

RE: IMCAP assessment work at Health - templates etc.

From: Grover, Brent CITZ:EX <Brent.Grover@gov.bc.ca>
To: Jager, Brenda HLTH:EX <Brenda.Jager@gov.bc.ca>, Jackson, Brittany CITZ:EX <Brittany.Jackson@gov.bc.ca>
Cc: Hall, Simon HLTH:EX <Simon.Hall@gov.bc.ca>, Wright, Richelle CITZ:EX <Richelle.Wright@gov.bc.ca>, Li, Stephen CITZ:EX <Stephen.Li@gov.bc.ca>
Sent: November 2, 2018 9:07:45 AM PDT

It will take us a little while to go over things as we are in the midst of another engagement but at first glance this looks like Great Work Brenda! Thank you for looping back with us.

Also, I would like to introduce our new Director Stephen Li, he will also be looking over this material.

Thanks

Brent Grover, MPA | Senior Auditor (Practice Reviews)

Investigations and Reviews | Privacy, Compliance and Training Branch | Ministry of Citizens' Services
Ph: 778-698-4992 | M: PO Box 9406, Stn Prov Gov, Victoria BC V8W 9V1

The dogmas of the quiet past are inadequate to the stormy present - Lincoln

Government confidentiality and privilege requirements apply to this message and any attachments. If you are not the intended recipient, you are hereby notified that any review, retransmission, conversion to hard copy, copying, circulation or other use is strictly prohibited. If you are not the intended recipient, please notify the sender immediately, and delete this message and any attachments from both your inbox and deleted items folder. Thank You.

From: Jager, Brenda HLTH:EX
Sent: Friday, November 2, 2018 8:57 AM
To: Grover, Brent CITZ:EX; Jackson, Brittany CITZ:EX
Cc: Hall, Simon HLTH:EX; Wright, Richelle CITZ:EX
Subject: IMCAP assessment work at Health - templates etc.

Hello Brent and Brittany,

To keep you in the loop with my IM maturity level assessments for the Ministry of Health, I thought I would send you my template report document and list of improvement tasks (Best Practises) that I developed to report out to the Branches in the HSIMT Division. To show how they work, I have provided a sample filled out report too.
I have completed the assessments and have circulated the reports. Just waiting for the branches to respond with any inaccuracies.

Please let me know your thoughts on these documents. I consider them continuous improvement projects.

Brenda Jager | Records Officer

Ministry of Health | Health Sector Information Management & Technology Division | Health IT Strategy Branch
Phone: 778 974-4969

Ministry of Health

Information Management

Best Practises for Continuous Improvement

DRAFT 2018-11-01

1. Governance and Accountability

- **Records management accountabilities**
 - **Ministry-specific records management policies / procedures**
- 1.1 Assign program level record custodians and delegate IM tasks.
 - 1.2 Produce program level IM task list with calendarized items for record custodians.
 - 1.3 Produce program level IM*Guide for staff. IM*Guide needs to include:
 - a. information on OPR for all records created or received,
 - b. official location for filing records (paper / LAN address / EDRMS CM),
 - c. list of who can create new folders in chosen locations, and
 - d. process step details and links to GRS guides for all IM tasks to assist current and future record custodians.
 - 1.4 Ensure each IM process step is assigned to staff and that those responsibilities are included in job description(s) and My Performance Plan(s). (Do all staff file records or is this task specialized?)
 - 1.5 Ensure Office of Primary Responsibility (OPR) is understood and assigned to all record types created or received by the Branch.
 - 1.6 For records with Superseded / Obsolete (SO) designations, ensure there are defined conditions or that a review of the records is calendarized and responsibility assigned.
 - 1.7 Specifically assign responsibility for Final Disposition steps for records. (DE/SR/FR).
 - 1.8 Assign orientation training responsibilities for new staff.
 - 1.9 Assign responsibility for checking IM work is completed to standards included in IM*Guide.
 - 1.10 Ensure staff know where to find the program IM*Guide. Have a standard location – webpage, LAN or paper copy.
 - 1.11 Assign responsibility to update IM*Guide.
 - 1.12 If EDRMS Content Manager is not available, use LAN with ARCS/ORCS coding for official digital filing.
 - 1.13 Clean up SharePoint site.
 - a. Move/Copy official records from SharePoint to ARCS/ORCS coded LAN folders.
 - b. Remove records from SharePoint that are no longer required for consulting or reference purposes.
 - c. Create schedule for moving/copying records from SharePoint to LAN. Complete filing regularly - do not wait for projects to be completed.

Branch or Division Level

- 1.14 Create and maintain inventory of record custodians for Division to ensure responsibilities have been assigned and to provide a contact list for communicating updates and changes to IM procedures.

2. Education and Awareness

- **Mandatory employee training**
- **Role specific training**

- 2.1 Develop reference list of IM training requirements and assign for each staff position with IM responsibilities. List to include Learning Centre and other courses.
- 2.2 Ensure current and new staff complete required IM training as assigned to their positions responsibilities.
- 2.3 Ensure new staff are aware of their training requirements during their initial orientation.
- 2.4 Assign responsibility for updating of training list.
- 2.5 Ensure during initial orientation, new staff are provided a program level IM*Guide.
- 2.6 Assign responsibility for checking new staff are oriented to IM standards and guidance materials. Add to My Performance Profiles or set up tracking if required.

Branch or Division Level

- 2.7 Centralized tracking of completion of IM117, by the Deputy Minister's office, is successfully working to ensure this course is completed by all staff.
- 2.8 Produce program level IM*Guide for staff which includes:
 - a. List of services provided by Records Officers and contact information.
 - b. Provide links/addresses to centralized GRS guides and tools.
 - c. Description of how to create short cuts in Internet Explorer to simplify filing to program level folders.
 - d. Best practises for email management; (link to GRS guide when developed)
 - i. Use of Outlook folders to separate transitory and official filing for each project/subject,
 - ii. Adding dates YYYY-MM-DD to beginning of subject line in Outlook, prior to filing emails,
 - iii. Use hyperlinks to reference documents in emails rather than attaching,
 - iv. How to create a hyperlink.

3. Classification

- **Record classification**

- 3.1 Program Area to develop standard folder and file naming conventions for IM
- 3.2 Program to use ARCS / ORCS coding, to classify their official records in all systems.
- 3.3 Ensure LAN file paths include folders labeled with ARCS/ORCS.
- 3.4 Move/refile records into ARCS/ORCS classified file paths where staff have chosen to create ad hoc folders rather than identify and use the most appropriate classifications.
- 3.5 Train all staff on ARCS/ORCS classifications and how to identify appropriate codes for use when they are not listed in program level IM*Guide.
- 3.6 File HR records in official location rather than in personal H: drives of admin staff. Give access to admin staff or provide alternative process for transferring records to official location.
- 3.7 Update LAN file path names to include ARCS/ORCS coding where records are currently sorted into ARCS/ORCS classifications.
- 3.8 Develop new ARCS/ORCS LAN framework to refile records currently stored on the LAN or SharePoint sites in ad hoc folder systems.
- 3.9 Produce program level IM*Guide for staff which includes:
 - a. List of commonly used ARCS and ORCS classifications for program area,
 - b. Method to identify ARCS/ORCS coding when not included in the IM*Guide.
 - c. List of standard naming conventions and folder naming options for all identified types of records produced in the branch.
 - d. Include version control labeling in naming convention standards.

Branch or Division Level

- 3.10 Division establish standard version control labeling for documents. Can be delegated to program level if best practise requires differences between program areas.

4. Digitization / Documentary Evidence

- GRS Digitizing Records Guide - Draft
 - 4.1 Scan paper records with on-going value and place into shared drives.
 - 4.2 Scan paper copies to be sent to off-site storage or destroyed based on Redundant Record Schedule best practises guide
 - 4.3 To prepare introduction of EDRMS Content Manager, develop new ARCS/ORCS LAN framework to clean up and file unclassified records.
 - 4.4 Refile records currently stored without ARCS/ORCS coding. Record sources include personal drives, LAN and SharePoint sites.

Branch or Division Level

- 4.5 Program level IM*Guide for staff which includes:
 - a Reference to GRS *Digitalization Best Practices Guide*.
GRS IM Digitizing Guide - Draft

5. Retention, Holds and Disposition

- **Information schedule development and maintenance**
- **Records retention, holds and disposition**
 - 5.1 Assess and clean up transitory paper records and classify official paper records, using ARCS/ORCS, not included in CRMS inventories or duplicated in LAN folders.
 - 5.2 Process on-site paper records through semi-active (off-site storage) and final dispositions (DE/SR/FR).
 - 5.3 Centralize paper HR records into “locked” cabinets or scan and file in ARCS LAN folders, then shred paper copies as per the Redundant Records Schedule best practices.
 - 5.4 Identify digital records, ensure ARCS classification and prepare inventories.
 - 5.5 Assign responsibility for tracking dispositions.
 - 5.6 Schedule review of dispositions of record inventories.
 - 5.7 Schedule disposition IM tasks for program area records.

Branch or Division Level

- 5.8 Identify and assign responsibility for on-site and off-site paper records through ownership of CRMS Org units. CRMS currently has unassigned record inventories.
- 5.9 Physically find and inventory on-site records listed in CRMS Org Units.
- 5.10 Develop official Hold procedure for litigation and FOI processes

6. Archiving / Preservation / Record Transfers

- **Identify and protect digital records scheduled for archiving**
 - **Record transfers to Information Management Act (IMA) bodies**
- 6.1 Ensure record custodian duties include assignment of processing of records through final disposition.
 - 6.2 Produce program level IM*Guide for staff which includes:
 - a. CRMS Org Units assigned ownership / responsibilities.
 - b. How to print record lists (inventories) from CRMS.
 - c. How to analyse LAN records for next steps in disposition processing.

Branch or Division Level

- 6.3 Work with IT staff to approve use of application that can print list of records in ARCS/ORCS dedicated shared drives (LANs). Lists need to include ARCS/ORCS schedules associated with records. (Beta version app has been developed to produce Excel document)
- 6.4 Produce Branch or Division Level IM*Guide for staff which includes:
 - a. Standard process, with associated required documentation to track record transfers, for ministry reorganizations, and through transfer of records to Ministry of Attorney General, the Royal Museum Archives or other government organizations such as Health Authorities.
- 6.5 Work with GRS to introduce EDRMS Content Manager.

