the information required to support the update of the Strategic Business Continuity Plan.

Business continuity strategies provide alternate arrangements and resources that can be put in place to minimize downtime while BCPs provide organizations with steps for managing events efficiently and maintaining their organization's critical service delivery. Following the BCM Framework, Sector and Portfolio BCM Coordinators are responsible for defining their own business continuity strategies as part of their BCP. During its examination, the audit team reviewed a sample of BCPs to assess whether they included business continuity strategies to maintain or restore the Department's critical services during a disruption. They found that the strategies were not fully developed in the operational BCPs. Key resource categories had been addressed to a varying extent (i.e., people, facilities, equipment, etc.), however, the BCPs lacked several continuity strategies implementation characteristics, as suggested by PS' guidance (i.e. adaptability,

sustainability, scalability, and flexibility). The audit also found that, while most of the BCPs included in the sample had been updated within the last two years, none of the sampled BCPs were updated using the new template to align with the guidance provided by PS. Although it was not a strict requirement to use the new templates provided by PS, the templates could help the Department identify and address the missing components to further refine the BCPs in areas such as workarounds for IT disruptions, workload transfer, sustainability elements pertaining to alternate site strategies, and more.

Furthermore, at the time of the audit, the Department was awaiting the finalization of the operational BCPs for its critical and sub-critical services before updating its Strategic Business Continuity Plan, which hadn't been updated in 10 years (since 2016). Without updated continuity strategies, departmental teams could be exposed to a heightened risk of not being able to deliver their services consistently and in a timely manner in the event of a disruption. This could lead to impacts such as reputational damage, financial losses or client-relationship strains.

While not all disruptions require BCP activation, those managed outside the BCM framework were not consistently documented or leveraged for continuous improvement.

As mentioned above, activation of the Department's BCPs, according to the CBCP, is for any significant incident that could cause a disruption of critical services. Examples of significant incidents include physical or cyber security risks; risks to Justice human resources, infrastructure or information assets; an emergency resulting in the activation of two or more continuity plans, possibly involving relocation of resources to pre-planned alternate sites, recovery or replacement of assets. During interviews, involved parties indicated that decisions to activate the BCP were determined by the critical or sub-critical service owner, based on the impact of a disruption on service delivery. As such, not all incidents (e.g., IT outages, fire alarms, snowstorms or facility issues) would automatically trigger a BCP activation. Activation of the BCP would be considered if established service delivery thresholds were exceeded or could be exceeded (e.g., six hours of maximum allowable downtime), which would be assessed by the various levels of governance.

As part of the audit work, the team selected two disruptions that occurred during the scope period, to understand how decision-making processes were carried out and what information was documented during these disruptions. While the audit did not assess the rationale to formally activate the BCP or not, the team expected to find a documented trail detailing the nature of the disruption, the sequence of actions, the impacts, the decisions made, and any after-action reviews or post-mortem analyses conducted following the disruption. During interviews, parties involved explained that the Department did not activate its operational BCPs for the impacted critical or sub-critical services. Instead, the disruptions were handled via the Department's IT incident management response, which is managed by Justice Canada's Information Solutions Branch (ISB). As these disruptions

were managed through ISB's IT incident management process and not through the BCPs, communication efforts and post-mortem discussions were not formally documented or shared with the Department's National BCM Coordinator. The audit team was also unable to obtain information or documentation relating to any corrective actions that may have been considered, monitored, or implemented as areas of improvement for the Department's BCM Program. While not all disruptions trigger a BCP activation, disruptions or events that are significant should be documented by the business lines, based on a risk-based approach. The BCM life cycle, more specifically the *Improve* element (*Maintenance and Improvement*), highlights these steps to ensure that continuous improvement is captured in the plans to improve the organization's resilience. Therefore, the lack of documentation for disruptions managed outside of BCM may limit the Department's ability to capture lessons learned, identify improvement opportunities, and incorporate them into its business continuity processes. As a result, opportunities to strengthen BCP's based on actual events may be missed.

Recommendation #1

In order to ensure that the Department has a robust BCM Program, the Chief Financial Officer and Assistant Deputy Minister, Management Sector should continue efforts for the completion and approval of the Department's Critical Service's operational BCPs to permit the timely revision of the Strategic Business Continuity Plan. To reinforce Justice's BCM Framework's accountability and governance:

- Operational BCPs for critical services, including related enabling functions, should be completed, reviewed and approved at the Assistant Deputy Minister (ADM) level by the respective service owners.
- The updated SBCP should be presented to Justice's SEMC for Deputy Minister approval and shared at the branch, sector or portfolio level with employees implicated in the BCP.

