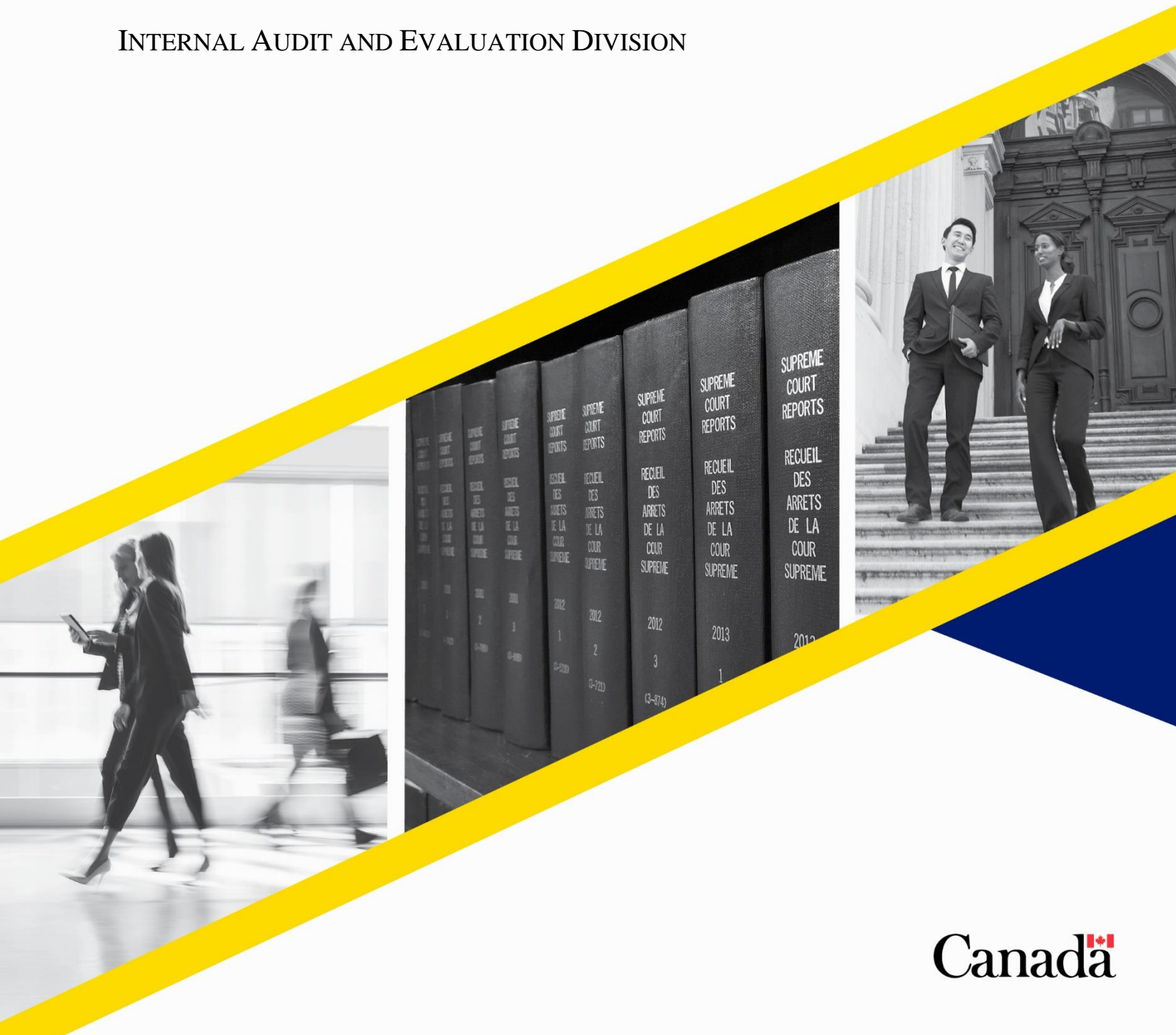




SYSTEM UNDER DEVELOPMENT AUDIT OF AMICUS IMPLEMENTATION REPORT

JANUARY 2023

INTERNAL AUDIT AND EVALUATION DIVISION



As recommended by the Departmental Audit Committee, subject to approval by the Director of Public Prosecutions, on December 2, 2022.