7. Records Maintenance and Storage

- **Manage information in record keeping systems (schedules)**
 - **Manage physical records**
 - **Inventory of Ministry systems and repositories**
- 7.1 Analyse paper records on-site to determine if they are currently listed in an inventory (CRMS) and process accordingly.
 - a. Add to CRMS if required.
 - b. Request destruction via GRS process for DE eligible records.
 - c. Send to off-site storage if time for DE is not within this next year.
 - d. Process and send records to off-site storage if final disposition is SR/FR.
 - 7.2 Assess LAN records and request destruction via GRS process for DE eligible digital records.
 - 7.3 Assess LAN records to place some digital records into semi-active LAN locations. (Museum Archives has requested ministries hold their SR/FR digital records at this time.)
 - 7.4 Produce program level IM*Guide for staff which includes:
 - e. Program level process to complete GRS destruction requests and to maintain required tracking.
 - f. Process for record recalls and returns to off-site storage including tracking.
 - g. Process for maintaining and updating staff authorizations via GRS, to recall records from off-site.
 - h. 60-day notice procedures to ensure approval and tracking of decision to destroy or hold records.

Branch or Division Level

- 7.5 Assign responsibility to CRMS Org Units. This will provide linkages to AXIS Indented Org Charts and off-site accessions.
- 7.6 Develop security Hold procedure that will mark paper or digital records to ensure the records are safeguarded from destruction or transfer to another organization. "Hold" is to avoid final disposition processing. (used for litigation and FOI purposes)
- 7.7 Assign management of record security Holds to a job position and add to the job description to ensure management of the Holds over time. (staff turn over issue)
- 7.8 Assign responsibility for checking that Divisional/Branch records management tasks are completed and up to documented standards.
- 7.9 Produce Division/Branch Level IM*Guide for staff which includes:
 - a. Assign responsibility to monitor records under litigation "Holds".

8. Information protection – related to IM not systems

- **Security program**
 - Employee Training – covered in section 2
 - Role Based Training – covered in section 2
 - **Employee accountabilities**
 - **Security classification**
 - **User access and responsibilities**
- 8.1 Analyse if current structure of LAN security restrictions is adequate to minimize access to records. Ensure staff only have access to the records they need to complete their duties.
- 8.2 Set up secure storage for Human Resource related documents.
- 8.3 Ensure administrative staff have a process to file HR records in a secure location. Discourage use of Personal drives (H: drives) for storing HR records.
- 8.4 Explore the use of LAN folders that offer access to all members within matrix teams. Teams that have members from different branches may wish to have common shared drive folders for official filing. Alternative is explicit process for filing and assignment of IM responsibilities.
- 8.5 Use EDRMS Content Manager or LANs for official storage of digital records. SharePoint systems are not IM systems – risks to using only SP are:
- a. lack of final disposition schedule will result in records being kept too long or not moving to archives,
 - b. searches for FOI and litigation are not easily completed if ARCS or ORCS are not used,
 - c. inventories of records for SP sites is a manual process,
 - d. access to records is restricted by SP administrators, rather than executive and IM officials,
 - e. Crashed SP sites are difficult to recall and at times records are lost.

Information Management Practices IM*Guide

Organized by IMPAC Criteria

Governance and Accountability

1. Information on OPR for all records created or received,
2. Official location for filing records (paper / LAN address / EDRMS CM,
3. List of who can create new folders in chosen locations, and
4. process step details and links to GRS guides for all IM tasks to assist current and future record custodians.
5. Assign responsibility to update IM*Guide.

Education and Awareness

6. List of services provided by Records Officers and contact information.
7. Provide links/addresses to centralized GRS guides and tools.
8. Description of how to create short cuts in Internet Explorer to simplify filing to program level folders.
9. Best practises for email management; (link to GRS guide when developed)
 - a. Use of Outlook folders to separate transitory and official filing for each project/subject,
 - b. Adding dates YYYY-MM-DD to beginning of subject line in Outlook, prior to filing emails,
 - c. Use hyperlinks to reference documents in emails rather than attaching,
 - d. How to create a hyperlink.

Classification

10. List of commonly used ARCS and ORCS classifications for program area,
11. Method to identify ARCS/ORCS coding when not included in the IM*Guide.
12. List of standard naming conventions and folder naming options for all identified types of records produced in the branch.
13. Include version control labeling in naming convention standards.

Digitization / Documentary Evidence

14. Reference to GRS *Digitalization Best Practices Guide*.
[GRS IM Digitizing Guide - Draft](#)

Retention, Holds and Disposition

15. Develop official Hold procedure for litigation and FOI processes.

continued...

Archiving / Preservation / Record Transfers

16. CRMS Org Units assigned ownership / responsibilities.
17. How to print record lists (inventories) from CRMS.
18. How to analyse LAN records for next steps in disposition processing.
19. Standard process, with associated required documentation to track record transfers, for ministry reorganizations, and through transfer of records to Ministry of Attorney General, the Royal Museum Archives or other government organizations such as Health Authorities.

Records Maintenance and Storage

20. Program level process to complete GRS destruction requests and to maintain required tracking.
21. Process for record recalls and returns to off-site storage including tracking.
22. Process for maintaining and updating staff authorizations via GRS, to recall records from off-site.
23. 60-day notice procedures to ensure approval and tracking of decision to destroy or hold records.
24. Assign responsibility to monitor records under litigation "Holds".

Security

No current recommendation for IM*Guide

IMCAP Assessment Form – HSIMT – Records/Information Management

Division	Branch	Program Area
HSIMT	HITS	

	1. Governance and Accountability <ul style="list-style-type: none"> • Records Management Accountabilities • Ministry-Specific Records Management Policies / Procedures 		
	Procedure Questions	Answers / Notes	Name of P&P Doc – Received Copy?
	Who creates records?		
	Are ARCS and ORCS codes applied to all records?		
	Are there standard naming conventions for records?		
	Is there a digital IM system available for your program area? (TRIM/CRMS/other)		
	Are there standard folders in the shared drive (LAN) for filing records?		
	Who can create folders and add records to the official IM system?		
	Who can create folders in the shared drives?		
	Is there a staff guide to communicate regularly used coding and standard naming conventions?		
	Is there a staff guide to using the official IM system?		
	Is there a staff guide to folder management in the shared drive? (LAN)		

IMCAP Assessment Form – HSIMT – Records/Information Management

	Are there official locations for records? (Paper, digital, maps, artifacts, other)		
	Who files records?		
	Who checks naming standards are being applied?		
	Who checks if records are filed and done correctly?		
	Who manages the records through their lifecycle (ARCS/ORCS Schedules for retention). Current, off-site, final disposition?		
	Is there documentation of who is responsible for checking naming, coding and filing records (RACI)?		
	Are there positions with job descriptions with responsibilities for record keeping?		
	Job Description(s) of Record Admin Personnel		Job descriptions
	Those with responsibility for IM - who do they report to?		
	Is there an Org chart with reporting structure?		
	Is the documentation for record keeping official or ad hoc?		
	Where are the official P&P stored, updated, managed?		
	How are changes to IM P&P communicated to staff responsible?		
	How are new staff informed of IM P&P and their responsibilities?		
	Are there new staff IM orientation documents?		
	Other? Participants ad hoc input.		

IMCAP Assessment Form – HSIMT – Records/Information Management

	2. Education and Awareness <ul style="list-style-type: none"> • Mandatory Employee Training • Role Specific Training 		
	Procedure Questions	Answers / Notes	Name of P&P Doc – Received Copy?
	Have ministry staff completed the mandatory IM117: Protection of Privacy, Access to Information and Records Management training course?		
	Have ministry staff completed IM118: Information Security and Awareness: Supporting Employees in the Workplace?		
	Are staff oriented to Program / Branch level IM standards? Who does the orientation?		
	Are there orientation materials provided at the Branch/Program level?		
	Is there documentation, for your program area, showing staff have completed IM orientation within their work group?		
	How are staff identified as needing “role specific” IM Training?		
	How does the ministry identify additional staff training "requirements" for records management?		
	Is a list of additional IM training maintained?		
	Does the work group maintain and communicate internal IM training documents/materials for employees?		

IMCAP Assessment Form – HSIMT – Records/Information Management

	Where / how are additional IM training documents communicated, stored for reference?		
	Is there documentation for your program area showing all staff have completed IM117 and other related records training?		
	How are training gaps and missed training addressed?		
	Other input from participants.		
	3. Classification <ul style="list-style-type: none"> Record Classification 		
	Procedure Questions	Answers / Notes	Name of P&P Doc – Received Copy?
	Are P&Ps established to support classification of records by function or business area? (Over and above those standardized by OCIO/GRS.)		
	Are there any associated 'retention' schedules used for records management? (guidance on SO?)		
	What is the name of the P&P and where are they stored?		
	Has the ministry established its own independent classification model? In-house filing other than ARCS/ORCS based distinctions.		
	4. Digitization / Documentary Evidence <ul style="list-style-type: none"> Digital Records 	Inform interviewee that this control will not be required to be supported <u>at this time</u> . Inform them	

IMCAP Assessment Form – HSIMT – Records/Information Management

		that this is for preparational purposes and that future reviews will cover this control.	
	Procedure Questions	Answers / Notes	Name of P&P Doc – Received Copy?
	Has there been any work to manage records in a digital format?		
	Does your program area officially manage records in a digital format? (Organized LAN or other software)		
	Has your work group had discussions about future digital IM that will comply with the Information Management Act and applicable laws, policies, directives, standards, and specifications.		
	5. Retention, Holds and Disposition <ul style="list-style-type: none"> • Information Schedule Development and Maintenance • Records Retention, Holds and Disposition 		
	Procedure Questions	Answers / Notes	Name of P&P Doc – Received Copy?
	Does your work group have an active schedule for management of records through their lifecycle? Example: when are records with SO assessed for next step in their lifecycle?		
	Does the work group area P&P describe requirements for disposition of records and does it align with the ARCS/ORCS schedules?		Request a sample (or someone who can assist) of a disposition activity that ties to a schedule.

