

**QUESTIONS AND ANSWERS
ADDENDUM #3**

RFP # 2020-2166

-
- 1. Title** SharePoint Migration to Microsoft Office 365 (O365)
Addendum #3
-
- 2. Requests for Clarification** The following questions and answers are added as an addendum to CDIC RFP 2020-2166
- Q1. Page 10, Section: 2 Statement of Work, states: “CDIC has completed an O365 migration roadmap (the “Roadmap”) and is now looking to engage with an independent party to perform the execution. Scope and approach have already been defined and the details are provided below.”**
- A) Did CDIC engage with a vendor to complete the Roadmap?**
B) If CDIC did engage with a vendor, is the vendor eligible to respond to this RFP?
C) If CDIC did engage with a vendor, can you share the name of the vendor?
D) If CDIC did engage with a vendor, did the vendor provide to CDIC an estimate to complete a portion of or all of the scope of this RFP?
- A1. For responses to A-C, bidders should refer to Addendum #1.
- The vendor who completed the Roadmap did not provide an estimate to complete this project.
- Q2. Page 11, Section: 2 Statement of Work, Heading: Configuring O365, states: “Configure event logging and forward the logs to a Security Information and Event Management (SIEM)”.**
- A) Is a SIEM already in place?**
B) If so, which SIEM is currently being used?
C) If a SIEM is not currently in place, can/should the respondent suggest a SIEM?
- A2.
- A) Yes, there is a SIEM in place already.
B) ArcSight.
C) Not applicable
- Q3. Does CDIC currently have a managed service provider for O365? If not, what are the plans to manage and support O365?**

The complete and official copy of this Addendum #3 to RFP # 2020-2166 can be found at no cost at Buyandsell.gc.ca

A3. CDIC is managing O365 with internal resources.

Q4. Could you please confirm if the resource must be fluent in English or French? Also, where should the work be performed?

A4. The Project Manager and proposed team members must be fluent in English. The work will be performed remotely and at CDIC's offices in Ottawa and Toronto.

Q5. How many external and Internal users will use the O365 new sites ? How many user groups are there for current system ?

A5. About 175 internal and 40 external users will use O365 new sites, the external users may fluctuate based on need. There are 1000 user groups in our current system, however many of these are currently inactive and will need to be cleaned up as part of the project.

Q6. External access and 3rd party sharing - What information will be accessed by outsiders ? What security requirements are needed for this activities?

A6. Protected B will be the highest classification level applicable to federal crown corporations for external sharing and the security requirements would be :

- CDIC protected data cannot be stored outside of Canadian data centers
- CDIC protected data should be encrypted in transit (TLS 1.2) and at rest (AES-256)
- Only authorized users have access to the CDIC data based on need to know and least privilege. Here are some examples of the controls:
 - o MFA authentication for external users and third party sharing
 - o Ability to restrict Editing/Copy/Paste/Printing to documents
 - o Ability to set Time to live for the documents shared with external
 - o Ability to revoke access to data shared with external users if access is no longer needed or data was shared by mistake
 - o Ability to restrict Sending/Forwarding emails based on data classification
 - o Ability to watermark classified documents
- All security events for external access and third party sharing are logged and forwarded to a SIEM solution
- All documents received by a third party or uploaded by an external user should be scanned for malware

Q7. What type application development process followed at CDIC - Waterfall or Agile?

The complete and official copy of this Addendum #3 to RFP # 2020-2166 can be found at no cost at Buyandsell.gc.ca

- A7. The application development process followed at CDIC is mostly agile.
- Q8. Section - 1 Background and Objectives : Page 9:How is the searching of documents planned in physical format?**
- A8. CDIC is planning to utilize a third-party tool which will provide the functionalities including search features to support the management of paper records.
- Q9. Section - 1 Background and Objectives : Page 10: Will migration of Data involves only 470 GB of SharePoint? Or the content on network drives data (7TB) as well to be considered**
- A9. The migration of data will involve both content from SharePoint and network drives. However, a cleanup exercise is in the scope of the project and must be performed on the network drives in order to delete transitory information prior to migration. CDIC is expecting the selected candidate to execute the content cleanup.
- Q10. Section - 1 Background and Objectives : Page 10: Is user adoption, change management in vendor scope? If so How do you quantify for efforts estimations ?Please let know if a custom user experience is required ? And Elaborate the same**
- A10. Yes, user adoption and change management are in scope and will include, but are not limited to: communication strategy, training content development, training delivery. CDIC has about 175 employees in 4 divisions. A custom user experience is not required.
- Q11. Section - 2 STATEMENT OF WORK : Page 10 : Is setup and configuring One drive and MS Teams in scope of Vendor ?**
- A11. Yes, the setup and configuration of OneDrive and MS Teams are in scope.
- Q12. Section - 2 STATEMENT OF WORK : Page 10 : Please elaborate Digitization of records ? How it has to be carried out ? Quantify the records?**

The complete and official copy of this Addendum #3 to RFP # 2020-2166 can be found at no cost at Buyandsell.gc.ca

A12. CDIC holds approximately 6,000 boxes (about 7,476.00 Cubic Foot) of inactive files and is looking at digitizing them. The selected candidate will provide advice and guidance based on best practices to manage a digitization project. This will include, but are not limited to:

- Define organizational business requirements to move towards digitization.
- Develop digitization process.
- Review, update and or develop digitization standard and procedures (metadata, image standards, etc).

Q13. Section - 2 STATEMENT OF WORK : Page 11 : Are you ok to host apps on Azure in case equivalent customizations could not be established on O365 (PaaS/IaaS based Applications)? Also are you ok to leverage other O365 services ?

A13. No, CDIC does not want to use any application other than the custom applications/forms created through Microsoft's O365 AppSource. However, CDIC is open to leverage other O365 services.

Q14. Section - 2 STATEMENT OF WORK : Page 11 : What type of content clean up is required? Please elaborate?

A14. The content clean up is in the scope of the project and is about the deletion of transitory information on network drives and SharePoint sites prior to migration. (for example inactive files designated as superseded, drafts, duplicates, personal files, etc.). We are expecting the selected candidate to facilitate the cleanup and identify content to migrate.

Q15. Section 3.2 : Design : Page 13 : Can you please share details / functions involved in 20 major function site collections

A15. Below is a non-exhaustive list of 20 major function sites collections :

1. Governance

Work conducted to ensure the successful and accountable delivery of all CDIC functions.

2. Audit Management

Implementing and participating in formal oversight activities by both internal and external authorities, in accordance with professional internal standards, necessary to demonstrate or protect the integrity of CDIC.

The complete and official copy of this Addendum #3 to RFP # 2020-2166 can be found at no cost at Buyandsell.gc.ca

3. **Acquisition Management**
Maintaining a rapport with the vendor community, identifying requirements for externally furnished services and assets, and the procurement, use, maintenance and disposal of services and assets that become possessions of or enter the control of CDIC.
4. **Communications**
Maintenance of an informed and effective relationship between CDIC and different elements of the internal and external stakeholder community.
5. **Financial Resources Management**
In accordance with International Financial Reporting Standards (IFRS), controlling incoming and outgoing funds, investing against corporate and ex-ante (operational) requirements, providing for sufficient funds to meet all obligations. Includes: All financial management materials pertaining to other CDIC functions.
6. **Human Resources Management**
Includes activities associated with: recruitment and selection processes, training and development, performance assessment, occupational safety and health, employee relations, compensation and benefits, human resources planning and utilization, classification, official languages, employment equity, personnel security and special programs.
7. **Information Management**
Ensuring the life cycle management of CDIC information resources, regardless of medium, to support the performance of all other functions, as well as compliance with legal and accountability obligations.
8. **Information Technology Services**
Enabling the functions of CDIC through project-based implementation of Information Technologies, and the regular deployment of up-to-date IT solutions.
9. **Facilities Management**
The life cycle management of all Facilities, acquired as a result of Projects or other means, involving the management of the Facility's configuration, the conduct of operations and maintenance.
10. **Security Management**
Assurance of a secure working environment in which CDIC functions may be performed, protecting personnel, facilities, information, and technology from disruption, harm, disturbance or injury.
11. **Assets Management**
The life cycle management of all tangible assets owned and/or used by CDIC, maintained to minimize costs, maximize availability, and minimize risk of theft and misuse, involving the receiving and registration of new assets, ad hoc stocktaking, and the release of assets to business units and employees.
12. **Policy Management**
Development, maintenance and interpretation of the formal policy framework that mandates, governs and constrains CDIC's administrative functions.