Approved by the Director of Public Prosecutions on February 21, 2023.

Cette publication est également disponible en français.

This publication is available in HTML formats on the Internet at <http://www.ppsc-sppc.gc.ca/eng/>

© His Majesty the King in Right of Canada, 2023.

Cat. No. J79-16/2023E-PDF

ISBN: 978-0-660-48092-3

TABLE OF CONTENTS

1.	EXECUTIVE SUMMARY	1
1.1	OBJECTIVES AND SCOPE.....	1
1.2	AUDIT CONCLUSION.....	1
1.3	SUMMARY OF RECOMMENDATIONS	1
1.4	STATEMENT OF ASSURANCE.....	2
2.	INTRODUCTION.....	3
2.1	BACKGROUND	3
2.2	OBJECTIVES AND SCOPE.....	3
2.3	METHODOLOGY	4
3.	OBSERVATIONS AND RECOMMENDATIONS	5
3.1	GOVERNANCE.....	5
3.2	PROJECT MANAGEMENT FRAMEWORK	5
3.3	CHANGE MANAGEMENT	7
3.4	APPLICATION CONTROLS AND BUSINESS REQUIREMENTS	8
3.5	AMICUS IMPLEMENTATION	9
4.	OPPORTUNITIES FOR IMPROVEMENT.....	10
5.	CONCLUSION	10
6.	MANAGEMENT RESPONSE AND ACTION PLAN.....	11
	APPENDIX A – AUDIT CRITERIA	13
	APPENDIX B - LIST OF ACRONYMS/ABBREVIATIONS.....	14

1. EXECUTIVE SUMMARY

1.1 OBJECTIVES AND SCOPE

The objectives of this audit were to provide management with an independent assessment of the progress, quality, and attainment of the Amicus project objectives at defined milestones within the project and an evaluation of the internal controls of proposed business processes during the various phases in the development cycle where enhancements can be easily implemented and processes adapted.

The audit focused on the governance structure around the project, project management framework, change management, identification and testing of business requirements, and the implementation approach of the Amicus system.

1.2 AUDIT CONCLUSION

The Internal Audit and Evaluation Division (IAED) examined the processes and controls for the implementation of the Amicus system against pre-established project management and system development criteria based on Treasury Board (TB) policies, directives and guidance, Public Prosecution Service of Canada (PPSC) policies, directives, and procedures, as well as general best practices.

Overall, there was some appropriate project management governance over the system development process; however, there were some controls and procedures not followed.

Improvements should be made in reporting on project plans to ensure management is aware of reasons for project delays, actual completion dates of activities, and changes in project schedules. Appropriate business management, prior to the design and build of a new system, should approve functional requirements. A change management process should include a process to hand over a new system after successful testing. Finally, a post implementation governance structure should be put in place prior to Amicus implementation in order to manage Amicus after implementation.

1.3 SUMMARY OF RECOMMENDATIONS

The IAED found that Information Technology Services was able to design and build the Amicus system, as well as begin a pilot test for Amicus. The project team updated the governance committee with project risks and changes. The project team also developed a high-level change management process to put in place after implementation of Amicus. The pilot test approach allows for the discovery of potential issues and appropriate approval to implement Amicus after successful completion of the pilot test.

This report contains the following recommendations:

- The Director General, Administration Services (DG, AS) and Chief Information Officer (CIO) should:
 - provide the Steering Committee an explanation for changes in the project schedule as soon as they become aware of possible changes and impacts, including both time and cost.

System Under Development Audit of Amicus
Implementation Report

- document and implement a governance structure to formally process and approve the handover of Amicus to a region after successful pilot testing, and to support the system after implementation.
- develop an acceptance test plan and execute an acceptance test with each region prior to full deployment of Amicus.
- ensure that each region conducts and documents a readiness assessment, in conjunction with the Chief Federal Prosecutor for the region, prior to full implementation of Amicus. This readiness assessment should include a tested, documented back out plan.
- The Deputy Head should appoint an Amicus business owner immediately. The business owner should formally approve business requirements, ensure that test plans cover all the business requirements, and approve all test results.