Management Response and Action Plan

Agreed.

Office of Primary Interest

Chief Financial Officer and Assistant Deputy Minister, Management Sector

Actions:

The Department will continue the implementation of its Business Continuity Management (BCM) refresh approach and will prioritize the completion and approval of operational Business Continuity Plans (BCPs) for departmental critical services, using standardized templates and existing governance mechanisms. Development of operational BCPs for non-critical and supporting functions will continue to be risk-informed and undertaken at management discretion where operationally justified.

To strengthen accountability and governance, completed operational BCPs for critical services will be reviewed and approved at the Assistant Deputy Minister (ADM) level by the respective service owner.

Following completion and approval of operational BCPs for critical services, SSEMD will coordinate the update of the Strategic Business Continuity Plan (SBCP) to reflect departmental continuity priorities, key dependencies, and enterprise-level response arrangements. The updated SBCP will be presented and submitted to Justice's SEMC for Deputy Minister approval and shared at the branch, sector or portfolio level with employees implicated in the BCP.

Deliverables:

1. Completed and ADM-approved operational BCPs for departmental critical services.
2. Updated Strategic Business Continuity Plan ready for submission to the DM for approval.
3. Record of dissemination of the SBCP to identified internal stakeholders.

Due date

June 2027

Recommendation #2

The Chief Financial Officer and Assistant Deputy Minister, Management Sector should, as part of updating its Strategic Business Continuity Plan, review the lessons learned process to determine a risk-based approach to integrate insights and lessons learned from other organizational resilience disciplines.

Management Response and Action Plan

Agreed.

Office of Primary Interest

Chief Financial Officer and Assistant Deputy Minister, Management Sector

Actions:

To support continuous improvement and strengthen integration across organizational resilience activities, SSEMD will implement a standardized framework for capturing and integrating lessons learned arising from material business continuity exercises, and other significant resilience events with implications for business continuity management. The framework will define criteria and thresholds for identifying events requiring documentation and will outline roles and responsibilities for responsible business areas to document observations and provide relevant inputs for continuity planning updates.

For events meeting the established threshold, SSEMD will maintain a standardized lessons learned register and require consideration of applicable observations during future updates of operational BCPs and the SBCP.

Deliverable:

Implemented lessons learned process, including:

- documented event thresholds and criteria;
- standardized lessons learned register/template; and
- records demonstrating that applicable lessons learned were assessed and reflected, where appropriate, in operational BCPs and SBCP updates.

Due date

September 2027

4.2 Governance and capacity

While governance structures were in place to support Business Continuity Management, they were not fully leveraged to enable effective coordination and decision-making. At the operational level, BCM Coordinators faced capacity and preparedness challenges that limited their ability to consistently implement and maintain key elements of the BCM life cycle within their respective areas.

Strong governance is essential to a robust BCM Program, to ensure clear accountability, consistent decision-making, and alignment across all areas of the organization before, during, and after a disruption. Effective governance also helps sustain program oversight, prioritize critical risks and resources, support timely, coordinated responses during incidents, and improve organizational resilience.

Governance structures were established to support Business Continuity Management.

In the Department of Justice Canada, BCM governance is supported by the Strategic Emergency Management Committee (SEMC) and the National Business Continuity Management Committee (NBCMC). The SEMC is the senior departmental committee responsible for providing strategic direction and setting priorities for the management of emergencies and business continuity, in accordance with the Treasury Board *Policy on Government Security*. The Department also has a NBCMC which has the broad mandate to review, assess, challenge, guide, advise and make decisions regarding the Department's BCM Program, thereby supporting the CSO in meeting responsibilities related to the Department's BCM Program. The NBCMC is also used to share information and best practices with respect to business continuity programs among committee members across the Department.

At the operational level, the Safety, Security and Emergency Management Division (SSEMD) is a division under the Corporate Services Branch, led by the Chief Security Officer, within the Department's Management Sector. It serves as the centre of subject-matter expertise for BCM. SSEMD is accountable for the implementation of the Department's BCM Program including the coordination for exercising and testing of the BCPs. Justice Canada's senior managers and BCM representatives also play an important role in BCM, but contributions are made at all levels.