IMCAP Assessment Form – HSIMT – Records/Information Management

	Do you report (e.g., annually) on the current disposition of records?		
	Does your work group regularly schedule disposition IM tasks for your lines-of-business?		
	How are dispositions tracked? By Whom?		
	Is there documentation of IM tracking for record dispositions in your work group?		
	Are procedures in place to support "hold" requests/instructions?		
	Is the procedure documented?		
	Where are the procedures stored?		
	Who is responsible for the 'hold' procedure?		
	Is this procedure included in an all-encompassing procedure? Where?		
	Who is responsible for monitoring "holds" (litigation/FOI etc.)? Process: Documenting offsite records sufficiently to enable locating, retrieving, administering litigation holds, and other purposes.		
	6. Archiving / Preservation / Record Transfers <ul style="list-style-type: none"> Identify and Protect Digital Records Scheduled for Archiving Record Transfers to IMA Bodies 		

IMCAP Assessment Form – HSIMT – Records/Information Management

	Procedure Questions (IMA – Information Management Act)	Answers / Notes	Name of P&P Doc – Received Copy?
	What procedures (guidance) is used for records management and maintenance for records scheduled for archive? (SR/FR)		
	Where is the procedure stored (archived) and who maintains the procedure(s)?		
	Does the procedure align to GRS policy? (example: 300 dpi, meta data and labels for photos)		
	Are procedures established for the management of records transfers to other bodies (costs, documentation, tracking)?		
	Where are the procedures stored?		
	Who is responsible for the management of the procedure (e.g., Chief Records Officer)?		
	How are records formatted (paper/digital)?		
	Are there any agreements in place with other IMA bodies pertaining to record transfers?		
	How are transfers recorded and tracked with other IMAs?		
	If no information schedule applies, how are approvals made for the management of information? (archiving or disposal) <i>Note: Information may be transferred between 2 government bodies whether or not an information schedule applies to or addresses that transfer.</i>		
	Are there P&P to approve transfers of records and are requirements made for the management (transfer, archiving or disposal) of records?		

IMCAP Assessment Form – HSIMT – Records/Information Management

	Are there ministry procedures for records transfers to non-IMA bodies?		
	Do the procedures include information schedules/CRO approval, legislation or court order to allow legal transfers to non-IMA entities?		
	Where is this procedure stored and who owns the document?		
	7. Records Maintenance and Storage <ul style="list-style-type: none"> • Manage Information in record keeping systems (schedules) • Manage Physical Records • Inventory of ministry Systems and Repositories 		
	Procedure Questions	Answers / Notes	Name of P&P Doc – Received Copy?
	Does the ministry maintain a recordkeeping system to manage government information? (CRMS/TRIM/LAN / Other)		
	Is there a ministry-wide initiative to adopt a recordkeeping system?		
	Does the ministry maintain requirements that include 'schedules' (IMA) for recordkeeping needs?		
	Are there procedures supporting the onsite/offsite management and storage of physical records for the ministry? (More than provided by GRS)		

IMCAP Assessment Form – HSIMT – Records/Information Management

	(Ministry managed records disposal - onsite or shred disposal services)		
	What documentation and tracking methods are in place to monitor stored records? (More than provided by GRS)		
	If offsite storage is used, who is the storage vendor under contract? (More than provided by GRS)	If other than GRS	
	Who in your program area is responsible for monitoring offsite records?		
	Are there procedures for off-site storage? (more than provided by GRS)		
	Do the procedures above align with GRS policy?		
	Are there procedures for inventory of the systems and locations of records for your program area?		
	What inventories are established and known for the management of ministry information?		
	Who is responsible for the monitoring and maintenance of the repositories?		
	Is the inventory updated and how often?		
	Are there multiple inventories and who is responsible for them?		

IMCAP Assessment Form – HSIMT – Records/Information Management

	8. Information protection – related to IM not systems <ul style="list-style-type: none"> • Security Program • Employee Training – covered in section 1 • Role Based Training – covered in section 1 • Employee Accountabilities • Security Classification • User Access and Responsibilities 	Systems based security not included in this assessment <ul style="list-style-type: none"> • External Parties • Asset management • Physical and Environmental Protection • Protection Against Malicious Code • Portable Media • Access Control • Security requirements for information systems • Technical Vulnerability Management • Logging and Monitoring • Business Continuity Management • Monitoring Service Provider Compliance with information Protection requirements 	
	Procedure Questions	Answers / Notes	Name of P&P Doc – Received Copy?
	Is there a Security Program based on the Information Security Policy (ISP) from OCIO/CIRMO for your records	HIPSL - ' - Comply to ISPs.13; s.15 s.13; s.15	
	Employee Accountabilities for the protection and privacy of records/information.	HIPSL -s.13; s.15 s.13; s.15 ITSB – Standards of Conduct reviewed annually, Acceptable Usage policy, least Privilege granted per ISP BMO - 'Awareness via onboarding branch procedures. s.13; s.15	

IMCAP Assessment Form – HSIMT – Records/Information Management

		ITS - Registries - Employees are trained on their roles and accountability relating to information protection s.13; s.15	
	Are records are organized so that security classifications can be applied to protect different classes of information based on their sensitivity.	<p>HIPSL - Follow OCIO framework, ad-hoc use, moving to a Ministry-developed framework, part of the CPS strategic projects stream.</p> <p>ITSB - As per HIPSL and OCIO guidance</p> <p>BMO - 'As per HIPSL and OCIO guidance s.13; s.15</p> <p>ITS – Registries - As per HIPSL and OCIO guidance Core govt' classification methods applied (H-M-L). Example, LAN share folders have established and restricted access restriction to information</p>	

Information Management Maturity Assessment Fall 2018

Health Sector Information Management and Technology Division

BRANCH NAME

Contents

Branch Summary and Overview Recommendations	2
program	4
program	6
program	8
program	10
program	12

Methodology:

The Records Officer met individually with all Directors and other identified staff to determine the information management practises currently in use within the Division. A standard set of questions was developed from CIRMO's Information Management Capacity Assessment Practises (IMCAP) framework to use during these interviews. The Records Officer requested copies of any program level policy & procedure and guidance documents identified within the interviews. The Records Officer did not follow up with investigations to validate answers.

The records management component of the IMCAP outlined 7 criteria with a range of 5 maturity levels. This assessment also includes an 8th criterion to cover the security of records through staff access controls. The maturity levels are described in this embedded Excel spreadsheet.



2018 Baseline
Assessment Framew

Included in this report are a set of overall recommendations to the Executive Director for best practises that will improve the information management in their Branch. This is followed by detailed reports for each program area with specific ratings and recommendations for each group.

BRANCH NAME

Branch Summary and Overview Recommendations

The below report summarizes current information management practises within your branch. Standard IMCAP ratings indicate the maturity level of current IM processes. Where improvements are required, I have referenced best practice tasks that, if completed, will assist to improve the routines in the branch. There are two levels of recommendations within this report – first an overall branch review with branch level recommendations and then reviews of the individual program areas.

Ratings within your Branch range from SCORErANGE. s.13
s.13

Ratings of 1 or 2 indicate s.13
s.13

Rating of 3 indicates s.13

Ratings of 4 or 5 indicate s.13
s.13

Brenda Jager | Records Officer

Ministry of Health | Health IT Strategy Branch - Phone: 778 974-4969

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services.

IM = Information Management


OPR = Office of Primary Responsibility IMCAP=OIPC Assessment Framework

CRMS = Corporate Records Management System

Page 2 of 12

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

Criteria	IMCAP Maturity Rating 1-5	Notes and Branch Level Best Practise Recommendations	 IM Best Practices 2018-11-01.docx
1. Governance and Accountability	Range Overall	Recommended Branch Action: S. 13	
2. Education and Awareness	Range Overall	Recommended Branch Action: S. 13	
3. Classification	Range Overall	Recommended Branch Action: S. 13	
4. Digitization / Documentary Evidence (future based)	Range Overall	Recommended Branch Action: S. 13	
5. Retention Holds and Disposition	Range Overall	Recommended Branch Action: S. 13	
6. Archiving/Preservation/ Record Transfers	Range Overall	Recommended Branch Action: S. 13	
7. Records Maintenance and Storage	Range Overall	Recommended Branch Action: S. 13	
8. Security	Range Overall		

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services.

IM = Information Management

OPR = Office of Primary Responsibility IMCAP=OIPC Assessment Framework

CRMS = Corporate Records Management System

Page 3 of 12

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

PROGRAM: Contact:

Criteria	Actions To Do List	Maturity Rating	Notes
1. Governance and Accountability			•
2 Education and Awareness			•
3. Classification			•
4. Digitization / Documentary Evidence (future based)			•
5. Retention Holds and Disposition			•
6. Archiving/Preservation/ Record Transfers			•
7. Records Maintenance and Storage			•
8. Security – HR and classified records located with security access	Issue for Managers		•

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services. **IM** = Information Management

OPR = Office of Primary Responsibility **IMCAP**=OIPC Assessment Framework

CRMS = Corporate Records Management System

Page 4 of 12

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

PROGRAM: Contact:

Criteria	Actions To Do List	Maturity Rating	Notes
1. Governance and Accountability			•
2 Education and Awareness			•
3. Classification			•
4. Digitization / Documentary Evidence (future based)			•
5. Retention Holds and Disposition			•
6. Archiving/Preservation/ Record Transfers			•
7. Records Maintenance and Storage			•
8. Security – HR and classified records located with security access	Issue for Managers		•

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services. **IM** = Information Management

OPR = Office of Primary Responsibility **IMCAP**=OIPC Assessment Framework

CRMS = Corporate Records Management System

Page 5 of 12

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

PROGRAM: Contact:

Criteria	Actions To Do List	Maturity Rating	Notes
1. Governance and Accountability			•
2 Education and Awareness			•
3. Classification			•
4. Digitization / Documentary Evidence (future based)			•
5. Retention Holds and Disposition			•
6. Archiving/Preservation/ Record Transfers			•
7. Records Maintenance and Storage			•
8. Security – HR and classified records located with security access	Issue for Managers		•

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services. **IM** = Information Management