The complete and official copy of this Addendum #3 to RFP # 2020-2166 can be found at no cost at Buyandsell.gc.ca

13. Member Management
The development and maintenance of mutually informative long-term relationships with Member institutions, enabling the fulfilment of other CDIC operational Functions.
14. Compliance Management
The methodical administration of certain sections of the CDIC Act, its By-laws and FIC obligations, with which Member institutions must comply, resulting in the receipt and analysis of both non-financial and financial information submissions from Members.
15. Member Data Management
The regular effort to gather and analyze data and related information from members for the purpose of risk assessment, insurance determination, compliance, policy development and intervention and preparedness planning.
16. Risk Assessment
The monitoring and communicating on the condition of CDIC Member Institutions in order to identify early warning signs of risks to depositors, and by extension, to CDIC.
17. Emerging Risk Management
Forward-looking assessments of risk-related issues and related research, primarily for proactive submission to or in response to requests from the Board or Senior Management.
18. Insurance
Under the Differential Premiums By-law, the classification of a Member, the determination and documentation of the terms of depositor insurance, and the administration of the resulting premium payments and any related delinquencies.
19. Intervention Management
Annual work to prepare for possible instances of Domestic Systemically Important Bank (DSIB) and non-DSIB Member Intervention and, when required, actual cases of Member Resolution.
20. International Affairs
Involvement in non-Canadian organizations, governmental and otherwise, with whom CDIC shares an interest in maintaining a stable financial environment, to advance and align policies.

Q16. Are there any file being used which does not natively support for information classification /Protection - Ex: .txt ? Please clarify

A16. CDIC mainly uses Microsoft Office Suite (Word, Excel, PowerPoint, Outlook), PDF, JPG files and a very few amount of text files (.txt)

The complete and official copy of this Addendum #3 to RFP # 2020-2166 can be found at no cost at Buyandsell.gc.ca

Q17. attachment_1_o365_roadmap-en : Section - Backup and Restore : Page 19 : Will the retention happen in O365, Is there any archival system planned by CDIC ? For multiple years retained data , which 3rd party tool CDIC prefers ?

A17. The retention will happen in O365 in the first place. CDIC is also expecting the selected candidate to suggest a records management 3rd party tool compatible with SharePoint Online which will meet CDIC needs in terms of records management.

Q18. Can you share the name of the company that completed the roadmap that is part of the bid package?

A18. Please refer to Addendum #1 for a response to this question.

Q19. Do you have a rough schedule or timeline for the completion of this migration?

A19. Approximately 10 to 12 months.

Q20. Is there a budget or other financial guideline we should work within?

A20. This RFP is a competitive process where Bidders Technical and Financial Offers are evaluated against the project requirements of CDIC. Bidders should provide their best price for the technical works they are proposing.

Q21. The implementation of software solutions can vary widely depending on project budget. Our firm has successfully delivered projects across various budget ranges. To help us best meet the goals of your solicitation, can you please approximate the anticipated budget range for this project? For example, is the approved or anticipated budget range:

- a. Less than \$100,000
- b. \$100,000 – \$150,000
- c. \$150,000 – \$250,000
- d. \$250,000 – \$350,000
- e. \$350,000 - \$500,000
- f. \$500,000+

A21. Please refer to A20 for a response to this question.

The complete and official copy of this Addendum #3 to RFP # 2020-2166 can be found at no cost at Buyandsell.gc.ca

Q22. We are a Microsoft SharePoint Deployment and Planning Services (SDPS) Provider; do you have any Microsoft Software Assurance vouchers that might be applied to the budget?

A22. No

Q23. Remote project delivery typically enables us to reduce project duration and costs. Most of the projects we do *could* be delivered 100% remotely however, we sometimes find it useful to be onsite during discovery meetings, training, etc. Considering the potential effect on project duration, resource availability, and cost on a scale from 1 to 5 where 1 represents "100% onsite project delivery" and 5 represents "100% remote project delivery", what are your requirements on this continuum?

A23. On a scale from 1 to 5 where 1 represents "100% onsite project delivery" and 5 represents "100% remote project delivery", CDIC's requirements on this continuum is 3. The work will be performed remotely and at CDIC's offices .

Q24. Do you already own any SharePoint-related products (e.g. ShareGate, Nintex, etc.) and if so, which ones?

A24. No, CDIC does not own any SharePoint related products to be brought into SharePoint Online. CDIC does use Collaboris' Doc Read on its SharePoint 2010 environment, but CDIC doesn't have any intention on bringing it into its SharePoint Online environment.

Q25. On a scale from 1 to 5 where 1 represents "None" and 5 represents "Expert", can you please indicate what SharePoint/O365 skills you currently have in house in terms of:

- a. Infrastructure, Administration and Maintenance
- b. Information Architecture Design and Implementation
- c. Content Owner/Authorship
- d. PowerShell and C# Development

A25.

With respect to SharePoint specifically, CDIC 's skill level is:

- a. Infrastructure, Administration and Maintenance: 2
- b. Information Architecture Design and Implementation: 1
- c. Content Owner/Authorship: 2

The complete and official copy of this Addendum #3 to RFP # 2020-2166 can be found at no cost at Buyandsell.gc.ca

d. PowerShell and C# Development: 3

With respect to general O365/Azure, CDIC's skill level is:

a. Infrastructure, Administration and Maintenance 2

b. Information Architecture Design and Implementation 0

c. Content Owner/Authorship 0

d. PowerShell 2 and C# Development 0

Q26. How many users should we account for as it relates to product pricing, implementation services scoping, etc.?

A26. About 175 internal and 40 external users will use O365 new sites, the external users may fluctuate based on need.

Q27. On a scale from 1 to 5 were 1 represents no Information Architecture and 5 represents a comprehensive Information Architecture including all necessary Document/Content Types and Term-Sets to fully support the solution in areas such as search, workflow, records management (i.e. retention policies), etc., how would you rank your current Information Architecture?

A27. CDIC rank would be 2.

Q28. Regarding your Records Management requirements:

- a. Can you please provide details about or a copy of your retention schedule/file plan including the number of record categories/series/types?
- b. How are Physical Records currently managed?
- c. Can you please provide details about the storage of Physical Records (e.g. # of locations, cabinets, containers, folders, documents, etc.)?
- d. Are you familiar with and/or interested in any of the Records Management Add-on products for O365 such as RecordPoint?

A28.

a. A copy of FAABI which is CDIC's current file plan and retention schedule is attached to this Addendum 3. It was approved in 2016 but never implemented

The complete and official copy of this Addendum #3 to RFP # 2020-2166 can be found at no cost at Buyandsell.gc.ca

and now needs to be revised to align with the new ISDA as well as CDIC's new Centre of Excellence division.

b. All files created by the Records Centre are captured in Meridio. However, since Meridio doesn't have a way to manage boxes CDIC lists dormant files and their respective boxes in Excel.

c. A small portion of Records are kept onsite in the files room and in CDIC's basement storage area. CDIC has approximately 6000 boxes stored offsite (the bulk are in Ottawa and a little under 200 are located in Toronto). There is roughly dozen cabinets spread across the two floors of CDIC's office in Ottawa. CDIC has approximately 74 000 dormant files. CDIC has 140 934 paper documents according to Meridio. CDIC has 335 electronic documents in Meridio.

d. CDIC is interested in Records Management Add-on products.

Q29. Can you please provide detailed requirements, scope, and use cases for the requirement stated as "Digitization of records"?

A29. Please refer to A12.