Based on the current phase of the Amicus project, some recommendations would not have been appropriate at this time. Instead, we have provided them as opportunities for improvement for PPSC management to consider for future projects.

1.4 STATEMENT OF ASSURANCE

In my professional judgment as the PPSC's Chief Audit and Evaluation Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusion provided and contained in this report. The audit findings and conclusion are based on a comparison of the conditions, as they existed at the time of the audit, against pre-established and approved audit criteria that were agreed upon with the PPSC's management. The findings and conclusion are applicable only to the entity examined. The audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada.

I appreciate the cooperation and assistance provided to the audit team by the PPSC Amicus team in Headquarters.

Cathy Rodrigue
Chief Audit and Evaluation Executive

2. INTRODUCTION

2.1 BACKGROUND

PPSC's current legal case management system, iCase, encountered architectural, functional, and performance limitations which prevents improving system capabilities to support the evolving requirements for PPSC management and users.

As a result of extensive consultations with the business community and the subsequent management approval, the project to replace iCase was launched in January 2016 as the Legal Case Management System (LCMS). Some of the expected outcomes of implementing LCMS include: improve overall user satisfaction and experience with the system, improve data quality and integrity by introducing built-in business rules, and provide the ability to disseminate up-to-the-minute file and timekeeping information.

Given the significance and size of the project, audit conducted this system under development audit in three parts and launched the audit work in 2016.

In May 2019, IAED issued its System Under Development Audit Report on the LCMS Planning Phase. Subsequent to that report, the LCMS project was renamed as Amicus.

At that time, the IAED concluded that the project governance could be improved by assigning and acting upon responsibilities and accountabilities; implementing and/or complying with change, issues and risk management procedures; and timely updating and disseminating of information to stakeholders. IAED provided seven recommendations. Upon further examination, we found that management has implemented five of the seven recommendations. Internal controls, testing, and implementation are further assessed during this Amicus implementation audit.

The Amicus project incurred approximately a two-year delay resulting from several factors including, but not limited to, delays obtaining TB Authority, contracting delays, technical delays, the COVID-19 pandemic, and enhanced agent processing changes.

As a result of those delays, and in conjunction with changes to the scope, the project budget increased by approximately \$1,000,000 from approximately \$4.8 million to approximately \$5.4 million in 2022.

The current audit, System Under Development Audit Implementation Phase, began in June 2019 and was postponed in early 2020 due to the COVID-19 pandemic. The audit was re-started in February 2021. Then in late 2021, the audit was postponed again due to delays within the Amicus project itself. The audit restarted in February 2022.

2.2 OBJECTIVES AND SCOPE

The objectives of this audit were to provide management with an independent assessment of the progress, quality, and attainment of the Amicus project objectives at defined milestones within the project and an evaluation of the internal controls of proposed business processes during the various phases in the development cycle where enhancements can be easily implemented and processes adapted.

This audit focused on the implementation phase of the project leading to the system deployment. The audit took place between June 2019 and July 2022.

Although complete implementation of Amicus has not occurred, and could take the rest of the year, sufficient work has been concluded in order to assess the project for audit purposes. The audit only comments on the Amicus project up to the start of Phase 1 of the pilot testing for the Manitoba Region.

2.3 METHODOLOGY

The audit complied with the Institute of Internal Audit's generally accepted auditing practices and was conducted in accordance with the TB Policy on Internal Audit.

The audit methodology included, but was not limited to:

- interviews with:
 - the DG, AS and CIO;
 - the Project Manager;
 - Project team members;
- a review and analysis of the project documents;
- attendance at an Amicus training class; and,
- attendance at Amicus project team meetings.

3. OBSERVATIONS AND RECOMMENDATIONS

3.1 GOVERNANCE

Generally, management provided adequate governance over the project. However, changes to the project schedule were not always explained.