The Business Continuity Management Coordinators (BCM Coordinators) are appointed by the Senior Executive of their Branch/Sector/Portfolio/Directorate and are responsible for defining, documenting, and maintaining business continuity practices and processes for their respective Branch, Portfolio, Sector or Directorate and collaborating with partners and involved parties including supply chain entities. BCM Coordinators focus on the application of BCM at the operational level. Both coordinators and alternates are crucial to the success of the Department's BCM Program.

Key operational challenges limited the consistent implementation of key elements of the BCM life cycle.

While the BCM Framework document outlines the BCM governance and key components of business continuity planning and defines the roles, responsibilities and accountabilities of each governance partner involved with the development, implementation and maintenance of business continuity plans, the audit team identified key operational challenges limiting the consistent implementation of key elements of the BCM life cycle (e.g. testing and training).

Governance committees were not fully leveraged for coordination and decision-making.

As mentioned above, the SEMC is responsible for providing strategic direction and setting priorities for the management of emergencies and business continuity, while the NBCMC has the broad mandate to review, assess, challenge, guide, advise and make decisions regarding the Department's BCM Program. The NBCMC was also used to share information and best practices with respect to business continuity programs among committee members across the Department. While this supports awareness and the sharing of practices across the Department, the audit found that the NBCMC functioned primarily as a downstream information-sharing forum and that it could be leveraged to strengthen coordination and decision-making. Although the Department's committees had appropriate membership to discuss business continuity management, they were not being fully utilized to address or coordinate BCM issues (e.g. joint planning or testing exercises, etc.). Opportunities to further leverage existing governance forums should be considered to enhance the BCM Program's maturity within the Department.

BCM coordinators had limited capacity to support all components of the BCM cycle.

As mentioned above, Justice Canada's BCM Coordinators are responsible for defining, documenting, and maintaining business continuity practices and processes for their respective branch, sector or directorate and collaborating with partners and involved parties including supply chain entities. They are appointed by the Senior Manager of their Branch/Sector/Portfolio/Directorate. At the time of the audit, the majority of coordinators were executives working in director-level positions (for instance, as Directors of Business Management [DBMs]). Their BCM responsibilities were therefore additional to their core responsibilities, which is common across the GC. They were trained by the National BCM Coordinator through workshops, one-on-one meetings, and through the NBCMC meetings. The coordinators also had the option to attend other BCM training through virtual courses hosted by the Canada School of Public Service and/or other external providers. During interviews, some coordinators indicated that despite the training provided and available, they were not always able to provide sufficient attention and time to develop their BCM competencies and knowledge and they did not always feel adequately prepared to carry out some of the BCM-related activities (e.g., developing and implementing BCM training, testing their BCP within their designated branch, sector, portfolio or directorate, etc.). As a result, some of them were not fully completing assigned BCM activities, focusing instead on the activities they understood to be required (or were instructed to complete), such as completing the BIA's and BCP's. Consequently, key elements of the BCM life cycle, such as testing, monitoring, and awareness activities, were not being carried out as defined in the guidance by PS. Carrying out all components of the BCM life cycle is important for improving the Program's maturity and the Department's overall resilience in the event of a disruption.

The Department's BCM governance model relies on a decentralized approach where SSEMD and the National BCM Coordinator provide department-wide coordination, guidance, and support, while responsibility for executing BCM activities is delegated to individual organizational units through their BCM Coordinators. This governance structure depends heavily on the branches, sectors or directorates' prioritization and capacity, while providing limited authority for SSEMD to enforce implementation. While SSEMD and the Management Sector can strengthen awareness, guidance and tools to facilitate the execution of practices and processes, accountability for implementing BCM activities rest with individual sector heads.

Recommendation #3

To clarify oversight and accountability mechanisms and help ensure BCM practices and processes are completed in accordance with the BCM Framework, the Chief Financial Officer and Assistant Deputy Minister, Management Sector should take steps to:

- Further engage SEMC members to strengthen the coordination of BCM activities and decision-making. This should include an onboarding process for new members to discuss governance and key components of business continuity planning that

assists those involved with the development, implementation and maintenance of business continuity plans.

- Engage members in a discussion on how oversight and accountability mechanisms could be strengthened to ensure BCM that practices and processes are completed in accordance with the BCM Framework.
- Strengthen the selection, onboarding, and ongoing development of BCM coordinators. This should include an onboarding package that defines core responsibilities, expected activities across the BCM lifecycle, and available tools and support mechanisms.