Q30. We utilize a proprietary utility to deploy an O365 Intranet comprised of Modern Team, Communication, and Hub Sites from an Excel workbook including the branding, taxonomy, 3rd party products, etc. The use license for the utility depends on the number of "Teams" you have, wherein a Team can be a Department, sub-department/Business Unit, committee, board, project, region, office location, etc. Can you please estimate the number of Team Sites that will be needed and/or provide a comprehensive Org Chart to assist us in estimating the cost?

A30. CDIC has about 175 employees in 4 divisions. The estimated number of team sites is approximately 35 to 40.

Q31. What is your vision for post implementation support in terms of anticipated number of hours per month?

A31. CDIC is planning to use its internal resources for post implementation support.

Q32. Is CDIC open to part of the work on the contract being performed outside the United States, if we can demonstrate significant benefits such as cost advantage, accelerated deliverables and/or other benefits?

The complete and official copy of this Addendum #3 to RFP # 2020-2166 can be found at no cost at Buyandsell.gc.ca

A32. No. The Project must be completed in Canada. All data (including cloud servers) must remain in Canada. Please refer to A6.

Q33. General

- i. What is the number of images or videos stored in SharePoint 2010 environment?**
- ii. What will be the total size of images and videos stored?**

A33.

i. Out of CDIC's approximately 400,000 files on its SharePoint 2010 system, around 20,000 of them are pictures and video taking up around 30 GB of space. However, a good portion of these files are quite old and likely won't be migrated. The same information for only the last 7 years works out to 12,000 pictures and video taking up around 25 GB of space.

Q34. Are there any timer jobs, event receivers deployed in SharePoint 2010 environment? If yes, then please confirm the number of timer jobs?

A34. The bulk of the timer jobs and event receivers are the defaults with the installation and maintenance of SharePoint, though there are some custom they are no longer in use. There isn't any custom timer jobs or event receivers needed moving forward at this point, unless recommended.

Q35. RFP – Background and Objectives

- i. Which all document file types are stored in SharePoint 2010?**
- ii. Is versioning enabled on the documents stored in SharePoint 2010?**
- iii. If yes, do we have to consider migration of versions from SharePoint 2010 to O365?**

A35.

- i. Refer to A16
- ii. Yes, versioning is enable on the documents stored in SharePoint 2010.
- iii. Yes.

Q36. O365 Roadmap –Workflow

Out of the 48 workflows, what is the number of running workflow instances?

A36. There are 405 running workflow instances for those 48 workflows.

The complete and official copy of this Addendum #3 to RFP # 2020-2166 can be found at no cost at Buyandsell.gc.ca

Q37. O365 Roadmap – Custom Solutions

How many of the custom solutions are Farm Solutions and how many of them are sandbox or client-side code solutions? Please confirm.

A37. All of CDIC's custom solutions to date have been farm solutions, not sandbox or client-side code solutions. In either case, CDIC does not intend on having these custom solutions going forward. Some are no longer needed and the rest can be replicated in SharePoint Online Out Of The Box features, or using Flow, PowerApps, etc.

Q38. O365 Roadmap – Forms

- i. As per the roadmap document few of the InfoPath forms will be converted to PDF. Please confirm no edit operations are expected on those PDF forms.**
- ii. Does the data related to InfoPath forms stored in SharePoint 2010 need to be considered for migration?**

A38.

- i. These forms that will be converted to PDF are solely for archiving purposes, they do not need to be editable.
- ii. Yes, the data from the old InfoPath forms will need to be migrated and archived as well.

Q39. O365 Roadmap – Third Party Tools – PointFire

- i. How is the multilingual scenario currently handled in SharePoint 2010? Is it through third party tools or handled explicitly through code?**
- ii. Is PointFire third Party tool finalized for multilingual translation or other third-party tools/custom solution need to be evaluated?**
- iii. Do we have to consider automatic translation of content stored in English to French or vice versa when user selects language in O365 environment?**

A39.

- i. The multilingual scenario in SharePoint 2010 is currently handled using Variations within the SharePoint platform.
- ii. PointFire has been recommended to CDIC while in the discovery phase of the project. CDIC intends on using PointFire at this stage, but are open to discussions with the vendor about other products.
- iii. Content (i.e. Documents) stored on SharePoint in English does not have to be automatically translated, nor vice-versa. The chosen language should affect elements such as navigation, intranet pages, and SharePoint settings/functions such as the ribbon.

Q40. O365 Roadmap – Learning

How many users are expected to be using the system?

A40. Please refer to A5 for a response to this question.



Function and Activity Based Information (FAABI) File Classification System (FCS)

with Security Classifications and Retention Periods

User's Guide

June 20, 2017

Table of Contents

Introduction to Function and Activity Based Information (FAABI)	3
A. Internal Functions (16).....	4
01 Governance	4
02 Audit Management	6
03 Policy Management – Administrative	7
04 Policy Management – Operational	8
05 Support - Board	8
06 Support - Executive Security: (U), Retention: 6 years	9
07 Committee Management.....	9
08 Acquisition Management.....	10
09 Communications	11
10 Financial Resources Management	13
11 Human Resources Management.....	14
12 Information Management	16
13 Information Technology Services.....	17
14 Facilities Management.....	19
15 Security Management.....	19
16 Asset Management	21
B. Operational Functions (9)	22
17 National Affairs	22
18 International Affairs	22
19 Member Management.....	23
20 Compliance Management.....	24
21 Member Data Management	25
22 Risk Assessment	26
23 Emerging Risk Management	27
24 Insurance.....	27

Function and Activity Based Information (FAABI) File Classification System (FCS) User Guide

Unclassified

25	Intervention Management.....	28
----	------------------------------	----

Introduction to Function and Activity Based Information (FAABI)

In most organizations, subjects come and go and organizational structures are always changing over time, but the organization's support functions and mandated are relatively very stable.

A function-based **File Classification System** (FCS), versus a subject-based Classification System, is a model of what an organization does and how it does it. It involves the identification and documentation of each business Function, Sub-Function and Activity, from which transactions, data, documents, records and Information Resources (IRs) arise. An FCS is also the approach the Treasury Board Secretariat (TBS) is using for the Government of Canada.

At CDIC, the FCS simply aims to standardize the way information is gathered and organized.

There are two main types of functions at CDIC: **Internal Functions** and **Operational Functions**.

The **Internal Functions** are the manner in which CDIC executes its various activities that are based on its corporate goals and objectives to supports its mandate. In other words, to "run the business."

01	Governance	09	Communications
02	Audit Management	10	Financial Resources Management
03	Policy Management – Administrative	11	Human Resources Management
04	Policy Management – Operational	12	Information Management
05	Support - Board	13	Information Technology Services
06	Support - Executive	14	Facilities Management
07	Committee Management	15	Security Management
08	Acquisition Management	16	Assets Management

The **Operational Functions** are performed in order for CDIC to meet its mandate.

17	National Affairs	22	Risk Assessment
18	International Affairs	23	Emerging Risk Management
19	Member Management	24	Insurance
20	Compliance Management	25	Intervention Management
21	Member Data Management		

A. Internal Functions (16)

01 Governance

Work conducted to ensure the successful and accountable delivery of all CDIC functions.

01-01 Corporate Planning Security: (U) or (B) Retention: 6 years

The annual development and renewal of planning instruments that allow CDIC to focus and prioritize its administrative and operational resources. Includes: The development of the corporate budget, which includes making provision for Operating Expenses (OpEx) and Ex-Ante funding, and the identification of strategic initiatives to be undertaken by Business Units.

Initiation
Consultation
Drafting
Approval

01-02 Operational Planning Security: (U) or (B) Retention: see below

Definition of strategic initiatives, determination of annual Business Unit-level plans and performance indicators, and identification of the best approach for achieving those goals, in line with the Corporate Plan and Budget.

Intelligence Retention: 6 years
Initiation Retention: 2 years
Consultation Retention: 2 years
Drafting Retention: 2 years
Approval Retention: 2 years

01-03 Enterprise Risk Management Security: (A) Retention: 6 years

The identification of CDIC risk factors, the formulation of mitigating strategies to be implemented by the business units, and the quarterly monitoring of risk reduction relative to pre-established indicators. Includes: Development of the CDIC Business Continuity Plan (BCP) to ensure that critical business functions may be maintained in the event of a disaster. Excludes: Risk management activities specific to a business unit (see "Operational Planning").