OPR = Office of Primary Responsibility **IMCAP**=OIPC Assessment Framework

CRMS = Corporate Records Management System

Page 6 of 12

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

PROGRAM: Contact:

Criteria	Actions To Do List	Maturity Rating	Notes
1. Governance and Accountability			•
2 Education and Awareness			•
3. Classification			•
4. Digitization / Documentary Evidence (future based)			•
5. Retention Holds and Disposition			•
6. Archiving/Preservation/ Record Transfers			•
7. Records Maintenance and Storage			•
8. Security – HR and classified records located with security access	Issue for Managers		•

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services. **IM** = Information Management

OPR = Office of Primary Responsibility **IMCAP**=OIPC Assessment Framework

CRMS = Corporate Records Management System

Page 7 of 12

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

PROGRAM: Contact:

Criteria	Actions To Do List	Maturity Rating	Notes
1. Governance and Accountability			•
2 Education and Awareness			•
3. Classification			•
4. Digitization / Documentary Evidence (future based)			•
5. Retention Holds and Disposition			•
6. Archiving/Preservation/ Record Transfers			•
7. Records Maintenance and Storage			•
8. Security – HR and classified records located with security access	Issue for Managers		•

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services. **IM** = Information Management

OPR = Office of Primary Responsibility **IMCAP**=OIPC Assessment Framework

CRMS = Corporate Records Management System

Page 8 of 12

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

PROGRAM: Contact:

Criteria	Actions To Do List	Maturity Rating	Notes
1. Governance and Accountability			•
2 Education and Awareness			•
3. Classification			•
4. Digitization / Documentary Evidence (future based)			•
5. Retention Holds and Disposition			•
6. Archiving/Preservation/ Record Transfers			•
7. Records Maintenance and Storage			•
8. Security – HR and classified records located with security access	Issue for Managers		•

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services. **IM** = Information Management

OPR = Office of Primary Responsibility **IMCAP**=OIPC Assessment Framework

CRMS = Corporate Records Management System

Page 9 of 12

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

PROGRAM: Contact:

Criteria	Actions To Do List	Maturity Rating	Notes
1. Governance and Accountability			•
2 Education and Awareness			•
3. Classification			•
4. Digitization / Documentary Evidence (future based)			•
5. Retention Holds and Disposition			•
6. Archiving/Preservation/ Record Transfers			•
7. Records Maintenance and Storage			•
8. Security – HR and classified records located with security access	Issue for Managers		•

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services. **IM** = Information Management

OPR = Office of Primary Responsibility **IMCAP**=OIPC Assessment Framework

CRMS = Corporate Records Management System

Page 10 of 12

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

PROGRAM: Contact:

Criteria	Actions To Do List	Maturity Rating	Notes
1. Governance and Accountability			•
2 Education and Awareness			•
3. Classification			•
4. Digitization / Documentary Evidence (future based)			•
5. Retention Holds and Disposition			•
6. Archiving/Preservation/ Record Transfers			•
7. Records Maintenance and Storage			•
8. Security – HR and classified records located with security access	Issue for Managers		•

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services. **IM** = Information Management

OPR = Office of Primary Responsibility **IMCAP**=OIPC Assessment Framework

CRMS = Corporate Records Management System

Page 11 of 12

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

PROGRAM: Contact:

Criteria	Actions To Do List	Maturity Rating	Notes
1. Governance and Accountability			•
2 Education and Awareness			•
3. Classification			•
4. Digitization / Documentary Evidence (future based)			•
5. Retention Holds and Disposition			•
6. Archiving/Preservation/ Record Transfers			•
7. Records Maintenance and Storage			•
8. Security – HR and classified records located with security access	Issue for Managers		•

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services. **IM** = Information Management

OPR = Office of Primary Responsibility **IMCAP**=OIPC Assessment Framework

CRMS = Corporate Records Management System

Page 12 of 12

Ministry of Health

Information Management

Best Practises for Continuous Improvement

DRAFT 2018-11-01

1. Governance and Accountability

- **Records management accountabilities**
 - **Ministry-specific records management policies / procedures**
- 1.1 Assign program level record custodians and delegate IM tasks.
 - 1.2 Produce program level IM task list with calendarized items for record custodians.
 - 1.3 Produce program level IM*Guide for staff. IM*Guide needs to include:
 - a. information on OPR for all records created or received,
 - b. official location for filing records (paper / LAN address / EDRMS CM),
 - c. list of who can create new folders in chosen locations, and
 - d. process step details and links to GRS guides for all IM tasks to assist current and future record custodians.
 - 1.4 Ensure each IM process step is assigned to staff and that those responsibilities are included in job description(s) and My Performance Plan(s). (Do all staff file records or is this task specialized?)
 - 1.5 Ensure Office of Primary Responsibility (OPR) is understood and assigned to all record types created or received by the Branch.
 - 1.6 For records with Superseded / Obsolete (SO) designations, ensure there are defined conditions or that a review of the records is calendarized and responsibility assigned.
 - 1.7 Specifically assign responsibility for Final Disposition steps for records. (DE/SR/FR).
 - 1.8 Assign orientation training responsibilities for new staff.
 - 1.9 Assign responsibility for checking IM work is completed to standards included in IM*Guide.
 - 1.10 Ensure staff know where to find the program IM*Guide. Have a standard location – webpage, LAN or paper copy.
 - 1.11 Assign responsibility to update IM*Guide.
 - 1.12 If EDRMS Content Manager is not available, use LAN with ARCS/ORCS coding for official digital filing.
 - 1.13 Clean up SharePoint site.
 - a. Move/Copy official records from SharePoint to ARCS/ORCS coded LAN folders.
 - b. Remove records from SharePoint that are no longer required for consulting or reference purposes.
 - c. Create schedule for moving/copying records from SharePoint to LAN. Complete filing regularly - do not wait for projects to be completed.

Branch or Division Level

- 1.14 Create and maintain inventory of record custodians for Division to ensure responsibilities have been assigned and to provide a contact list for communicating updates and changes to IM procedures.

2. Education and Awareness

- **Mandatory employee training**
- **Role specific training**

- 2.1 Develop reference list of IM training requirements and assign for each staff position with IM responsibilities. List to include Learning Centre and other courses.
- 2.2 Ensure current and new staff complete required IM training as assigned to their positions responsibilities.
- 2.3 Ensure new staff are aware of their training requirements during their initial orientation.
- 2.4 Assign responsibility for updating of training list.
- 2.5 Ensure during initial orientation, new staff are provided a program level IM*Guide.
- 2.6 Assign responsibility for checking new staff are oriented to IM standards and guidance materials. Add to My Performance Profiles or set up tracking if required.

Branch or Division Level

- 2.7 Centralized tracking of completion of IM117, by the Deputy Minister's office, is successfully working to ensure this course is completed by all staff.
- 2.8 Produce program level IM*Guide for staff which includes:
 - a. List of services provided by Records Officers and contact information.
 - b. Provide links/addresses to centralized GRS guides and tools.
 - c. Description of how to create short cuts in Internet Explorer to simplify filing to program level folders.
 - d. Best practises for email management; (link to GRS guide when developed)
 - i. Use of Outlook folders to separate transitory and official filing for each project/subject,
 - ii. Adding dates YYYY-MM-DD to beginning of subject line in Outlook, prior to filing emails,
 - iii. Use hyperlinks to reference documents in emails rather than attaching,
 - iv. How to create a hyperlink.

3. Classification

- **Record classification**

- 3.1 Program Area to develop standard folder and file naming conventions for IM
- 3.2 Program to use ARCS / ORCS coding, to classify their official records in all systems.
- 3.3 Ensure LAN file paths include folders labeled with ARCS/ORCS.
- 3.4 Move/refile records into ARCS/ORCS classified file paths where staff have chosen to create ad hoc folders rather than identify and use the most appropriate classifications.
- 3.5 Train all staff on ARCS/ORCS classifications and how to identify appropriate codes for use when they are not listed in program level IM*Guide.
- 3.6 File HR records in official location rather than in personal H: drives of admin staff. Give access to admin staff or provide alternative process for transferring records to official location.
- 3.7 Update LAN file path names to include ARCS/ORCS coding where records are currently sorted into ARCS/ORCS classifications.
- 3.8 Develop new ARCS/ORCS LAN framework to refile records currently stored on the LAN or SharePoint sites in ad hoc folder systems.
- 3.9 Produce program level IM*Guide for staff which includes:
 - a. List of commonly used ARCS and ORCS classifications for program area,
 - b. Method to identify ARCS/ORCS coding when not included in the IM*Guide.
 - c. List of standard naming conventions and folder naming options for all identified types of records produced in the branch.
 - d. Include version control labeling in naming convention standards.

Branch or Division Level

- 3.10 Division establish standard version control labeling for documents. Can be delegated to program level if best practise requires differences between program areas.

4. Digitization / Documentary Evidence

- GRS Digitizing Records Guide - Draft
 - 4.1 Scan paper records with on-going value and place into shared drives.
 - 4.2 Scan paper copies to be sent to off-site storage or destroyed based on Redundant Record Schedule best practises guide
 - 4.3 To prepare introduction of EDRMS Content Manager, develop new ARCS/ORCS LAN framework to clean up and file unclassified records.
 - 4.4 Refile records currently stored without ARCS/ORCS coding. Record sources include personal drives, LAN and SharePoint sites.

Branch or Division Level

- 4.5 Program level IM*Guide for staff which includes:
 - a Reference to GRS *Digitalization Best Practices Guide*.
GRS IM Digitizing Guide - Draft

5. Retention, Holds and Disposition

- **Information schedule development and maintenance**
- **Records retention, holds and disposition**
 - 5.1 Assess and clean up transitory paper records and classify official paper records, using ARCS/ORCS, not included in CRMS inventories or duplicated in LAN folders.
 - 5.2 Process on-site paper records through semi-active (off-site storage) and final dispositions (DE/SR/FR).
 - 5.3 Centralize paper HR records into “locked” cabinets or scan and file in ARCS LAN folders, then shred paper copies as per the Redundant Records Schedule best practices.
 - 5.4 Identify digital records, ensure ARCS classification and prepare inventories.
 - 5.5 Assign responsibility for tracking dispositions.
 - 5.6 Schedule review of dispositions of record inventories.
 - 5.7 Schedule disposition IM tasks for program area records.