Management Response and Action Plan

Agreed.

Office of Primary Interest

Chief Financial Officer and Assistant Deputy Minister, Management Sector

Actions:

The Department will strengthen the implementation of the BCM Program by formalizing roles, responsibilities, and onboarding approach for Business Continuity Management (BCM) Coordinators and designated alternates.

SSEMD will establish a standardized BCM Coordinator package that defines core responsibilities, expected activities across the BCM lifecycle, and available tools and support mechanisms. The package will support consistent onboarding of newly designated coordinators and alternates and clarify accountability for maintaining operational BCPs and supporting departmental BCM activities. Newly designated BCM Coordinators and designated alternates will be expected to complete foundational BCM training identified by SSEMD as part of onboarding and role-readiness activities.

To support consistent governance and awareness, SSEMD will develop and maintain a formal BCM briefing package for Strategic Emergency Management Committee (SEMC) members and designated alternates that outlines their roles, responsibilities, decision-making expectations, and oversight responsibilities within the Department's BCM governance framework. The briefing package will be provided to all newly appointed SEMC members and newly designated alternates as part of established governance onboarding processes.

Orientation and supporting guidance materials will be provided through existing governance and engagement mechanisms and maintained in a central repository accessible to coordinators and governance members. Responsibilities for designating BCM Coordinators and alternates will be documented and communicated through existing BCM governance mechanisms.

The Department will continue to leverage existing management structures for assignment of BCM responsibilities and will not establish dedicated BCM positions or additional governance structures as part of this action.

Deliverables:

1. Updated BCM Coordinator roles and responsibilities document.
2. Standardized BCM Coordinator onboarding and guidance package, including foundational BCM orientation requirements.
3. BCM briefing package and documented onboarding approach for newly appointed SEMC members and alternates.

Due date

June 2027

4.3 Coordination and communication

The Department had established coordination and communication mechanisms, but they were not fully consistent and leveraged to support an integrated BCM approach.

Effective communication is important to ensure that business continuity efforts are aligned across the Department, enabling timely, consistent, and well-coordinated responses to disruptions and reducing the risk of fragmented or delayed recovery.

Coordination and communication practices in place were informal and limited consistency across the BCM program.

As outlined in the BCM Framework, BCM Coordinators play key liaison, coordination, and communication roles within the Department's BCM Program. The National BCM Coordinator is primarily responsible for reviewing operational BCPs, consolidating identified resource requirements, and updating the Department's Strategic Business Continuity Plan. Effective coordination among the National BCM Coordinator, BCM Coordinators, and critical and sub-critical service owners is essential to ensure consistency across BCM documentation and operational BCPs covering similar functions or business units. This coordination also helps align continuity strategies across teams and reduces unnecessary duplication where multiple operational BCPs apply to the same or related services. Information gathered through interviews for coordination among BCM Coordinators revealed that, in practice, coordination seemed to be easier among Coordinators who it worked in similar substantive work positions or business units (i.e., DBMs, Regional Accommodation and Integrated Security Operations [RAISOs]).

PS' guidance on BCM, states that internal and external communications with parties are important throughout the BCM life cycle, as well as during times of disruptions. The audit team found that communication protocols were not formally defined or documented for internal and external parties. This gap with internal communication protocols impacted SSEMD's ability to stay on track with their BCM cycle timelines as set out in the BCM life cycle. Formal communication protocols would help maintain operational resilience by ensuring timely, accurate, and secure information flow throughout the BCM life cycle.

Recommendation #4

The Chief Financial Officer and Assistant Deputy Minister, Management Sector, should formally define departmental protocols for internal and external communications during times of disruptions for all affected parties.

Management Response and Action Plan

Agreed.

Office of Primary Interest

Chief Financial Officer and Assistant Deputy Minister, Management Sector

Actions:

The Department will develop and approve a concise Business Continuity Management (BCM) communications protocol to establish roles, escalation triggers, communication pathways, and minimum documentation expectations for internal and external communications during disruptions.

The protocol will leverage existing departmental governance, emergency management, and incident management mechanisms and will not create additional governance structures. The protocol will define communication responsibilities and minimum notification expectations for affected parties and supporting functions during disruptions.

To support operational readiness, SSEMD will establish a process to maintain BCM stakeholder contact information, including identifying ownership for updates and defining when contact lists are to be reviewed and refreshed.