Identification
Mitigation
Monitoring

01-04 Control-Financial Security: (A) or (B) Retention: 6 years

The mapping, analyzing and testing of financial processes and controls necessary to ensure employee adherence to CDIC financial policy, establishing and exercising an ICFR framework. Excludes: Audits of business processes (see "Audit/Assurance").

01-05 Representation by Organization Security: (U) or (A) Retention: 6 years

Negotiating and establishing terms of reference and other expectations of CDIC participation in external organizations such as the RPWG, SAC WG, foreign regulators, Association of Departmental Assurers, GC Round-table of Auditors etc.

01-06 Reporting-Performance Security: (U) or (A) Retention: 6 years

Preparation and submission of all reports to internal authorities demonstrating the administrative and operational performance of business units and CDIC overall.

01-07 Reporting-Compliance Security: (A) Retention: 6 years

Coordination, preparation and submission of all reports to external authorities demonstrating CDIC compliance with law and policy. Includes: ATIP reports, reports approved for submission by Committees, and those submitted to the Board and therefore included in the agenda and minutes of Board meetings.

01-08 Issue Management Security: (U), (B) or (S) Retention: 6 years

Responses to inquiries and complaints from the general public, depositors, employees and stakeholders about CDIC's role, services and programs. Includes: Referral of inquiries to specific Business Units and review by Legal Services.

*Initiation
Consultation
Drafting
Dissemination*

01-09 Proactive Disclosure Security: (U) Retention: 2 years

The gathering and publishing information, as required by law and policy, thus reducing the number of informal and formal requests for access to CDIC information. Includes: The reconciliation and publication of the President's expense statements.

01-10 ATIP Response

Security: see below

Retention: 2 years

The handling of and response to formal requests for CDIC information assets. Includes: ATI Consultations, ATI Requests, Privacy Requests and Parliamentary Questions (PQ). Excludes: Litigation related to a request.

Request

Security: (U)

Consultation

Security: (A) or (B)

Review

Security: (A) or (B)

Dissemination

Security: (U)

01-11 Advice-Legal

Security: (B – Client Privilege)

Retention: 12 or 25 years

The investigation of significant administrative and operational matters resulting in formally prepared opinions, written comments about those matters, the revision of documents, and verbally delivered guidance, supporting particular CDIC Functions and decisions. Note: Most cases of Advice-Legal are designated 'Solicitor-Client Privileged' and Protected B. Includes: Briefings to the Board and to Board Members included or not in agenda packages.

General

Corporate Governance

01-12 Litigation

Security: (B – Client Privilege)

Retention: 12 or 25 years

Protection of the integrity of CDIC, against Member institutions and other parties, in all administrative and operational matters, whether cases proceed to court or are settled in an alternative manner, both as plaintiff and as defendant, typically lead by External Counsel. Includes: Investigations.

02 Audit Management

Implementing and participating in formal oversight activities by both internal and external authorities, in accordance with professional internal standards, necessary to demonstrate or protect the integrity of CDIC.

02-01 Planning

Security: (A) or (B)

Retention: 10 years

The yearly identification of auditable entities or centres (of which there are approximately 94, forming an 'audit universe'), their scoring relative to corporate objectives, and their prioritization for study over a 5 year cycle. Includes: The integration of ad hoc consulting assignments into the Annual Plan.

02-02 Assurance Security: (A) or (B) Retention: 6 years

Planned and formal evidence-based assignments involving notification of a Business Unit, assignment of a resource to the assignment, holding a kick-off meeting, fieldwork (gathering data and documents and conducting interviews and inspections), drafting, review and presentation of findings to the Audit Committee or the Board. Includes: Hypothetically, investigations into possible wrong-doing by employees.

02-03 Consulting Security: (A) or (B) Retention: 3 years

Ad hoc assignments, of varying scope, assisting a Business Unit in the identification of solutions to problems typically identified by that Business Unit.

02-04 Follow-up Security: (A) or (B) Retention: 3 or 6 years

Monitoring the implementation of recommendations made in assurance and review cases, and reporting progress to the Audit Committee.

03 Policy Management – Administrative

Development, maintenance and interpretation of the formal policy framework that mandates, governs and constrains CDIC's administrative functions. Includes: Tools, such as forms and templates that embody CDIC practices.

03-01 Policies Security: (U) or (A) Retention: 6 years

The development, drafting, approval, interpretation and renewal of CDIC policies, approved by the Board. Includes: Instruments that are reviewed and approved by the Board that mandate practices, and policies and procedures (e.g. Security Policy and handling procedures, some HR Policies, etc.) Excludes: Informal instruments, not approved by the Board but sometimes referred to as 'policies'.

03-02 Standards and Procedures Security: (U) Retention: 6 years

The development or adoption and maintenance of standards and procedures, approved by Heads of Business Units, which specify the level of quality or achievement or which define or limit work options to a single pre-established approach.

03-03 Tools Security: (U) Retention: 6 years

The development and maintenance of methodologies, processes, architectures, models, templates and samples facilitating productive and efficient work.

04 Policy Management – Operational

Development, maintenance and interpretation of the formal policy framework that mandates, governs and constrains CDIC's operational functions. Includes: Tools, such as forms and templates, which embody CDIC practices.

04-01	Legislation and Regulations	Security: see below	Retention: 20 years or permanent
--------------	------------------------------------	----------------------------	---

The interpretation and renewal of the CDIC Act and any other legislation that defines the CDIC's mandate.

<i>Initiation</i>	Security: (U) or (B)
<i>Consultation</i>	Security: (U)
<i>Drafting</i>	Security: (S)
<i>Submission for Approval</i>	Security: (U)
<i>Implementation</i>	Security: (U)

04-02	By-Laws	Security: see below	Retention: 20 years or permanent
--------------	----------------	----------------------------	---

The interpretation and renewal of By-laws that define the operational functions of CDIC.

<i>Initiation</i>	Security: (U) or (B)
<i>Consultation</i>	Security: (U)
<i>Drafting</i>	Security: (B)
<i>Submission for Approval</i>	Security: (U)
<i>Implementation</i>	Security: (U)
<i>Monitoring</i>	Security: (U)
<i>Interpretation</i>	Security: (U)

04-03	Guidelines, Procedures and Tools	Security: (U)	Retention: 6 years
--------------	---	----------------------	---------------------------

The adoption or development, drafting, approval, interpretation and renewal of CDIC guidelines, procedures, methodologies, models, samples, templates and forms establishing methods and facilitating productive and efficient CDIC functions.

<i>Initiation</i>
<i>Consultation</i>
<i>Drafting</i>
<i>Implementation</i>

05 Support - Board

Services provided to the Board to facilitate its effective, expeditious and evidence-based decision-making.

05-01 Governance Security: (U) Retention: 6 years

The empowerment of the Board by statute and its occasional clarification.

05-02 Orientation Security: (U) or (B) Retention: 6 years

The briefing of new Board Members regarding all aspects of CDIC organization and its functions, as well as any immediate issues that the Board Member must address.

05-03 Logistics Security: (U) Retention: 6 years

The coordination and forecasting of facilities, travel, schedules and other elements necessary for the effective communication of CDIC Executives with the Board and for the conduct of regular Board meetings.

05-04 Correspondence Management Security: (B) Retention: 6 years

Forwarding, upon reception, of correspondence to the Board, either because it is addressed to the Board, because it will inform Board decision-making, or because it seeks or requires a response from the Board. Includes: The forwarding, upon reception, of any requests for briefings from the Board to specific Business Units.

05-05 Meetings Security: (B) Retention: 50 years

Involvement of CDIC staff in the regular and ad hoc sittings of the Board to resolve matters brought before them or of their own initiation. Includes: Listing in the agenda any correspondence forwarded to the Board in the period between meetings.

