Government of Canada

Gouvernement du Canada

Targeted control audit of CARM business readiness: Appendices

← Previous page

Table of contents

On this page

Appendix A: Key stakeholders and their responsibilities

VP, Commercial and Trade Branch

Oversees CARM Project

Deloitte

Vendor responsible for delivering the CARM Solution

Department of Justice (Legal Counsel)

Provides legal advice upon request to CARM Team

Strategic Policy Branch

Supports CARM with legislative and regulatory amendments

Information, Science, and Technology Branch (ISTB)

Responsible for conducting security assessments for the CARM Solution and liaising on IT issues

Business and Project Readiness Implementation Division

Responsible for CARM business readiness, client service support, and CBRIB Secretariat

CARM Business Readiness and Implementation Board

Responsible for providing oversight of progress and accountability toward CARM business readiness and implementation

CARM Change Enablement Division

Responsible for training and innovation, stakeholder engagement, and program authorities

CARM Project Management Office

Responsible for the Integrated Project Plan, contract management, communication with TBS, enforcing contract terms with Deloitte

CARM Solution Delivery

Responsible for systems integrations, security management action plans, and managed services

Appendix B: About the audit

Audit objectives and scope

The objective of this audit is to assess the state of business readiness activities to support the operations impacted for R2 release of CARM in May 2022 (i.e. full implementation of the core CARM solution).

This audit was approved by the agency's Audit Committee as part of the 2021 risk-based audit plan.

The audit scope covered the period April 1, 2021, to September 30, 2021, including the completed and planned activities for the launch of CARM R2 in May 2022. This audit scope included:

- risk management practices across the agency in order to address CARM R2 risks across the agency

- progress toward elements identified as key to internal and external readiness to support the R2 release date (including business readiness plans)

- IT processes surrounding IT security for CARM R2

This audit scope did not include the following:

- any detailed examinations of business readiness activities related to R0 (January 2021) and R1 (May 2021) releases

    - these release activities served as a historical backdrop for R2 release activities but the audit did not examine the strengths or weaknesses for these CARM phases
    - additionally, contractor performance and the CARM budget were not examined

- assessment of activities and operations to be implemented and/or considered for a post R2 release or "steady-state"

    - these processes involve such things as vendor management once R2 has been released, and project teams created specifically for CARM steady-state

- examination of specific issues/challenges that contributed to the Vendor Solution build

Due to limitations surrounding the COVID-19 pandemic, there was no travel during this audit. However, all regions were included and some were contacted for interviews, survey and/or documentation requests.

Risk assessment

A preliminary risk assessment was conducted during the audit planning phase to identify potential areas of risk as well as audit priorities. Methodology used to develop the risk assessment included interviews with stakeholders involved in CARM, review of relevant documentation, and analysis of available reports. As a result of this assessment, the following key risks related to CARM business readiness were identified and used to develop the audit objective, scope and criteria:

- the governance structures in place may not adequately identify key risks to CARM in order to support timely risk-based decision making

- the agency may not have the required enabling legislation and regulatory measures in place to enforce the new TCP compliance requirements CARM will introduce by the planned launch date of May 2022

- the agency may be unable to track, monitor and/or document whether system integration and security issues are being followed; thus jeopardizing the authority to launch and operate the system

- the agency may not have key internal business readiness activities, such as training, operational impact assessments and client service capabilities, established or performed in a timely manner

- the agency may not be effectively engaging and/or communicating with external stakeholders to ensure that training, CARM registration and key IT system requirements are in place in order to ensure that external stakeholders are ready to use CARM

Approach and methodology

The audit was conducted in accordance with the Directive on Internal Auditing and the Institute of Internal Auditors' Standards for the Professional Practice of Internal Auditing.

The examination phase of this audit was performed using the following approach:

1. interviews with key stakeholders including CARM Directorate personnel, and most affected program areas such as:

   - Trade and Anti-Dumping Programs Directorate (TAPD)
   - Commercial Programs Directorate (CPD)
   - agency Comptroller (FCMB)

2. review of relevant documentation including but not limited to:

   - internal and external business readiness
   - governance related documents such as terms of reference and records of decision, and meeting minutes from working committees
   - risk dashboards, status reports, and deck presentations related to CARM
   - systems integration and security assessment and accreditation processes

3. assessment of processes and procedures in place, as well as validation of key controls in place

Audit criteria

The following lines of enquiry and audit criteria were developed to assess the areas of risk.

Line of enquiry	Audit criteria
1. Risk Management Processes/Procedures	1.1 A risk management process is in place that effectively identifies, assesses, communicates and monitors key CARM R2 risks in order to enable the agency to support effective risk-based decision-making
2. Internal and External Readiness	2.1 Internal business readiness activities are being executed in a timely and effective manner to support the release of CARM R2
	2.2 External readiness activities are in place and being implemented in an effective and timely manner in order to support adoption by external stakeholders and Trade Chain Partners
3. IT Systems Integration and Security	3.1 Systems Integration work is performed as planned, and managed to proactively address risks
	3.2 Security Assessments are being managed in a manner to ensure the mitigation of challenges for R2 go-live

Appendix C: List of acronyms

ARL

Accounts Receivable Ledger

ARMB

Annual Regulatory Modernization Bill

BIA

Budget Implementation Act

CARM

CBSA Assessment and Revenue Management

CBRIB

CARM Business Readiness and Implementation Board

CBSA

Canada Border Services Agency (the agency)

CCSH

CARM Client Service Helpdesk

CPB

CARM Project Board

CSAR

Critical Security Assessment Report

CSP

Cloud Service Provider

CTU

CARM Training Unit

EC

Executive Committee

FIMC

Finance and Investment Management Committee

FSAR

Final Security Assessment Report

GC

Government of Canada

IPP

Integrated Project Plan

ISTB

Information, Science, and Technology Branch

IT

Information Technology

OAG

Office of the Auditor General

OIA

Operational Impact Assessment

PACP

Standing Committee on Public Accounts

PMF

Project Management Framework

R1

Release 1

R2

Release 2

ROD

Record of Decision

SOW

Statement of Work

SA&A

Security Assessment and Accreditation

SMAP

Security Management Action Plan

SPB

Strategic Policy Branch

TCP

Trade Chain Partner

TBS

Treasury Board Secretariat

TOR

Terms of Reference

TRAS

Tariff Risk Assessment Service

UAT

User Acceptance Testing

VP

Vice-President

← Previous page | Table of contents

Date modified:

2023-01-06