Communication expectations and related procedures will be communicated through existing BCM governance forums and incorporated into the Business Continuity Framework and supporting BCM guidance material.

Deliverables:

1. Approved BCM communications protocol, including supporting a communications matrix defining roles and escalation pathways.
2. BCM stakeholder contact list.
3. Documented process identifying ownership and updated requirements for maintaining BCM contact information.

Due Date

June 2027

4.4 Justice Canada's BCM Exercise Program

Justice Canada's three-year BCM Exercise Program helped improve business continuity planning, but inconsistent and infrequent testing at the operational level has limited the Department's preparedness and resilience in the event of a disruption.

The BCM Exercise Program and centralized testing supported continuous improvement.

A structured exercise program is critical to validating the effectiveness of business continuity plans, identifying gaps, and ensuring timely corrective actions to reduce the risk of ineffective response during disruptions.

Justice Canada developed a BCM Exercise Program that spanned three fiscal years (2022-2023 to 2024-2025) to address the testing, monitoring and corrective action controls of BCM, and to support the continuous improvement of the Department's resiliency. The Exercise Program included regular testing of BCPs, monitoring, and corrective action (review and maintenance of BIAs and BCPs through environmental scans and results of tests) throughout the BCM life cycle.

The audit found that the Department conducted tests of its BCPs through the annual SSEMD-led SEMC exercises. In addition to this testing, a few departmental organizational units responsible for critical and sub-critical services conducted their own testing initiatives to further strengthen their operational BCP. These tests resulted in after-action reports being prepared by the designated observer (e.g., the National BCM Coordinator, RAISOs, etc.), and the resulting observations and recommendations were documented and monitored to ensure their implementation, with a view to strengthening identified areas of weakness.

Operational-level testing was inconsistent and did not fully meet program objectives.

While centralized testing provides important department-wide assurance, operational-level testing is essential to ensure that business continuity plans are practical, tailored to specific functions, and effective within individual organizational units.

During interviews, the audit team found that not all BCM Coordinators responsible for operational BCPs conducted annual testing, and that the testing performed varied in scope, complexity, and consistency across the Department.

These inconsistencies were driven in part by issues identified in earlier sections of the report. The need to update BCPs reduced the perceived value of testing, as exercises based on outdated plans were unlikely to yield meaningful insights, thereby contributing to lower prioritization and frequency of operational-level testing. Further, capacity constraints and gaps in preparedness among BCM Coordinators limited their ability to design and lead testing exercises for their respective organizational unit (i.e. portfolio,

sector, branch, etc.). Overall, these factors resulted in a lower testing frequency which did not align with the originally established objectives of the Exercise Program.

BCM testing allows the Department to assess its ability to respond to disruptions or events that may negatively impact the organization's ability to operate. It is also used to identify gaps, weaknesses and areas for improvement in the execution of the BCPs. Testing can also enhance BCM Coordinators' knowledge and capabilities with respect to the BCM lifecycle, as it engages them in real scenarios that promote learning and requires them to update the plans following the exercises. Without regular BCP testing, this may affect the reliability of the plans, limit organizational readiness, and increase the likelihood of prolonged disruptions to the Department's critical an/or sub-critical services during an event or disruption.

Once again, it's important that SSEMD update the Department's Exercise Program and continue to conduct centralized testing on a regular basis. Furthermore, individual branches, sectors, portfolios, and directorates are responsible for regular testing within their respective areas.

Recommendation #5

The Chief Financial Officer and Assistant Deputy Minister, Management Sector, should update the Department's BCM Exercise Program and establish clear accountabilities for the conduct, monitoring, and documentation of routine BCP tests (i.e. SBCEP and operational BCPs), as prescribed in the BCM Program. This may include exercise guidance and tools to support critical services owners.

Management Response and Action Plan

Agreed.

Office of Primary Interest

Chief Financial Officer and Assistant Deputy Minister, Management Sector

Actions:

The Department will refresh the Business Continuity Management (BCM) Exercise Program to establish a risk-informed and scalable approach for exercising Business Continuity Plans (BCPs), recognizing differences between departmental-level and operational-level continuity requirements.

The refreshed Exercise Program will establish minimum expectations for when and how BCP exercises are conducted and will clarify accountabilities for planning, support, documentation, and follow-up activities.

The Department will leverage existing governance mechanisms and existing exercise activities and will not establish additional approval requirements as part of this action.