Branch or Division Level

- 5.8 Identify and assign responsibility for on-site and off-site paper records through ownership of CRMS Org units. CRMS currently has unassigned record inventories.
- 5.9 Physically find and inventory on-site records listed in CRMS Org Units.
- 5.10 Develop official Hold procedure for litigation and FOI processes

6. Archiving / Preservation / Record Transfers

- **Identify and protect digital records scheduled for archiving**
 - **Record transfers to Information Management Act (IMA) bodies**
- 6.1 Ensure record custodian duties include assignment of processing of records through final disposition.
 - 6.2 Produce program level IM*Guide for staff which includes:
 - a. CRMS Org Units assigned ownership / responsibilities.
 - b. How to print record lists (inventories) from CRMS.
 - c. How to analyse LAN records for next steps in disposition processing.

Branch or Division Level

- 6.3 Work with IT staff to approve use of application that can print list of records in ARCS/ORCS dedicated shared drives (LANs). Lists need to include ARCS/ORCS schedules associated with records. (Beta version app has been developed to produce Excel document)
- 6.4 Produce Branch or Division Level IM*Guide for staff which includes:
 - a. Standard process, with associated required documentation to track record transfers, for ministry reorganizations, and through transfer of records to Ministry of Attorney General, the Royal Museum Archives or other government organizations such as Health Authorities.
- 6.5 Work with GRS to introduce EDRMS Content Manager.

7. Records Maintenance and Storage

- **Manage information in record keeping systems (schedules)**
- **Manage physical records**
- **Inventory of Ministry systems and repositories**

- 7.1 Analyse paper records on-site to determine if they are currently listed in an inventory (CRMS) and process accordingly.
 - a. Add to CRMS if required.
 - b. Request destruction via GRS process for DE eligible records.
 - c. Send to off-site storage if time for DE is not within this next year.
 - d. Process and send records to off-site storage if final disposition is SR/FR.
- 7.2 Assess LAN records and request destruction via GRS process for DE eligible digital records.
- 7.3 Assess LAN records to place some digital records into semi-active LAN locations. (Museum Archives has requested ministries hold their SR/FR digital records at this time.)
- 7.4 Produce program level IM*Guide for staff which includes:
 - e. Program level process to complete GRS destruction requests and to maintain required tracking.
 - f. Process for record recalls and returns to off-site storage including tracking.
 - g. Process for maintaining and updating staff authorizations via GRS, to recall records from off-site.
 - h. 60-day notice procedures to ensure approval and tracking of decision to destroy or hold records.

Branch or Division Level

- 7.5 Assign responsibility to CRMS Org Units. This will provide linkages to AXIS Indented Org Charts and off-site accessions.
- 7.6 Develop security Hold procedure that will mark paper or digital records to ensure the records are safeguarded from destruction or transfer to another organization. "Hold" is to avoid final disposition processing. (used for litigation and FOI purposes)
- 7.7 Assign management of record security Holds to a job position and add to the job description to ensure management of the Holds over time. (staff turn over issue)
- 7.8 Assign responsibility for checking that Divisional/Branch records management tasks are completed and up to documented standards.
- 7.9 Produce Division/Branch Level IM*Guide for staff which includes:
 - a. Assign responsibility to monitor records under litigation "Holds".

8. Information protection – related to IM not systems

- **Security program**
 - Employee Training – covered in section 2
 - Role Based Training – covered in section 2
 - **Employee accountabilities**
 - **Security classification**
 - **User access and responsibilities**
- 8.1 Analyse if current structure of LAN security restrictions is adequate to minimize access to records. Ensure staff only have access to the records they need to complete their duties.
- 8.2 Set up secure storage for Human Resource related documents.
- 8.3 Ensure administrative staff have a process to file HR records in a secure location. Discourage use of Personal drives (H: drives) for storing HR records.
- 8.4 Explore the use of LAN folders that offer access to all members within matrix teams. Teams that have members from different branches may wish to have common shared drive folders for official filing. Alternative is explicit process for filing and assignment of IM responsibilities.
- 8.5 Use EDRMS Content Manager or LANs for official storage of digital records. SharePoint systems are not IM systems – risks to using only SP are:
- a. lack of final disposition schedule will result in records being kept too long or not moving to archives,
 - b. searches for FOI and litigation are not easily completed if ARCS or ORCS are not used,
 - c. inventories of records for SP sites is a manual process,
 - d. access to records is restricted by SP administrators, rather than executive and IM officials,
 - e. Crashed SP sites are difficult to recall and at times records are lost.

Information Management Practices IM*Guide

Organized by IMPAC Criteria

Governance and Accountability

1. Information on OPR for all records created or received,
2. Official location for filing records (paper / LAN address / EDRMS CM,
3. List of who can create new folders in chosen locations, and
4. process step details and links to GRS guides for all IM tasks to assist current and future record custodians.
5. Assign responsibility to update IM*Guide.

Education and Awareness

6. List of services provided by Records Officers and contact information.
7. Provide links/addresses to centralized GRS guides and tools.
8. Description of how to create short cuts in Internet Explorer to simplify filing to program level folders.
9. Best practises for email management; (link to GRS guide when developed)
 - a. Use of Outlook folders to separate transitory and official filing for each project/subject,
 - b. Adding dates YYYY-MM-DD to beginning of subject line in Outlook, prior to filing emails,
 - c. Use hyperlinks to reference documents in emails rather than attaching,
 - d. How to create a hyperlink.

Classification

10. List of commonly used ARCS and ORCS classifications for program area,
11. Method to identify ARCS/ORCS coding when not included in the IM*Guide.
12. List of standard naming conventions and folder naming options for all identified types of records produced in the branch.
13. Include version control labeling in naming convention standards.

Digitization / Documentary Evidence

14. Reference to GRS *Digitalization Best Practices Guide*.
[GRS IM Digitizing Guide - Draft](#)

Retention, Holds and Disposition

15. Develop official Hold procedure for litigation and FOI processes.

continued...

Archiving / Preservation / Record Transfers

16. CRMS Org Units assigned ownership / responsibilities.
17. How to print record lists (inventories) from CRMS.
18. How to analyse LAN records for next steps in disposition processing.
19. Standard process, with associated required documentation to track record transfers, for ministry reorganizations, and through transfer of records to Ministry of Attorney General, the Royal Museum Archives or other government organizations such as Health Authorities.

Records Maintenance and Storage

20. Program level process to complete GRS destruction requests and to maintain required tracking.
21. Process for record recalls and returns to off-site storage including tracking.
22. Process for maintaining and updating staff authorizations via GRS, to recall records from off-site.
23. 60-day notice procedures to ensure approval and tracking of decision to destroy or hold records.
24. Assign responsibility to monitor records under litigation "Holds".

Security

No current recommendation for IM*Guide

Information Management Maturity Assessment Fall 2018

Health Sector Information Management and Technology Division

Office or Program Name

Contents

Branch Summary and Overview Recommendations	3
Program 1 – Interviewee	5
Program 2 – Interviewee	7
Program 3 – Interviewee	9

Methodology:

The Records Officer met individually with all Directors and other identified staff to determine the information management practises currently in use within the Division. A standard set of questions was developed from CIRMO's Information Management Capacity Assessment Practises (IMCAP) framework to use during these interviews. The Records Officer requested copies of any program level policy & procedure and guidance documents identified within the interviews. The Records Officer did not follow up with investigations to validate answers.

The records management component of the IMCAP outlined 7 criteria with a range of 5 maturity levels. This assessment also includes an 8th criterion to cover the security of records through staff access controls. The maturity levels are described in this embedded Excel spreadsheet.



2018 Baseline
Assessment Framework

Included in this report are a set of overall recommendations to the Executive Director for best practises that will improve the information management in their Branch. This is followed by detailed reports for each program area with specific ratings and recommendations for each group.

BRANCH NAME

BRANCH NAME

Branch Summary and Overview Recommendations

The below report summarizes current information management practises within your branch. Standard IMCAP ratings indicate the maturity level of current IM processes. Where improvements are required, I have referenced best practice tasks that, if completed, will assist to improve the routines in the branch. There are two levels of recommendations within this report – first an overall branch review with branch level recommendations and then reviews of the individual program areas.

s.13

Ratings of 1 or 2 indicate s.13
s.13

Rating of 3 indicates s.13

Ratings of 4 or 5 indicate s.13
s.13

Brenda Jager | Records Officer

Ministry of Health | Health IT Strategy Branch - Phone: 778 974-4969

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services.


IM = Information Management

OPR = Office of Primary Responsibility IMCAP=OIPC Assessment Framework

Page 3 of 10

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

Criteria	IMCAP Maturity Rating 1-5	Notes and Branch Level Best Practise Recommendations	 IM Best Practices 2018-10-18.docx
1. Governance and Accountability	s.13		
2. Education and Awareness			
3. Classification			
4. Digitization / Documentary Evidence (future based)			
5. Retention Holds and Disposition			
6. Archiving/Preservation/ Record Transfers			
7. Records Maintenance and Storage			
8. Security	s.13	s.13; s.15	

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services.

IM = Information Management

OPR = Office of Primary Responsibility IMCAP=OIPC Assessment Framework

Page 4 of 10

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

Program 1

Contact: Interviewee

Criteria	Actions To Do List	Maturity Rating	Notes
1. Governance and Accountability	s.13		
2 Education and Awareness			
3. Classification			
4. Digitization / Documentary Evidence (future based)			
5. Retention Holds and Disposition			

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services.