*Deliberation
Approval*

06 Support - Executive Security: (U), Retention: 6 years

Logistical services provided to Executives to facilitate their effectiveness. Includes: The coordination and forecasting of facility availability, scheduling and the provision of other elements necessary for the effective communication of CDIC Executives with employees and stakeholders. Excludes: Logistics related to activities of the Board and Board Committees.

07 Committee Management

The activities of virtual business CDIC units composed of Board Members, CDIC employees, contracted or volunteer experts, and other stakeholders. Excludes: Participation of CDIC employees in external committees, such as the RPWG, even should a CDIC employee be the Chair of the Committee (see "National Affairs" and "International Affairs").

07-01 Governance

Security: (U)

Retention: 6 years

The empowerment of the Committee by statute, the Board or by Senior Management, and its occasional clarification.

07-02 Recruiting

Security: (U)

Retention: 6 years

Inquiry into the availability, suitability and willingness of individuals to assume roles in committees, and recommending the names of persons or of slates of persons to authorities. Includes: Confirmation of Board Member participation in some committees, as mandated by the terms of their appointment.

07-03 Appointment

Security: (U)

Retention: 6 years

The selection and assignment of roles and responsibilities to Members of Committees. Includes: Declaration of any conflict of interest and tracking of Committee Member terms to ensure that they are not inadvertently exceeded.

*Confirmation
Declaration
Orientation*

07-04 Logistics

Security: (U)

Retention: 6 years

The preparation and circulation of briefing binders, the coordination and forecasting of facilities, travel, schedules and other elements necessary for the effective communication of CDIC Executives and Board Members with committees and for the conduct of regular and ad hoc committee meetings. Includes: Photos of events primarily focused on or for CDIC employees which would be owned by the committee responsible for social events. Excludes: CDIC participating at events primarily for attendees who are not CDIC employees and for outreach (see "Communications/Outreach" and "Communications/Events").

07-05 Meetings

**Security: (U) or
(B)**

Retention: 6 years

The regular and ad hoc sitting of Committees to resolve matters brought before them or of their own initiation. Includes: Listing in the Agenda any correspondence forwarded to a Committee in the period between meetings.

08 Acquisition Management

Maintaining a rapport with the vendor community, identifying requirements for externally furnished services and assets, and the procurement, use, maintenance and disposal of services and assets that become possessions of or enter the control of CDIC. Includes: Directed as well as competitive procurements, including those that result in the provision of professional and other services, such as the use of offices and subscriptions, necessary for the conduct CDIC Functions.

08-01 Liaison Security: (U) Retention: 6 years

Informal interaction with vendors, procurement authorities and other stakeholders to facilitate potential instances of Procurement. Excludes: RFI, RFQ, etc. that might lead to a RFP.

08-02 Requirements Analysis Security: (U) Retention: 6 years

Regular and long-term analysis of acquisition needs, study of acquisition options, and planning of particular approaches and methods. Excludes: Individual instances of procurement.

08-03 Procurement Security: (U) Retention: 6 years

Cases of procurement, whether sole-sourced or competitive, using a variety of vehicles, resulting in the furnishing of a product or service and the incurring of a financial liability. Includes: Establishment of Standing Offers, as well as call-ups against SO's and other forms of agreement. Excludes: Payment of invoices (see "Financial Management/Transactions").

- Initiation*
- Review*
- Solicitation*
- Evaluation*
- Award*
- Administration*

09 Communications

Maintenance of an informed and effective relationship between CDIC and different elements of the internal and external stakeholder community.

09-01 Internal Security: (U) or (A) Retention: 2 years

Bilateral communication between CDIC Senior Management and employees, consisting of published materials, oral presentations, and meetings keeping staff updated with regard to corporate goals, priorities, initiatives or other matters that affect their work. Includes: Employees' Newsletters, Executive emails to employees, internal web content and any Intranet-based messages intended to inform staff of events and developments.

- Initiation*
- Consultation*
- Drafting*
- Dissemination*

09-02 Media Relations Security: (U) Retention: 10 years

Monitoring and clipping or news items pertinent to CDIC, and the maintenance of mutually beneficial relations with representatives of the media.

09-03 External Security: see below Retention: see below

Providing the public, stakeholders and other non-Member organizations with timely and accurate information about CDIC products, programs, services, initiatives and any specific issues that arise from time to time. Includes: Communications Strategies public release of Reports, production and release of publications, advertising (regardless of medium e.g. print, web content etc.), and responses to incoming calls to the CDIC 1-800 information line. Excludes: Release of information to the public and to Stakeholders that is specific to a case of Resolution e.g. the Dark Site Web Content (see “Intervention Management/Resolution”). Specific communications to members (see “Member Management/Communications”).

<i>Initiation</i>	Security: (U) or (B)	Retention: 10 years
<i>Drafting</i>	Security: (U) or (B)	Retention: 10 years
<i>Dissemination</i>	Security: (U)	Retention: 10 years or permanent

09-04 Parliamentary Security: (U), (B) or (S) Retention: 6 years or permanent

Specific communication with Parliamentarians to either proactively provide information or responsively answer questions about the role of CDIC or about specific cases with which they are concerned. Excludes: Release of information to the public and to Stakeholders that is specific to a case of Resolution e.g. the Dark Site Web Content (see “Intervention Management/Resolution”). Parliamentary Questions (PQ) (see “Governance/ATIP Response”).

09-05 Outreach Security: (U) Retention: 6 years

Proactive efforts to raise awareness of the role, capabilities, accomplishments and internal work environment of CDIC to maintain its stature, increase the use of its operational services, and to encourage employment applications and employee retention. Includes: Events and activities organized or co-organized by CDIC. Excludes: CDIC participating at events primarily focused on or for CDIC employees (see “Committee Management/Logistics”).

09-06 Events Security: (U) Retention: see below

Planning and preparation of CDIC participation in external events, such as trade shows, conferences, and the Annual Public Meeting, where a Board Member or Senior Executive is often the Spokesperson, for the purpose of communicating with the public or a stakeholder group. Includes: Events initiated by other organizations, but where CDIC employees participate for the purpose of engaging with the public. Excludes: CDIC participating at events primarily focused on or for CDIC employees (see “Committee Management/Logistics”).

<i>Planning</i>	Retention: 6 years
-----------------	---------------------------

Unclassified

Implementation

Retention: 6 years or permanent

Review

Retention: 6 years

09-07 Services-Internal

Security: (U)

Retention: 2 years

Provision of a wide variety of supporting services to Business Units in response to requests. Includes: Assistance with the promotion of job opportunities for the Human Resources business unit.

09-08 Translation

Security: Same as IR being translated

Retention: 2 years

Fulfilment of requests for the translation of all CDIC documents, whether intended for internal or external dissemination, regardless of the Business Unit making the request.

10 Financial Resources Management

In accordance with International Financial Reporting Standards (IFRS), controlling incoming and outgoing funds, investing against corporate and ex-ante (operational) requirements, providing for sufficient funds to meet all obligations. Includes: All financial management materials pertaining to other CDIC functions.

10-01 Forecasting

Security: (A) or (B)

Retention: 6 years

The reconciliation of accounts, and verification of actual and anticipated expenditures by business units against the approved budget for a Fiscal Year.

10-02 Transactions Management Reporting

Security: see below

Retention: see below

The collection of revenue from a variety of external sources, such as interest, recoveries and rent, and their deposit, along with premiums collected from Members, into CDIC's own treasury accounts, as well as the control of the expenditure of CDIC funds, and the recording of all such transactions in the ledger. Includes: Payroll and reimbursements of Board Member and employee expenses, payment of all forms of taxes, and the payment of invoices from suppliers and contractors. Excludes: The analysis of premiums received from Members (see "Insurance/Collection").

Revenue

Security: (A) or (B)

Retention: 6 years

Payroll

Security: (A) or (B)

Retention: 3 or 6 years

Taxation

Security: (A) or (B)

Retention: 3 or 6 years

Contractual

Security: (A) or (B)

Retention: 6 years

Resolution Payouts

Security: (B - Personal)

Retention: 6 years

Reimbursement - Premiums

Security: (A) or (B)

Retention: 6 years

Monitoring-Budget

Security: (A) or (B) Retention: 6 years

10-03 Treasury-Management

Security: (U)

Retention: 6 years

The responsible investment of all CDIC funds, ensuring capital preservation and liquidity with which to address operating needs, involving occasional study of economic trends, revenue and expenditure expectations. Includes: Operating and ex-ante funds.