Roles and responsibilities of the project team were identified and appropriate subject matter experts and stakeholders actively participated on the project team.

The original scope of the Amicus project was defined and approved. Responsibility for managing scope changes was also defined and procedures were in place to obtain approval of scope changes from the project steering committee.

We have seen evidence that the Steering Committee reviewed and acted upon some change requests. However, there were meetings where the Project Manager notified the Steering Committee of possible changes in the project schedule without providing an explanation or reasons for changes in the project schedule, nor did the Steering Committee ask for a reason.

For example, during the development project new agent processing requirements were approved. The additional cost and resource requirements were presented to the Steering Committee. However, the Project Manager also indicated that even without the new agent processing requirements there would be an additional 30-day delay due to delays in testing and complications with data migration. The Steering Committee was not aware of this 30-day delay. Without learning why there are changes to project schedules, governance committees are at risk of proceeding with a project that may exceed its approved budget.

Recommendation #1

The DG, AS and CIO should provide the Steering Committee an explanation for changes in the project schedule as soon as they become aware of possible changes and impacts, including both time and cost.

3.2 PROJECT MANAGEMENT FRAMEWORK

The project management framework provided reasonable assurance that the project achieved its objectives, adhered to timelines, and stayed within budget. Although the framework was adequate, project management practices need improvement on risk management/reporting, contracting, milestone reporting, and financial controls.

We found that the Amicus project team reported on risks to the Steering Committee; however, the project team only identified that there were “no additional risks”. If there was a new risk, the project team named the new risk. There was no reporting on the risk exposures, measures in place to mitigate any risks, or the identification of outstanding risks. For example, at the February 18, 2021 Steering Committee meeting, the Amicus team reported that there was one item in the risk log related to GCdocs and there were challenges with integration. There were no further details on those risks provided.

System Under Development Audit of Amicus
Implementation Report

When receiving notice of a new risk, the Steering Committee was neither informed of a risk management plan nor about any level of risk accepted by the project team. Costs to mitigate risks or the benefits obtained after mitigating risks were not identified in the risk log.

There is no evidence of an escalation and follow-up process for monitoring project risk exceptions in place. The Amicus risk framework did not identify the risk owner, mitigation schedule, mitigation activities or potential consequences if the risk materialized. We found that not all risks were updated and not all issues were identified.

We found no formally approved contracting strategy or plan. The LCMS Project Management Plan does identify the type of resources to be contracted and provides a summary of a Procurement Management Plan. There was a LCMS Project Contracting Needs Summary, although the Summary had no date or approval. The Summary identifies five contracting requirements for ten resources but it does not identify when those resources would be required, when the contracting process should begin for each resource, and the approximate time required from Request for Proposal (RFP) issue to contract award for each contract. There were no milestones associated with each proposed contract.

We learned of two contracting issues. The first issue occurred in 2019, when the project team found the RFP process was taking longer than expected. A recent contracting issue for the security expert almost resulted in delays to the Pilot Test and Amicus not receiving its authorization to operate. In addition, there was no contracting plan identified in the Amicus reporting to the Steering Committee. This created a risk of further delaying Amicus implementation.

Effective project management includes the development and continuous updating of a project plan. The project plan is many things to the project manager. It is a record of what has occurred on the project. It illustrates what is currently happening on the project and it prepares the project team by showing what will be coming up. The approval of the project plan establishes a baseline target and the project proceeds.

A project plan should show the effect of changes in the cost, time, and scope on the overall project. Anytime one of those three elements changes it should generate a change to the project plan with the distribution of the revised plan to key stakeholders.

We found that after the August 2020 go-live date changed, updates to the Amicus project plans stopped. Presentations to governance committees reported on any further changes to the go-live dates. However, updates to the project plans did not occur to reflect those changes.

This exposed the project to the risk of confusion related to the implementation of the new system. Stakeholders may not have had a clear view of what happened and what was due to happen with Amicus.