IM = Information Management

OPR = Office of Primary Responsibility **IMCAP**=OIPC Assessment Framework

Page 5 of 10

BRANCH NAME

	s.13	
6. Archiving/Preservation/ Record Transfers		
7. Records Maintenance and Storage		
8. Security – HR and classified records located with security access	s.13	s.13; s.15

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

Program 2 Contact: Interviewee

Criteria	Actions To Do List	Maturity Rating	Notes
1. Governance and Accountability	s.13		
2 Education and Awareness			
3. Classification			
4. Digitization / Documentary Evidence (future based)			

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services. **IM** = Information Management

OPR = Office of Primary Responsibility **IMCAP**=OIPC Assessment Framework

Page 7 of 10

BRANCH NAME

	s.13	
5. Retention Holds and Disposition		
6. Archiving/Preservation/Record Transfers		
7. Records Maintenance and Storage		
8. Security – HR and classified records located with security access	s.13	s.13; s.15

Information Management Maturity Assessment Fall 2018
Health Sector Information Management and Technology Division

BRANCH NAME

Program 3: Contact: Interviewee

Criteria	Actions To Do List	Maturity Rating	Notes
1. Governance and Accountability	s.13		
2 Education and Awareness			
3. Classification			
4. Digitization / Documentary Evidence (future based)			

Maturity Ratings: 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimized

GRS = Government Records Services at Citizens Services. **IM** = Information Management

OPR = Office of Primary Responsibility **IMCAP**=OIPC Assessment Framework

Page 9 of 10

BRANCH NAME

5. Retention Holds and Disposition	s.13	
6. Archiving/Preservation/Record Transfers		
7. Records Maintenance and Storage		
8. Security – HR and classified records located with security access	s.13	s.13; s.15

Ministry of Health

Information Management

Best Practises for Continuous Improvement

DRAFT 2018-10-15

1. Governance and Accountability

- **Records management accountabilities**
 - **Ministry-specific records management policies / procedures**
- 1.1 Assign program level record custodians and delegate IM tasks.
 - 1.2 Produce program level IM task list with calendarized items for record custodians.
 - 1.3 Produce program level *Guide for staff needs to include:
 - a. information on OPR for all records created or received,
 - b. official location for filing records (paper / LAN address / EDRMS CM,
 - c. list of who can create new folders in chosen locations, and
 - d. process step details and links to GRS guides for all IM tasks to assist current and future record custodians.
 - 1.4 Ensure each IM process step is assigned to staff and that those responsibilities are included in job description(s) and My Performance Plan(s). (Do all staff file records or is this task specialized?)
 - 1.5 Ensure Office of Primary Responsibility (OPR) is understood and assigned to all record types created or received by the Branch.
 - 1.6 For records with Superseded / Obsolete (SO) designations, ensure there are defined conditions or that a review of the records is calendarized and responsibility assigned.
 - 1.7 Specifically assign responsibility for Final Disposition steps for records. (DE/SR/FR).
 - 1.8 Assign orientation training responsibilities for new staff.
 - 1.9 Assign responsibility for checking IM work is completed to standards included in *IM Guide.
 - 1.10 Ensure staff know where to find the program *IM Guide. Have a standard location – webpage, LAN or paper copy.
 - 1.11 Assign responsibility to update *IM Guide.
 - 1.12 If EDRMS Content Manager is not available, use LAN with ARCS/ORCS coding for official digital filing.
 - 1.13 Clean up SharePoint site.
 - a. Move/Copy official records from SharePoint to ARCS/ORCS coded LAN folders.
 - b. Remove records from SharePoint that are no longer required for consulting or reference purposes.
 - c. Create schedule for moving/copying records from SharePoint to LAN. Complete filing regularly - do not wait for projects to be completed.

Branch or Division Level

- 1.14 Create and maintain inventory of record custodians for Division to ensure responsibilities have been assigned and to provide a contact list for communicating updates and changes to IM procedures.

2. Education and Awareness

- **Mandatory employee training**
- **Role specific training**

- 2.1 Develop reference list of IM training requirements and assign for each staff position with IM responsibilities. List to include Learning Centre and other courses.
- 2.2 Ensure current and new staff complete required IM training as assigned to their positions responsibilities.
- 2.3 Ensure new staff are aware of their training requirements during their initial orientation.
- 2.4 Assign responsibility for updating of training list.
- 2.5 Ensure during initial orientation, new staff are provided a program level IM *Guide.
- 2.6 Assign responsibility for checking new staff are oriented to IM standards and guidance materials. Add to My Performance Profiles or set up tracking if required.

Branch or Division Level

- 2.7 Centralized tracking of completion of IM117, by the Deputy Minister's office, is successfully working to ensure this course is completed by all staff.
- 2.8 Produce program level *Guide for staff which includes:
 - a. List of services provided by Records Officers and contact information.
 - b. Provide links/addresses to centralized GRS guides and tools.
 - c. Description of how to create short cuts in Internet Explorer to simplify filing to program level folders.
 - d. Best practises for email management; (link to GRS guide when developed)
 - i. Use of Outlook folders to separate transitory and official filing for each project/subject,
 - ii. Adding dates YYYY-MM-DD to beginning of subject line in Outlook, prior to filing emails,
 - iii. Use hyperlinks to reference documents in emails rather than attaching,
 - iv. How to create a hyperlink.

3. Classification

- **Record classification**

- 3.1 Program Area to develop standard folder and file naming conventions for IM
- 3.2 Program to use ARCS / ORCS coding, to classify their official records in all systems.
- 3.3 Ensure LAN file paths include folders labeled with ARCS/ORCS.
- 3.4 Move/refile records into ARCS/ORCS classified file paths where staff have chosen to create ad hoc folders rather than identify and use the most appropriate classifications.
- 3.5 Train all staff on ARCS/ORCS classifications and how to identify appropriate codes for use when they are not listed in program level IM *Guide.
- 3.6 File HR records in official location rather than in personal H: drives of admin staff. Give access to admin staff or provide alternative process for transferring records to official location.
- 3.7 Update LAN file path names to include ARCS/ORCS coding where records are currently sorted into ARCS/ORCS classifications.
- 3.8 Develop new ARCS/ORCS LAN framework to refile records currently stored on the LAN or SharePoint sites in ad hoc folder systems.
- 3.9 Produce program level *Guide for staff which includes:
 - a. List of commonly used ARCS and ORCS classifications for program area,
 - b. Method to identify ARCS/ORCS coding when not included in the guide.
 - c. List of standard naming conventions and folder naming options for all identified types of records produced in the branch.
 - d. Include version control labeling in naming convention standards.

Branch or Division Level

- 3.10 Division establish standard version control labeling for documents. Can be delegated to program level if best practise requires differences between program areas.

4. Digitization / Documentary Evidence

- GRS Digitizing Records Guide - Draft
 - 4.1 Scan paper records with on-going value and place into shared drives.
 - 4.2 Scanned paper copies to be sent to off-site storage or destroyed based on Redundant Record Schedule best practises guide
 - 4.3 To prepare introduction of EDRMS Content Manager, develop new ARCS/ORCS LAN framework to clean up and file unclassified records.
 - 4.4 Refile records currently stored without ARCS/ORCS coding. Record sources include personal drives, LAN and SharePoint sites.

Branch or Division Level

- 4.5 Program level *Guide for staff which includes:
 - a Reference to GRS *Digitalization Best Practices Guide*.
GRS IM Digitizing Guide - Draft

5. Retention, Holds and Disposition

- **Information schedule development and maintenance**
- **Records retention, holds and disposition**
 - 5.1 Assess and clean up transitory paper records and classify official paper records, using ARCS/ORCS, not included in CRMS inventories or duplicated in LAN folders.
 - 5.2 Process on-site paper records through semi-active (off-site storage) and final dispositions (DE/SR/FR).
 - 5.3 Centralize paper HR records into “locked” cabinets or scan and file in ARCS LAN folders, then shred paper copies as per the Redundant Records Schedule best practices.
 - 5.4 Identify digital records, ensure ARCS classification and prepare inventories.
 - 5.5 Assign responsibility for tracking dispositions.
 - 5.6 Schedule review of dispositions of record inventories.
 - 5.7 Schedule disposition IM tasks for program area records.

Branch or Division Level

- 5.8 Identify and assign responsibility for on-site and off-site paper records through ownership of CRMS Org units. CRMS currently has unassigned record inventories.
- 5.9 Physically find and inventory on-site records listed in CRMS Org Units.
- 5.10 Develop official Hold procedure for litigation and FOI processes

6. Archiving / Preservation / Record Transfers

- **Identify and protect digital records scheduled for archiving**
 - **Record transfers to Information Management Act (IMA) bodies**
- 6.1 Ensure record custodian duties include assignment of processing of records through final disposition.
 - 6.2 Produce program level *Guide for staff which includes:
 - a. CRMS Org Units assigned ownership / responsibilities.
 - b. How to print record lists (inventories) from CRMS.
 - c. How to analyse LAN records for next steps in disposition processing.

Branch or Division Level

- 6.3 Work with IT staff to approve use of application that can print list of records in ARCS/ORCS dedicated shared drives (LANs). Lists need to include ARCS/ORCS schedules associated with records. (Beta version app has been developed to produce Excel document)
- 6.4 Produce Branch or Division Level *Guide for staff which includes:
 - a. Standard process, with associated required documentation to track record transfers, for ministry reorganizations, and through transfer of records to Ministry of Attorney General, the Royal Museum Archives or other government organizations such as Health Authorities.
- 6.5 Work with GRS to introduce EDRMS Content Manager.

7. Records Maintenance and Storage

- **Manage information in record keeping systems (schedules)**
- **Manage physical records**
- **Inventory of Ministry systems and repositories**

- 7.1 Analyse paper records on-site to determine if they are currently listed in an inventory (CRMS) and process accordingly.
 - a. Add to CRMS if required.
 - b. Request destruction via GRS process for DE eligible records.
 - c. Send to off-site storage if time for DE is not within this next year.
 - d. Process and send records to off-site storage if final disposition is SR/FR.
- 7.2 Assess LAN records and request destruction via GRS process for DE eligible digital records.
- 7.3 Assess LAN records to place some digital records into semi-active LAN locations. (Museum Archives has requested ministries hold their SR/FR digital records at this time.)
- 7.4 Produce program level *Guide for staff which includes:
 - e. Program level process to complete GRS destruction requests and to maintain required tracking.
 - f. Process for record recalls and returns to off-site storage including tracking.
 - g. Process for maintaining and updating staff authorizations via GRS, to recall records from off-site.
 - h. 60-day notice procedures to ensure approval and tracking of decision to destroy or hold records.