*Assessment
Placement
Monitoring
Maturation*

10-04 Analytical Services

Security: (A) or (B)

Retention: 6 years

Proactive study of financial transactions to identify trends, opportunities and anomalies, as well as response to requests for financial analysis support for Business Units e.g. Corporate Planning requiring analysis of ex-ante amounts to provide a basis for new premium recommendations.

11 Human Resources Management

Includes activities associated with: recruitment and selection processes, training and development, performance assessment, occupational safety and health, employee relations, compensation and benefits, human resources planning and utilization, classification, official languages, employment equity, personnel security and special programs. Note: Many information resources arising from this function are 'protected'.

11-01 Workforce Management

Proactive and responsive work ensuring the maintenance of an effective workforce, able to fulfill all of the functions of CDIC.

Forecasting

Security: (A)

Retention: 6 years

Risk Management

Security: (A)

Retention: 6 years

Succession Management

Security: (A)

Retention: 6 years

Coaching

Security: (A)

Retention: 6 years

Employee Relations

Security: (U) or (B - Personal)

Retention: 2 years

Conflict Resolution

Security: (B)

Retention: 2 years

Investigations

Security: (B)

Retention: 2 years

11-02 Position Management

Security: (U)

Retention: 2 years

Job analysis - collecting information about the duties, responsibilities, necessary skills of a particular job. Job evaluation: Assessing job worth using the job evaluation system approved by the Canadian Human Rights Commission as gender neutral.

Definition
Evaluation
Approval

11-03 Staffing

Security: see below

Retention: 5 years

Locating and hiring employees able to fulfill the requirements of specific positions. Includes: All modes of staffing e.g. secondments, transfers, summer students etc., and the performance of credit, criminal and reference checks relating to potential and current employees, as well as any onboarding briefings for new employees.

Initiation

Security: (U) or (B - Personal)

Advertising

Security: (U) or (B - Personal)

Screening

Security: (U) or (B - Personal)

Selection

Security: (B - Personal)

Offer

Security: (B - Personal)

Onboarding-Corporate

Security: (B - Personal)

11-04 Supervision

Security: (B - Personal)

Retention: see below

The deployment and management of individual employees. Excludes: Support to Management Unit leaders and advice to employees regarding HR matters (see “Human Resource Management/Workforce Management/Coaching” and “Human Resource Management/Workforce Management/Employee Relations”, respectively).

Onboarding-Business Unit

Retention: 20 years

Performance Evaluation Documentation

**Retention: 5 years
Retention: 2, 3, 6 or 10 years**

Compensation Review

Retention: 2, 3, 6 or 10 years

Offboarding

Retention: 2, 3, 6 or 10 years

11-05 Training and Development Security: (U) Retention: 2 years

In-house or outsourced design of curricula in response to documented requirements, as well as sourcing of pre-existing programs that meet CDIC's needs, so that courses may be offered to employees in response to requests, leading to improvements or maintenance of their operational effectiveness. Includes: Review of requirements; Pre-training assessments; Coordination of courses; Delivery of Courses; Post-training surveys/evaluations by employees.

*Sourcing
Curriculum
Logistics
Attendance
Evaluation*

12 Information Management

Ensuring the life cycle management of CDIC information resources, regardless of medium, to support the performance of all other functions, as well as compliance with legal and accountability obligations. Includes: Business analysis, the instruction of employees in sound Information Management practices, the classification of information resources, the safe storage of information resources, response to requests for the retrieval of information resources, and the methodical disposition of information resources. Excludes: The life cycle management of the hardware and software assets that house information resources.

12-01 Business Analysis Security: (U) Retention: 2 years

The methodical and detailed study of the functions and requirements of CDIC to establish information resources life cycle management rules and structures.

12-02 Outreach Security: (U) Retention: 2 years

Proactive efforts to raise employee awareness of information management obligations and to improve skills and practices. Includes: Training and one-on-one coaching.

12-03 Classification Security: (U) Retention: 2 years

The application of a standardized code or descriptor, from the FCS, to an information resource, while storing it in an approved repository. Includes: In some cases, the scanning or conversion of information resources from less manageable paper format to digital media.

12-04 Storage Security: (U) Retention: Permanent

The maintenance of an inventory of CDIC Information Resources (IRs) in physical and digital repositories during their life cycle, ensuring preservation and privacy, while also ensuring retrievability.

12-05 Requests Security: (U) Retention: 2 years

Responses to research requests, resulting in the gathering or other handling of information resources from any repository or group of repositories.

12-06 Disposition Security: (U) Retention: see below

The annual removal of information resources from the responsibility of the CDIC through destruction, transfer, alienation, and other means. Includes: IM audits of information holding, both paper and electronic. Excludes: system backup tapes because they are for business continuity during a DR, not information repositories.

<i>Preparation</i>	Retention: 5 years
<i>Approval-OPI</i>	Retention:
<i>Approval-Final</i>	Permanent
<i>Implementation</i>	Retention:
	Permanent

12-07 Advice-IM Security: (U) Retention: 2 years

Providing IM advice, support, and guidance to apply best IM practices to the management of information, throughout its life cycle for structured and non-structured information. Includes: Incident management for IM tickets opened via the Records Request, the FCS, retention, disposition, security designation applied to the information's life cycle, metadata, content types, taxonomy, etc. Excludes: Outreach, Security Management, research requests, systems requirements, and technical support via the Service Desk.

13 Information Technology Services

Enabling the functions of CDIC through project-based implementation of Information Technologies, and the regular deployment of up-to-date IT solutions.

13-01 Pre-Project Management Security: (U) or (B) Retention: 2 years

Work leading to the identification and validation of existing and emerging Information Technologies as possible solutions for CDIC requirements. Excludes: Work that is intended to lead to the near-term procurement or implementation of an Application or Infrastructure (see "Project Management").

Requirements Analysis
Implementation
Review

13-02 Project Management Security: (U) or (B) Retention: 6 years

Work leading to the facilitation of Business Unit and CDIC Functions with Applications and Infrastructure as possible solutions for CDIC requirements. Includes: The management of projects involving intervention tools. Excludes: Procurement of Applications and Infrastructure (see "Acquisition Management").

Initiation
Requirements Analysis
Design
Implementation
Deployment
Testing

13-03 Operations Security: (U) or (B) Retention: 2 years

Continuous intervention to ensure the reliable functioning of deployed Applications and Infrastructure. Includes: Enabling of Internet access in offices. Excludes: Installation of new landlines (see "Facilities Management/Operations").

Baselining
Support
Quality Management
Analytical Services
Maintenance-Planned
Monitoring
Maintenance-Corrective
Enforcement
Retirement

13-04 Inventory Management Security: (U) Retention: see below

The life cycle management of all IT equipment and software owned and/or used by CDIC, to minimize costs, maximize availability, and minimize risk of theft and misuse. Includes: Management of iPads, cell phones, desktops, keyboards, laptops etc. Excludes: Procurement (see "Acquisition Management").

Receiving
Storing
Tracking
Release
Disposal

Retention: 2 years
Retention: 2 years
Retention: 2 years
Retention: 2 years
Retention: 2 or 6 years

14 Facilities Management

The life cycle management of all Facilities, acquired as a result of Projects or other means, involving the management of the Facility's configuration, the conduct of operations and maintenance.

14-01 Project Management Security: (U) or (B) Retention: 6 years

Work leading to the construction or modification of a Facility, often driven by plans to staff new positions. Excludes: Procurement of goods and services (see "Acquisition Management").

*Requirements Analysis
Specification
Supervision*

14-02 Configuration Management Security: (U) Retention: 6 years

The documentation and control of the actual, or as-built, configuration of facilities capturing their physical and functional characteristics, as well as the relationship between facilities and their sub-components and surroundings. Includes: Sub-components such as major mechanical equipment e.g. generators etc.