Project plans should also identify project milestones and deliverables. Amicus project milestones/deliverables, as presented to the Steering Committee, only show that a milestone/deliverable was completed and its planned end date. The project plan does not show the actual completion date and, therefore, the Steering Committee cannot tell if the completion of a milestone/deliverable was on time or delayed. For example, the March 29, 2021 presentation to the Steering Committee identified that thirteen milestones were completed. However, the presentation only showed the planned end date of each milestone and not the actual date of completion. Therefore, the Steering Committee may not have been able to determine whether those milestones were completed on time.

Opportunities for improvement have been provided to address the deficiencies noted above as it would not be appropriate, or relevant, to have the corrections made at this time for Amicus.

3.3 CHANGE MANAGEMENT

A change management process documents a systematic approach to dealing with changes. However, there was insufficient detail describing emergency changes, prioritizing changes, and the handover from testing into production. In addition, there is no governance structure to support Amicus after implementation.

We reviewed a copy of the proposed high-level change management process planned for Amicus. This process requires documented approval from user management and system development for any suggested changes to Amicus. The change management process includes a Change Management Board (CMB), responsible for reviewing the risk and budget of any change and recommends proceeding with the change or rejecting the change. We found that user management and system development management are both on the proposed CMB.

There is also an Emergency Change Advisory Board, responsible for authorizing emergency changes to Amicus. However, it does not indicate to inform CMB of emergency changes. Adding emergency changes to Amicus could affect the changes going through the CMB and vice versa.

The change management overview shows that the Change Manager determines the priority of each change request. However, the overview does not describe the change review or change prioritization process. Nor does the overview identify a change schedule. We cannot determine whether changes will be implemented monthly, quarterly, semi-annually or on an ad-hoc basis. Based on the documentation, we cannot determine when in the change management process the cost of the change will be identified.

Change management should also include formal approval processes when implementing new systems. We found no formal approval process on the handover of Amicus into production. At the time of the audit, management was considering that the DG, AS and CIO of PPSC and the Chief Federal Prosecutor for each region will sign-off on the implementation in each region.

Change management requires an effective governance structure to support a new system after that system implementation. The PPSC does not currently have a business governance structure to support Amicus after implementation. This type of structure can decide whether to approve Amicus and whether to approve/reject business requirement changes. The DG, AS and CIO put forward this request to the Amicus Steering Committee on March 18, 2022 and identified this issue to the Department Audit Committee in March 2022. As of September 2022, there has been no approved governance structure to support Amicus after implementation.

Without a formal, post implementation governance structure and approval process for the handover into production, the project is at risk of implementing a system that may not meet the requirements of the Department. There are also risks that the capture, prioritization, and implementation of future changes may not occur. In addition, communication of new features between business areas and technology areas may not take place.

Recommendation #2

The DG, AS and CIO should document and implement a governance structure to formally process and approve the handover of Amicus to a region after successful pilot testing, and to support the system after implementation.

3.4 APPLICATION CONTROLS AND BUSINESS REQUIREMENTS

Application controls and business requirements are identified. However, business management has not formally approved those requirements. In addition, the DG, AS and CIO is the only official to approve test plans. Business management have not approved test plans.

Amicus team members developed Business Requirements Documents (BRD) identifying the initial requirements for the system. Although the BRDs were discussed with some users, we found that no business users signed off or approved those BRDs. The Amicus team has been working with what they believe are the business requirements.

We found that management, other than the DG, AS and CIO, did not approve test plans. There is no business management validating testing to ensure that all the user stories and functions were being adequately tested. Expectations are that once test plans are complete, functionality and development are complete, and Amicus is in a stable environment it will be easier to determine that all functions have been tested.

There is no evidence of the proper review of test results and approval by management and business owners. There is no actual business owner of Amicus, which is required in order for signoff from one testing stage to the next. However, there is a proposal to have the DG, AS and the Chief Federal Prosecutor of each region signoff on each pilot testing stage prior to initiating the next pilot test stage.

Recommendation #3

The Deputy Head should appoint an Amicus business owner immediately. The business owner should formally approve business requirements, ensure that test plans cover all the business requirements, and approve all test results.