Branch or Division Level

- 7.5 Assign responsibility to CRMS Org Units. This will provide linkages to AXIS Indented Org Charts and off-site accessions.
- 7.6 Develop security Hold procedure that will mark paper or digital records to ensure the records are safeguarded from destruction or transfer to another organization. "Hold" is to avoid final disposition processing. (used for litigation and FOI purposes)
- 7.7 Assign management of record security Holds to a job position and add to the job description to ensure management of the Holds over time. (staff turn over issue)
- 7.8 Assign responsibility for checking that Divisional records management tasks are completed and up to documented standards.
- 7.9 Produce Branch or Division Level *Guide for staff which includes:
 - a. Assign responsibility to monitor records under litigation "Holds".

8. Information protection – related to IM not systems

- **Security program**
 - Employee Training – covered in section 2
 - Role Based Training – covered in section 2
 - **Employee accountabilities**
 - **Security classification**
 - **User access and responsibilities**
- 8.1 Analyse if current structure of LAN security restrictions is adequate to minimize access to records. Ensure staff only have access to the records they need to complete their duties.
- 8.2 Set up secure storage for Human Resource related documents.
- 8.3 Ensure administrative staff have a process to file HR records in a secure location. Discourage use of Personal drives (H: drives) for storing HR records.
- 8.4 Explore the use of LAN folders that offer access to all members within matrix teams. Teams that have members from different branches may wish to have common shared drive folders for official filing. Alternative is explicit process for filing and assignment of IM responsibilities.
- 8.5 Use EDRMS Content Manager or LANs for official storage of digital records. SharePoint systems are not IM systems – risks to using only SP are:
- a. lack of final disposition schedule will result in records being kept too long or not moving to archives,
 - b. searches for FOI and litigation are not easily completed if ARCS/ORCS is not used,
 - c. inventories of records for SP sites is a manual process,
 - d. access to records is restricted by SP administrators, rather than executive and IM officials,
 - e. Crashed SP sites are difficult to recall and at times records are lost.

Information Management Practices *Guide

Organized by IMPAC Criteria

Governance and Accountability

1. Information on OPR for all records created or received,
2. Official location for filing records (paper / LAN address / EDRMS CM,
3. List of who can create new folders in chosen locations, and
4. process step details and links to GRS guides for all IM tasks to assist current and future record custodians.
5. Assign responsibility to update *Guide.

Education and Awareness

6. List of services provided by Records Officers and contact information.
7. Provide links/addresses to centralized GRS guides and tools.
8. Description of how to create short cuts in Internet Explorer to simplify filing to program level folders.
9. Best practises for email management; (link to GRS guide when developed)
 - a. Use of Outlook folders to separate transitory and official filing for each project/subject,
 - b. Adding dates YYYY-MM-DD to beginning of subject line in Outlook, prior to filing emails,
 - c. Use hyperlinks to reference documents in emails rather than attaching,
 - d. How to create a hyperlink.

Classification

10. List of commonly used ARCS and ORCS classifications for program area,
11. Method to identify ARCS/ORCS coding when not included in the guide.
12. List of standard naming conventions and folder naming options for all identified types of records produced in the branch.
13. Include version control labeling in naming convention standards.

Digitization / Documentary Evidence

14. Reference to GRS *Digitalization Best Practices Guide*.
[GRS IM Digitizing Guide - Draft](#)

Retention, Holds and Disposition

15. Develop official Hold procedure for litigation and FOI processes.

continued...

Archiving / Preservation / Record Transfers

16. CRMS Org Units assigned ownership / responsibilities.
17. How to print record lists (inventories) from CRMS.
18. How to analyse LAN records for next steps in disposition processing.
19. Standard process, with associated required documentation to track record transfers, for ministry reorganizations, and through transfer of records to Ministry of Attorney General, the Royal Museum Archives or other government organizations such as Health Authorities.

Records Maintenance and Storage

20. Program level process to complete GRS destruction requests and to maintain required tracking.
21. Process for record recalls and returns to off-site storage including tracking.
22. Process for maintaining and updating staff authorizations via GRS, to recall records from off-site.
23. 60-day notice procedures to ensure approval and tracking of decision to destroy or hold records.
24. Assign responsibility to monitor records under litigation "Holds".

Security

No current recommendation for *Guide

RE: 2018 IMPR Framework

From: Jackson, Brittany CITZ:EX
s.15; s.22
To: Grover, Brent TRAN:EX <Brent.Grover@gov.bc.ca>
Cc: Li, Stephen CITZ:EX <Stephen.Li@gov.bc.ca>
Sent: November 27, 2018 12:48:52 PM PST
Attachments: 2018 Practice Review Framework CURRENT.xlsx

Hi Brent,

Attached below is our 2018 Practice Review Framework:

Let me know if you have any questions :-)

Brittany

Brittany Jackson | Senior Auditor
Privacy, Compliance and Training Branch <<https://intranet.gov.bc.ca/thehub/corporate-information-and-records-management-office/privacy-compliance-training>>
Corporate Information and Records Management Office
Ministry of Citizens' Services | T: (250) 356-9639

From: Grover, Brent TRAN:EX
Sent: Tuesday, November 27, 2018 12:40 PM
To: Jackson, Brittany CITZ:EX; Li, Stephen CITZ:EX
Subject: 2018 IMPR Framework

Hi Brittany/Stephen, can you please send me a copy of the 2018 Practice Review Framework please.

Thanks

Brent Grover
Project Manager, Information Management and Records
Information Management Branch | Finance and Management Services Department | Ministry of Transportation and Infrastructure
3rd Floor 940 Blanshard Street, Victoria BC
Cell: 250-886-6360

2018 Practice Review Framework

Criteria	
Domain	# of Assessment Criteria
Privacy	23
Records Management	14
Information Access	7
Information Protection	17
	61

NOTE: certain criteria are grayed out within the domain tabs of this framework. These criteria relate to requirements that are not yet in force. Staff will gather information about the criteria to raise awareness and encourage development of work processes but will not score ministries on these criteria until those requirements are fully implemented.

Source Requirements

The criteria are based on existing legislative and policy requirements which include the following sources.

PMAP	Privacy Management and Accountability Policy
FOIPPA	Freedom of Information and Protection of Privacy Act
ETA	Electronic Transactions Act
CPC12	Core Policy Chapter 12
AUP	Appropriate Use Policy
WOWP	Working Outside the Workplace Policy
ISP	Information Security Policy
RIM	Recorded Information Management (RIM) Manual
IMA	Information Management Act
Loukidelis	Loukidelis Report
OIPC	OIPC Recommendations

Privacy		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Accountability for Privacy Management						
1.1	Designated Ministry Privacy Officer The Deputy Minister has named a Ministry Privacy Officer and roles and responsibilities related to privacy in the ministry have been defined.	A Ministry Privacy Officer (MPO) has not been named and privacy matters are addressed reactively in an informal and/or ad hoc manner.	An MPO has been identified and is accountable for privacy management, but no documentation regarding roles and responsibilities exists. The responsibilities of the role are not captured in the MPO's job description.	The responsibilities of the MPO have been documented and included in the MPO's job description.	The Deputy Minister (or delegate) monitors the performance of the MPO's duties to confirm that responsibilities are being addressed and support continual improvement over time. Privacy initiatives are supported by the Deputy Minister.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include defining roles and responsibilities related to privacy throughout the Ministry (beyond the MPO), privacy performance is regularly assessed internally, and where appropriate, by independent reviewers, and a formal process of continual improvement is in place.
1.2	Deputy Delegation of Duties If the Deputy Minister has delegated any duties, powers or functions a delegation instrument is in place and all privacy related delegation instruments are maintained and communicated to CIRMO.	The Deputy Minister has not delegated any duties, powers, or functions or assigned responsibilities or has done so without proper documentation. Privacy issues and the delegation of activities are addressed reactively, on a case-by-case basis.	No delegation is documented, but there is informal recognition that there are individual(s) with accountability for certain duties, powers or functions.	The Deputy Minister documents the delegation of any duties, powers, or functions to the MPO using a FOIPPA Delegation Instrument.	The MPO maintains and monitors all FOIPPA Delegation Instruments and assists CIRMO in documenting and monitoring the delegation process.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the MPO working with CIRMO to analyse the delegation process and assignment of responsibilities to determine its effectiveness and compliance with PMAP and FOIPPA. Where required, changes and improvements are made in a timely and effective fashion. The MPO ensures that all changes are documented, Instruments remain current, and all updates are sent to CIRMO.
1.3	MPO Delegation of Duties If the MPO has delegated any duties, powers or functions (such as MPO delegating to an Analyst the review and sign off of PIAs), a formal PMAP delegation instrument is documented, in place, and current. Delegation instruments are maintained and communicated to CIRMO.	The MPO has not delegated any duties, powers, or functions or assigned responsibilities. Privacy issues and the delegation of activities are addressed reactively.	No delegation is documented, but there is informal recognition that there are individual(s) with accountability for certain duties, powers or functions.	The MPO documents the delegation of roles and responsibilities using a PMAP Delegation Instrument to delegate any roles and responsibilities assigned to them. Roles and responsibilities are developed, assigned and documented. Delegation instruments have been communicated to CIRMO.	The MPO maintains and monitors all PMAP Delegation Instruments and assists CIRMO in documenting, keeping updated copies, and monitoring the delegation process.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the MPO working with CIRMO, to analyse the delegation process and assignment of responsibilities to determine its effectiveness and compliance with PMAP and FOIPPA. Where required, changes and improvements are made in a timely and effective fashion. The MPO ensures that all changes are documented, Instruments remain current, and all updates are sent to CIRMO.
1.4	Privacy Policies/Procedures Ministry-specific privacy policies and procedures, incorporating Ministry-specific privacy requirements, have been developed and deployed, where appropriate.	If needed, no documented ministry-specific privacy policies exist. Privacy-related practices across the Ministry are variable and reactive.	No documented Ministry-specific privacy policies are in place, but Ministry-specific privacy practices have been developed. These practices are inconsistent across the Ministry.	Ministry-specific privacy policies have been developed and documented where appropriate.	Ministry-specific privacy policies have been developed and are regularly reviewed and updated to reflect changes in policy and/or privacy risks in the Ministry (e.g., arising from new programs or information systems).	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include having the MPO assist CIRMO with the monitoring and compliance review of policies and procedures concerning personal information and/or the identification of issues of non-compliance and implementation of remedial action to ensure compliance in a timely fashion, and update policies where necessary.
2. Education and Awareness						
2.1	Mandatory Employee Training Employees have completed mandatory training related to privacy (IM117 or equivalent) within an appropriate amount of time and updated periodically.	A large proportion of Ministry employees have not completed mandatory privacy training, and there is no process for monitoring training completion.	Mandatory privacy training has been completed by a majority of Ministry employees, but it is not consistently delivered or monitored.	Employees receive training when they are hired, and refresh training at least every two years. Training is scheduled, timely, consistent and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.)	A Ministry-wide privacy awareness and training program exists and is monitored by the MPO. Mandatory training requirements are tracked and monitored. Additional training activities are regularly scheduled to provide timely and consistent privacy awareness (e.g., emails, posters, presentations, etc.) Employees certify that they are aware of, and understand, their responsibilities under FOIPPA regarding the sharing and protection of personal information in their care.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include demonstration of a strong privacy culture across the Ministry, the requirement that employees complete assignments to validate their understanding, and when privacy incidents or breaches occur, remedial training and awareness activities are conducted and changes to the training curriculum are made in a timely fashion.
2.2	Role Based Privacy Training A process is in place to develop and deliver additional privacy training (beyond IM117) to employees.	There is a general understanding of the need for role-based privacy training, however, employees who require additional privacy training are not identified. Additional training is provided in an ad hoc, reactive manner.	Employees who require additional training relevant to their job are identified by the MPO, but implementation is sporadic and inconsistent, and completion is not tracked or documented.	The MPO has documented a process to identify employees who require additional training and that training is scheduled and delivered in a timely and consistent fashion.	A Ministry-wide privacy awareness and training program, including any additional or role-based training, exists and is monitored by the MPO.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the demonstration of a strong privacy culture across the Ministry, and/or the requirement that all additional training requires employees to complete assignments to validate their understanding specific to their roles and responsibilities. When privacy incidents or breaches occur, remedial training as well as changes to the training curriculum take into account role-based training, and are made in a timely fashion.
3. Privacy Impact Assessments						
3.1	Process for PIAs The MPO has developed and communicated Ministry processes for the completion of PIAs within their Ministry, and these are easily accessible by all employees.	The MPO has not developed an internal process regarding assessing privacy impacts within their Ministry. Privacy impacts are assessed in an ad hoc, reactionary manner.	Privacy impacts are considered during some changes to business processes and/or supporting application systems; however, these processes are not documented, and the procedures are inconsistently applied.	The MPO has developed, maintained, and made available processes regarding the completion of PIAs within their Ministry, and these are easily accessible by all employees.	The MPO monitors and reviews compliance with policies and procedures regarding the completion of, and access to, privacy impact assessments.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of PIA processes within the Ministry. Such information is analyzed and, where necessary, changes are made to improve effectiveness and accessibility.