Deliverables:

1. Updated BCM Exercise Program defining exercise expectations and governance, including documented roles and responsibilities for exercise planning, facilitation, reporting and support (including the National BCM Coordinator and RAISOs).
2. Develop a standardized exercise reporting and lessons learned template.

Due date

September 2027

5 Audit opinion and conclusion

The Department of Justice Canada has a BCM Program that supports and enables its continued capacity to provide its critical and sub-critical services. This includes those services or activities that directly enable or support the delivery of these critical services, to Canadians and other government departments in the case of a disruption. While at the time of this audit, the Department was in the process of updating its BCM Program, an existing strong foundational framework is already in place, enabling the continued development and enhancement of the Program.

To further improve the Program, the Department should leverage lessons learned from other organizational resilience disciplines to strengthen its ability to effectively respond to and learn from disruptions; it should clarify oversight and accountability mechanisms and help ensure BCM practices and processes are completed in accordance with the BCM Framework; and it should adopt a more coordinated approach to sharing information and documenting decisions during disruptions.

Appendix A: About the audit

Audit objective:

The objective of this audit was to provide assurance that the Department's Business Continuity Management Program was adequate to ensure the continued availability of its critical services and resources to support the functioning of government during a disruption.

Audit scope:

The scope for this audit included the Department's refreshed Business Continuity Program beginning from 2021 to present and examined the testing, validation and improvement of the plans, including the collaboration and continuity strategies to maintain or restore critical services throughout a disruption. Those services or activities that directly enable or support the delivery of Justice's critical services were also included in the scope.

While there were other organizational resilience disciplines (i.e. emergency management, crisis management, incident management, etc.) that support and work in conjunction during events, this audit focused specifically on the discipline of Business Continuity Management that maintained or supported the critical functioning of the government during a disruption.

Audit approach:

This engagement was conducted in accordance with the Treasury Board of Canada Secretariat's Policy and Directive on Internal Audit, and the Global Internal Audit Standards issued by the Institute of Internal Auditors (IIA). These standards require that the engagement be planned and performed to obtain reasonable assurance that the objectives of the engagement were achieved.

Audit lines of enquiry and criteria:

Line of enquiry 1: Business Continuity Plans and Coordination

The Department's business continuity strategies and coordination mechanisms prepare the Department for timely recovery of its critical services and related enabling functions during a disruption.

- 1.1. Business Continuity Plans include continuity strategies to maintain or restore the Department's critical services and related enabling functions during a disruption

(e.g., alternate sites, telework, manual workarounds, restoration of IT systems and infrastructure, and the distribution of IT assets, etc.).

- 1.2. Coordination mechanisms between the Department's Portfolios, Sectors and Branches exist (e.g., IT, joint planning exercises) to ensure that plans are aligned, cohesive, and adequately resourced during a disruption.
- 1.3. Communication protocols are established to inform key parties involved internally and externally.

Line of enquiry 2: Testing, Validation and Improvement of Business Continuity Plans

The Department has established processes to test, validate, and update its business continuity plans (departmental, Portfolio, Sector and Branch) to ensure they remain effective in delivering critical services and related enabling functions during a disruption.

- 2.1 The Department conducts regular testing of its business continuity plans (e.g. tabletop exercises, simulations, etc.)
- 2.2 After-action reports are produced following testing activities, and corrective actions (including those that may be identified from actual disruptions or events) are incorporated into updates and improvements to the plan and reported to senior management.
- 2.3 The Department provides BCM training and awareness for employees to lead, participate in, or support its business continuity strategies at the departmental, Portfolio, Sector and Branch levels.

Appendix B: List of acronyms and abbreviations

ADM	Assistant Deputy Minister
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CBCP	Consolidated Business Continuity Plan
CSO	Chief Security Officer
DBM	Director, Business Management
Department	Department of Justice Canada
DM	Deputy Minister
DSM	Directive on Security Management
EC	Executive Committee
EMA	Emergency Management Act
FAA	Financial Administration Act
FPEM	Federal Policy for Emergency Management
GC	Government of Canada
Guide	Business Continuity Management Guide
ISB	Information Solutions Branch
IT	Information Technology
NBCMC	National Business Continuity Management Committee
PGS	Policy on Government Security
PS	Public Safety Canada
RAISO	Regional Accommodation and Integrated Security Operations
SBCP	Strategic Business Continuity Plan
SEMC	Strategic Emergency Management Committee
SSEMD	Safety, Security and Emergency Management Division
TBS	Treasury Board Secretariat