Acceptance testing is the phase where the region decides Go/No-Go for Amicus before approving it for full production. The region assesses whether Amicus is working correctly for the region. Acceptance testing is conducted after Amicus is deployed and:

- focuses on how users will experience the software;
- determines to what degree Amicus meets end users' approval;
- ensures Amicus matches business requirements and end-user needs; and
- results in either a pass or a fail.

Acceptance testing should be scheduled after the pilot test in sufficient time to make any required changes prior to full deployment. Appropriate regional and national management should approve results of acceptance testing.

We have not seen an acceptance test schedule for Amicus. Without the acceptance test, regions are at risk of implementing a system that does not meet their key requirements.

Recommendation #4

The DG, AS and CIO should develop an acceptance test plan and execute an acceptance test with each region prior to full deployment of Amicus.

3.5 AMICUS IMPLEMENTATION

The Amicus team developed a project implementation approach. However, it does not include a documented back-out plan to maintain the integrity of the data. In addition, there is no tool developed to assess departmental readiness for implementing Amicus.

The Manitoba region will be the first region to use Amicus. Prior to full implementation, the Manitoba region will go through a four phase pilot test. Phase 1 will be a small pilot with very few Amicus files. Amicus and iCase will both have duplicate files between them; iCase will be the definitive source of information. Phase 2 will use a larger number of files and Amicus will be the definitive source of information. Phase 3 will be a full in-house launch of Amicus with full migration of all data into Amicus. Phase 4 will be the Agent launch. The project will freeze all non-critical business requests until September 2022. The Amicus team expects Phase 1 of the pilot test to take four weeks with no documented timeframe for phases 2-4; however, as of September 2022 Phase 1 has not been completed.

There is no governance structure to support Amicus after implementation. The governance structure decides on business changes and approves decisions about Amicus functionality and performance. The formation of the governance structure should be part of a readiness assessment. A readiness assessment identifies the potential challenges and solutions that might arise when implementing new procedures and new systems. Conducting a readiness assessment will give the PPSC the knowledge and assurance that the Amicus implementation will be successful. The readiness assessment will also provide the appropriate approval to continue with implementation. We are aware that the project team is supposed to develop a readiness checklist approximately one month prior to implementation. There is an agreement that for the Manitoba region, the Chief Federal Prosecutor and the DG, AS and CIO will jointly approve continuing with each pilot phase.

A back out plan enables both the project team and users the ability to stop using the Amicus pilot and revert to using iCase. Decision points used to determine whether PPSC has to back out of implementing Amicus would be included in a back out plan. The back out plan is only used in the event that Amicus encounters major problems during the pilot phase, acceptance test, or initial implementation. The back out plan is a safety net so that PPSC legal operations can continue to work even if Amicus does not work properly. With the phased pilot test approach, it will not be necessary to have a back out plan until phase 3 of the pilot test due to the limited amount of Amicus data used. However, there currently is no documented back out plan. This exposes the PPSC to the risk of not being able to work efficiently or effectively if Amicus fails.

Recommendation #5

The DG, AS and CIO in conjunction with the Chief Federal Prosecutor of each region should ensure that each region conducts and documents a readiness assessment prior to full implementation of Amicus. This readiness assessment should include a tested, documented back out plan.

4. OPPORTUNITIES FOR IMPROVEMENT

In addition to the recommendations included in this report, several other areas PPSC management should consider when undertaking future projects:

- Identify a business owner at the start of a project.
- Ensure a project risk framework identifies a risk owner, mitigation schedule, potential consequences if the risks materialize, costs to mitigate or the benefits obtained after mitigating risks, and the level of acceptable risk.
- Establish a contracting plan prior to starting a project and that the appropriate governance committees or management receives updates on the status of contracting.
- Ensure that project standards include updating project plans whenever there is a change to the cost, schedule or scope of any project. Updates of project milestones/deliverables noted in the project plans and presented to governance committees or management should show the planned completion date and the actual completion date of milestones.
- Document a change management process, which includes the definition of the different types of changes, detail process for emergency changes, detail description of prioritizing changes and the change schedule.