14-03 Operations Security: (U) or (A) Retention: see below

Regular work ensuring the usability of a facility as an environment in which to conduct the functions of CDIC. Includes: Interaction with users of a facility and supervision of any contractors charged with the operation of a facility.

Inspections **Retention: 2, 5, 10 or 30 years**
Maintenance **Retention: 2, 5, 10 or 30 years**
Supply **Retention: 2 years**
Stakeholder Management **Retention: 2 years**

15 Security Management

Assurance of a secure working environment in which CDIC functions may be performed, protecting personnel, facilities, information, and technology from disruption, harm, disturbance or injury. Includes: Applying safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information. Excludes: Investigations (see "Governance/Litigation").

15-01 Protection-Personnel Security: see below Retention: see below

The identification and monitoring of employee positions and circumstances that require particular treatment to mitigate security risks, the analysis and mitigation of these risks with suitable solutions.

Function and Activity Based Information (FAABI) File Classification System (FCS) User Guide

Unclassified

Includes: Performing Security Clearances relating to potential new employees and the handling of any incidents where personnel security is breached. Excludes: Conduct of credit, reference and criminal checks for new employees (see “Human Resource Management/Staffing”).

Screening

Security: (A) or (B- Personal)

Retention: 2 years

Incident Management

Security: (U) or (A)

Retention: 2 or 10 years

15-02 Protection-Facilities

Security: (A)

Retention: see below

The identification and monitoring of zones within CDIC facilities that require particular treatment to mitigate security risks, the analysis and mitigation of these risks with suitable solutions, and the handling of any incidents where the security of facilities is breached. Includes: The deployment of staff to mitigate security risks.

Risk Assessment

Retention: 2 years

Monitoring

Retention: 1 years

Incident Management

Retention: 2 years

15-03 Protection-Information

Security: (A) or (B)

Retention: 2 years

The identification and monitoring of information resources and repositories that require particular treatment to mitigate security risks, the analysis and mitigation of these risks with suitable solutions, and the handling of any incidents where information security is breached.

Risk Assessment

Monitoring

Incident Management

15-04 Protection-Technology

Security: (A) or (B)

Retention: 2 years

Identification, monitoring, analysis and mitigation of technological vulnerabilities within the CDIC technological infrastructure and application environment. Includes: Handling of any incidents where the security of technology is breached.

Risk Assessment

Monitoring

Incident Management

15-05 Emergency Management Security: (A) Retention: 5 years

Response to any serious interruptions in normal business activities, actual or threatened, often involving an external threat to CDIC infrastructure and/or the safety of employees.

16 Asset Management

The life cycle management of all tangible assets owned and/or used by CDIC, maintained to minimize costs, maximize availability, and minimize risk of theft and misuse, involving the receiving and registration of new assets, ad hoc stocktaking, and the release of assets to business units and employees. Includes: Assets such as desks, chairs, printers/copiers, landline desk phones etc., and their eventual disposal. Excludes: Procurement (see "Acquisition Management") and the management of IT equipment and software (see "Information Technology Services").

16-01 Receiving Security: (U) Retention: 2 years or permanent

The physical reception, verification, assignment of a tracking or serial number, and internal delivery of assets acquired through "Acquisition Management" or other means. Includes: gifts, honorariums, and awards that CDIC receives. Excludes: Damaged items and / or those specifically addressed to an employee.

16-02 Storage Security: (U) Retention: 2 years

The physical housing of all CDIC assets in anticipation of their release as required. Includes: Maintenance of an inventory of assets.

16-03 Tracking Security: (U) Retention: 2 years

Ad hoc and regular reconciliation of the inventory with the actual asset holdings of CDIC, whether performed by employees, auditors or contractors, to permit more timely replenishment, as a basis for insurance negotiation, to prevent theft etc. Includes: Referral of suspicious matters to the function of "Security Management/Incident Management".

16-04 Release Security: (U) Retention: 2 years

Issuing from inventory and physical delivery of assets to business units. Includes: Notice of a need to replenish, which may initiate procurement (see "Acquisition Management").

16-05 Disposal Security: (U) Retention: 2 or 6 years

Sale, destruction or removal of assets that are of no further use in the performance of CDIC Functions. Includes: gifts and honorariums that CDIC receives and may auction for charity.

B. Operational Functions (9)

17 National Affairs

Involvement in Canadian organizations, governmental and otherwise, with whom CDIC shares an interest in maintaining a stable financial environment, to advance and align policies.

17-01 Liaison Security: (U) or (A) Retention: 6 years

Informal interaction and correspondence with members of national organizations and other stakeholders to facilitate more specific work.

17-02 Technical Assistance Security: (U) or (A) Retention: 6 years

Services provided to organizations and other stakeholders in accordance with or consistent with an MOU or other agreement. Includes: Review and comment on plans, onsite visits and consultative support, tours and demonstrations of CDIC systems and methods etc.

17-03 Meetings Security: (U) or (A) Retention: 6 years

Involvement of CDIC staff in the regular and ad hoc sittings of Organizations with whom CDIC has an MOU or other agreement, providing CDIC with opportunity to influence national standards and policies.

17-04 Policy Consultation Security: (U) or (A) Retention: 6 years

Support for and interaction with national organizations to facilitate the creation of sound policy that incorporates or is compatible with CDIC positions and interests.

*Initiation
Drafting
Approval
Dissemination
Deployment*

18 International Affairs

Involvement in non-Canadian organizations, governmental and otherwise, with whom CDIC shares an interest in maintaining a stable financial environment, to advance and align policies.

18-01 Liaison Security: (U) Retention: 6 years

Informal interaction and correspondence with members of international organizations and other stakeholders to facilitate more specific work.

18-02 Technical Assistance-Outbound Security: (U) Retention: 6 years

Services provided to organizations and other stakeholders. Includes: Review and comment on plans, onsite visits and consultative support, tours and demonstrations of CDIC systems and methods etc.

18-03 Technical Assistance-Inbound Security: (U) Retention: 6 years

Services received from organizations and other stakeholders. Includes: Review and comment on plans, onsite visits and consultative support, tours and demonstrations of an organization's systems and methods etc.

18-04 Meetings Security: (U) Retention: 6 years

Involvement of CDIC staff in the regular and ad hoc sittings of Organizations, providing CDIC with opportunity to influence international standards and policies.

18-05 Policy Consultation Security: (U) Retention: 6 years

Support for and interaction with international organizations to facilitate the creation of sound policy that incorporates or is compatible with CDIC positions and interests.

*Initiation
Drafting
Approval
Dissemination
Deployment*

19 Member Management

The development and maintenance of mutually informative long-term relationships with Member institutions, enabling the fulfilment of other CDIC operational Functions.

19-01 Identification Security: (U) or (B) Retention: 6 years

The confirmation of fundamental factual information about the new or renewing Member. Includes: Discussions with organizations, such as provincial loan and trust companies, leading to their application for Membership or the determination that they need not be a Member or that they may voluntarily opt out of Membership. Also includes the cancellation of a Member's policy of deposit insurance.

19-02 Briefing Security: (B) Retention: 6 years

Initial and ongoing exchanges with Members to set compliance expectations, including detailed rules regarding the representation of CDIC Membership and depositor insurance coverage to depositors.

Initiation

Onboarding

19-03 Communications Security: (B) Retention: 6 years

Regular and ad hoc Member notification of events.

19-04 Continuing Education Security: (U) Retention: 6 years

Regular and ad hoc training of Member representatives, for which credit is awarded, to ensure that Members have the knowledge necessary to correctly promote and explain depositor insurance to the public. Includes: Instances where incorrect representation of CDIC depositor insurance is observed and where Members are actively corrected.

Design

Delivery

Evaluation

19-05 Courtesy Calls Security: (B) Retention: 6 years

Occasional meetings with Members, at their locations, for the purpose of further clarifying compliance expectations, answering any procedural questions, and maintaining a mutually helpful and respectful relationship.

19-06 Debriefing Security: (U) or (B) Retention: 6 years

Debriefing of Members on the occasion of their ceasing to be a Member, for any reason.