5. CONCLUSION

The IAED assessed the adequacy and effectiveness of the control framework surrounding the Amicus project implementation against predetermined audit criteria based on the Office of the Comptroller General of Canada's Core Management Controls.

Overall, the control framework is appropriate; however, there are opportunities for improvement in the following areas: governance over the project, project management, change management, risk management, business requirements development, and implementation.

Recommendations have been provided for those areas where changes would benefit the ongoing work related to management. Opportunities for improvement were provided for PPSC management to consider when undertaking new project; these address deficiencies noted during this audit but would not necessarily be appropriate or relevant to correct at this time for the Amicus project.

6. MANAGEMENT RESPONSE AND ACTION PLAN

RECOMMENDATION	MANAGEMENT RESPONSE AND ACTION PLAN	OFFICE OF PRIMARY INTEREST	TARGET DATE
<p>1. The DG, AS and CIO should provide the Steering Committee an explanation for changes in the project schedule as soon as they become aware of possible changes and impacts, including both time and cost.</p> <p>Risk: Medium</p>	<p>Management accepts this recommendation and will advise the Steering Committee as the information becomes available.</p>	<p>DG, AS</p>	<p>Immediate</p>
<p>2. The DG, AS and CIO should document and implement a governance structure to formally process and approve the handover of Amicus to a region after successful pilot testing, and to support the system after implementation.</p> <p>Risk: High</p>	<p>Management accepts this recommendation and will complete an implementation signoff checklist.</p>	<p>DG, AS</p>	<p>March 31, 2023</p>
<p>3. The Deputy Head should appoint an Amicus business owner immediately. The business owner should formally approve business requirements, ensure that test plans cover all the business requirements, and approve all test results.</p> <p>Risk: High</p>	<p>Management accepts this recommendation will appoint a business owner to fulfill these functions.</p>	<p>Deputy Director of Public Prosecutions</p>	<p>December 31, 2022</p>
<p>4. The DG, AS and CIO should develop an acceptance test plan and execute an acceptance test with each region prior to full deployment of Amicus.</p> <p>Risk: High</p>	<p>Management partially accepts this recommendation. An acceptance test plan will be formally developed and completed; however, it is unlikely that a full acceptance test plan be necessary or useful once it has been completed with a select few regions. The management actions for #2 and #5 should be sufficient to ensure sufficient individual regional readiness.</p>	<p>DG AS</p>	<p>March 31, 2023</p>

System Under Development Audit of Amicus
Implementation Report

RECOMMENDATION	MANAGEMENT RESPONSE AND ACTION PLAN	OFFICE OF PRIMARY INTEREST	TARGET DATE
<p>5. The DG, AS and CIO in conjunction with the Chief Federal Prosecutor of each region should ensure that each region conducts and documents a readiness assessment prior to full implementation of Amicus. This readiness assessment should include a tested, documented back out plan.</p> <p>Risk: High</p>	<p>Management accepts this recommendation and will develop this assessment checklist as part, or as a subset of the checklist in management action #2.</p>	<p>DG AS</p>	<p>March 31, 2023</p>

APPENDIX A – AUDIT CRITERIA

Audit Criteria

1. Management provides adequate governance over the project.
2. The project management framework ensures the project achieves its objectives, adheres to timelines, and stays within budget
3. Change management ensures a systematic approach to dealing with changes and issues associated with the implementation of Amicus
4. Application controls and business requirements are identified, implemented, and working as intended
5. A project implementation approach is developed and followed, including maintaining the integrity of the data and assessing Departmental readiness.

APPENDIX B - LIST OF ACRONYMS/ABBREVIATIONS

BRD	Business Requirement Document
CIO	Chief Information Officer
CMB	Change Management Board
DG, AS	Director General, Administrative Services
IAED	Internal Audit and Evaluation Division
LCMS	Legal Case Management System
PPSC	Public Prosecution Service of Canada
RFP	Request for Proposals
TB	Treasury Board of Canada