Initiation

Onboarding

20 Compliance Management

The methodical administration of certain sections of the CDIC Act, its By-laws and FIC obligations, with which Member institutions must comply, resulting in the receipt and analysis of both non-financial and financial information submissions from Members. Excludes: The regular gathering of financial datasets from Members (see "Data and System Requirements Verification/Gathering").

20-01 Assessment Security: (B) Retention: 6 years

Determination and clarification, with reference to the CDIC Act and By-laws, of what administrative data and access are required of Members and verification of the accuracy and completeness of submissions received.

20-02 Corroboration Security: (B) Retention: 6 years

Discussion with the Member and other parties and stakeholders to ensure the accuracy and interpretation of submissions received.

20-03 Enforcement Security: (B) Retention: 6 years

Actions taken when Members are delinquent in providing data required. Includes: Levying interest, premium surcharges and other penalties, and, ultimately, stripping an institution of Membership.

20-04 Data and System Requirements Verification Security: (B) Retention: 6 years

The generally irregular, but sometimes annual, verification that, in the event of failure, Members can/will provide depositor data, access and other submissions sufficient to permit resolution.

*Notification
Gathering
Processing
Debriefing*

21 Member Data Management

The regular effort to gather and analyze data and related information from members for the purpose of risk assessment, insurance determination, compliance, policy development and intervention and preparedness planning.

21-01 Requirements Definition Security: (B) Retention: 10 years

The identification of data and information needs from members.

21-02 Coordination Security: (B) Retention: 10 years

The regular and periodic uploading and testing of the data received from members via RRS and follow-up with them to correct problems and errors in the data revealed by testing. Includes: Re-filings by Members in conjunction with OSFI Data Management.

21-03 Data Analysis Security: (B) Retention: 10 years

The development of tools and systems to analyze the data in order to identify trends, patterns, anomalies to support CDIC employees and Business Units and their functions.

21-04 Training Security: (U) Retention: 2 years

One-on-one coaching of CDIC employees who are working with the tools and systems to analyze the data.

21-05 Support

Security: (U)

Retention: 2 years

First line assistance to CDIC employees who are working with data, tools and systems. IM team will provide non-technical IM support, including records management (see “Information Management/Support”), while IT will provide technical support (see “Information Technology Services/Operations/Support”).

22 Risk Assessment

The monitoring and communicating on the condition of CDIC Member Institutions in order to identify early warning signs of risks to depositors, and by extension, to CDIC. In order to meet CDIC’s objectives and management’s responsibilities under its relevant board policies, CDIC must be able to assess the risk associated with member institutions and have the capacity to effectively and expeditiously carry out required interventions that are consistent with its statutory objectives.

22-01 Members

Security: (B)

Retention: 20 years

The regular review of information to comprehensively understand members' risk profiles in order to determine the appropriate level of monitoring and risk assessment preparedness activities undertaken by of CDIC. These functions are performed on at least a quarterly basis with annual reporting, and are sometimes more frequent depending on a member's financial or regulatory conditions.

Monitoring
Corroboration
Consultation
Analysis
Drafting

22-02 Peer Group

Security: (B)

Retention: 20 years

At least once a year, the Risk Assessment Department discusses the relative scoring of peer group members, makes changes to risk assessment ratings based on new information for increases/decreases in the intervention ratings of members.

Initiation
Analysis
Drafting

22-03 Membership Review

Security: (B)

Retention: 20 years

CDIC produces a Membership Review which is a comprehensive analysis of financial, market, regulatory, economic, and emerging issues for Canadian banking. To manage insurance risk and support CDIC’s “Readiness” corporate strategy, this internal report is presented to the CDIC Board of Directors.

Initiation
Analysis
Drafting

23 Emerging Risk Management

Forward-looking assessments of risk-related issues and related research, primarily for proactive submission to or in response to requests from the Board or Senior Management. Excludes: Any work more specifically associated with individual Members, Peer Groups and the annual Membership Review.

23-01 Initiation Security: (A) or (B) Retention: 20 years

Proactive recognition of a need to advise Senior Management or the Board regarding a risk issue or theme relevant to CDIC's role and its Membership, or receipt of an ad hoc request for advice from Senior Management or the Board.

23-02 Analysis Security: (A) or (B) Retention: 20 years

The methodical study of quantitative data resulting from monitoring, corroboration and consultation, leading to drafting.

23-03 Drafting Security: (A) or (B) Retention: 20 years

Iterative development of a suitable Risk Assessment Report or other form of report e.g. Memorandum, presentation, briefing etc., and its submission to Senior Management or the Board.

24 Insurance

Under the Differential Premiums By-law, the classification of a Member, the determination and documentation of the terms of depositor insurance, and the administration of the resulting premium payments and any related delinquencies.

24-01 Calculation Security: (B) Retention: 6 years

The differentiation of a Member from its peers, and thus its classification, permitting the algorithmic determination of the insurance premium payable, each year, by a Member. (This work is performed by the Members themselves.)

24-02 Notification Security: (B) Retention: 6 years

Advising Members of the particulars of filings required pursuant to calculation, such as the category and rate of premium payable, and invoicing.

24-03 Collection Security: (B) Retention: 6 years

Working with Finance, the analysis of filings and premium payments made by Members. Excludes: The actual receipt of funds (see “Finance Resources Management/Transaction Management Reporting”).)

24-04 Enforcement Security: (B) Retention: 6 years

Measures taken to collect any delinquent filings or premium payments, including reminders and compliance measures such as the levying of interest and surcharges. Includes: Handling of complaints regarding the calculation of the premium payable by a Member.

25 Intervention Management

Annual work to prepare for possible instances of Domestic Systemically Important Bank (DSIB) and non-DSIB Member Intervention and, when required, actual cases of Member Resolution.

25-01 Preparation Security: (B) Retention: 6 years

Analysis and development of methodologies, tools, and other resources necessary for the effective conduct of possible cases of Resolution.

- Initiation*
- Consultation*
- Analysis*
- Design*
- Testing*

25-02 Project Management by Project Name Security: (U) or (B) Retention: 6 years

Work leading to substantial new capability to engage in Intervention Management. Excludes: The management of technology projects that support Intervention Management (see “Information Technology Services/Project Management”).

- Initiation*
- Requirements Analysis*
- Design*
- Implementation*
- Testing*
- Deployment*

25-03 Planning by Member Security: (B) Retention: 6 years

The ongoing development and maintenance of comprehensive and implementable Resolution Plans for Members that demonstrates how they could be credibly resolved in a manner that ensures continuity of critical financial services while not exposing taxpayers to loss.

Initiation
Consultation
Analysis
Corroboration
Drafting
Assessment Review
Feedback
Testing

25-04 Simulation Security: (A) Retention: 5 years

For a given hypothetical scenario, all of the planned steps for a resolution, permitting confirmation of the efficacy of the Resolution Plan.

Planning
Execution
Evaluation

25-05 Examination-Preparatory Security: (B) Retention: 6 years

When identified and required, a more detailed analysis of the deficiencies in the Member's Resolution Plan and further interaction with the Member to seek remedies, to refine the Resolution Plan or to prepare for a possible intervention or resolution.

25-06 Cooperation Security: see below Retention: 6 years

CDIC's coordination (including cooperation and member-specific information sharing) with other domestic and international regulatory authorities and key Stakeholder groups, in preparation for possible cases of Resolution. Excludes: Regular establishment and maintenance of relationships with external Organizations (see "National Affairs" and "International Affairs").

Outreach Security: (B) or (B-Personal)
Analysis Security: (B)

25-07 Resolution Security: see below Retention: 10 years or permanent

Work to facilitate the orderly liquidation or re-structuring of a Member that is approaching non-viability or that has failed. Includes: Release of information to the public, Parliamentarians, and to Stakeholders that is specific to a case of Resolution e.g. the Dark Site Web Content. Excludes: Payouts (see "Financial Resources Management/Transactions Management Reporting/Resolution Payouts").

Notification

Security: (B)

Examination

Security: (B)

Intervention

Security: (U) or (B)

Support-Post-Intervention

Security: (U) or (B)