3.2	Inventory of PIAs The MPO has a current inventory of PIAs completed and in progress, and a process to follow up on outstanding items.	The MPO has not developed an inventory of completed or in-progress PIAs, and there is not a process to follow up on outstanding items.	The MPO has an understanding of which PIAs have been completed by the Ministry and where there are outstanding items; however, tracking is done informally and is not fully documented or complete.	The MPO has developed, maintained and published a PIA inventory to track which PIAs are completed or are in progress. The MPO has established a documented process to follow up on outstanding items.	The MPO monitors and reviews all updates to the PIA inventory, and monitors the completion of outstanding items.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include conducting regular quality reviews and other assessments to determine the effectiveness of the PIA inventory and any formalized follow up processes, and the incorporation of findings into process improvements where necessary.
3.3	Requirement to Complete PIAs There is a process in place to ensure that PIAs are completed prior to the start of any proposed enactment, system, project, program or activity. This process includes the sharing of PIAs with CIRMO and follow up to ensure CIRMO feedback is addressed prior to the PIA being finalized. Once complete, PIAs are sent to CIRMO for retention and entry into the Personal Information Directory (PID).	The MPO has not developed a process to ensure compliance with the requirement to complete PIAs prior to the start of any proposed enactment, system, project, program or activity. There is little to no communication with CIRMO during impact assessments prior to their finalization.	The MPO has not documented a process to ensure compliance with the requirement to complete PIAs prior to the start of any proposed enactment, system, project, program or activity. There is some communication with CIRMO during impact assessments prior to their finalization; however, these processes are not documented, and are inconsistent in practice.	There is a documented process in place to ensure that PIAs are completed prior to the start of any proposed enactment, system, project, program or activity. This process includes sharing PIAs with CIRMO and following up to ensure CIRMO feedback is addressed prior to the PIA being finalized. Once complete, PIAs are sent to CIRMO for retention and to be entered into the Personal Information Directory (PID).	The MPO monitors and reviews compliance with the internal policies and procedures for ensuring the timing of completed PIAs, sharing PIAs with CIRMO and following up with feedback, and sending the PIA to CIRMO within 30 days.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include conducting regular quality reviews and other assessments to assess the effectiveness of internal processes to track PIA completion timing and engagement with CIRMO prior to finalization, and updates to processes to address findings where necessary.
4. Agreements						
4.1	Completion and updating of ISAs, RAs, CPAs and IPAs The MPO has a process to identify when ISAs, RAs, CPAs, and IPAs need to be developed and/or updated. This process includes engagement by the MPO as part of the development or updating of the agreement to ensure the agreements are completed as required.	The MPO has not developed a process to identify instances when ISAs, RAs, CPAs and IPAs must be completed or updated. Agreements are not reviewed by the MPO, and any reviews that do occur are ad hoc and reactionary.	The MPO has developed a process to track the completion and update of ISAs, RAs, CPAs and IPAs. Employee awareness of, and adherence to, these processes is sporadic and inconsistent. The MPO is sporadically engaged in the completion of the agreements.	The MPO has documented processes regarding the completion and updating of ISAs, RAs, CPAs and IPAs and these agreements are completed as required. The MPO is consulted during the development or updating of agreements.	The MPO proactively and regularly engages with ministry employees to inform them about when ISAs, RAs, CPAs and IPAs are to be completed, updated and reviewed.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include conducting regular reviews to determine the effectiveness of the process for identifying when the completion, update, or review of ISAs, RAs, CPAs and IPAs is needed and the updating of processes based on the results of such reviews.
4.2	ISAs are reported to CIRMO The MPO has a process in place to ensure ISAs are reported to CIRMO for entry into the Personal Information Directory (PID) once completed.	The MPO has not developed a process to ensure that ISAs are reported to CIRMO once completed. Any reports to CIRMO are done in an ad hoc and reactionary manner, such as in response to specific requests.	The MPO understands that ISAs should be reported to CIRMO for entry into the PID; however, there is no documented process to ensure this occurs.	The MPO has a documented process to ensure that ISAs are reported to CIRMO for entry into the PID as soon as they are completed.	The MPO monitors and reviews the ISA reporting process to ensure process compliance.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include conducting regular quality reviews to determine the effectiveness of the process for ensuring ISAs are reported to CIRMO and updating the process based on the results of such reviews.
4.3	Inventory of all Research Agreements The MPO has a current inventory of all RAs completed and in progress, and a process to follow up on outstanding items.	The MPO has not developed an inventory of RAs that are completed or in progress, and there is no documented process to follow up on outstanding items.	The MPO understands which RAs have been completed and where there are outstanding items; however, tracking processes are informal and not documented.	The MPO has a documented agreement inventory to track which RAs are completed and in progress. The MPO has established a documented process to follow up on outstanding items.	The MPO monitors and reviews updates to the RA inventory, and monitors and documents the completion of outstanding items.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of the RA inventory and any formalized follow up processes. Such information is analyzed and, where necessary, changes are made to improve effectiveness.
4.4	Monitoring compliance with privacy and security requirements in agreements There is a process in place for the ongoing monitoring of compliance with privacy requirements (e.g. section 30 of FOIPPA) outlined in agreements.	There is no process in place for monitoring counterparty compliance with privacy requirements.	The MPO communicates certain privacy requirements to counterparties; however, the requirements are not documented, and there is no formal process to track compliance.	There is a documented process for the ongoing monitoring of counterparty compliance with privacy requirements.	The MPO monitors and reviews the process for monitoring counterparty compliance with privacy requirements. Corrective actions are discussed with counterparties.	Through review of prior agreements, the MPO is kept current on the effectiveness of the monitoring process. Where necessary, changes are made to existing and future agreements in order to improve compliance.
5. Service Provider Management						
5.1	Privacy Protection Schedules Privacy Protection Schedules are included for contracts containing personal information, and the MPO is made aware of all such contracts.	The MPO has little or no awareness about which contracts contain personal information and Privacy Protection Schedules are often not included in contracts containing personal information.	The MPO has some understanding about which contracts contain personal information, but there is no documented process for ensuring that the MPO is aware of such contracts. Privacy Protection Schedules are sometimes included in contracts containing personal information, but are incomplete or inconsistently applied.	Privacy Protection Schedules are included for contracts containing personal information, and the MPO is made aware of all such contracts.	The MPO monitors and reviews contracts containing personal information to ensure that Privacy Protection Schedules are included and accurate.	Through assessments and the analysis of lessons learned from prior contracts, the MPO is informed of the effectiveness of including and reviewing Privacy Protection Schedules in contracts containing personal information. Such information is analyzed and, where necessary, changes are made to existing and future contracts.
5.2	Inventory of Access to Personal Information The MPO maintains an up to date inventory of service providers or volunteers with access to personal information within the Ministry's custody and control.	The MPO has not developed an inventory of service providers or volunteers with access to personal information.	The MPO has an understanding of which service providers and volunteers have access to personal information however, tracking processes are informal and not documented.	The MPO maintains an inventory of service providers or volunteers with access to personal information, and the inventory is up to date.	The MPO monitors and reviews updates to the inventory of service providers and volunteers with access to Personal Information, including monitoring any relevant changes to access privileges.	Through regular review of the monitoring process, the MPO is kept current on its effectiveness. Where necessary, changes are made to ensure the inventory is accurate and up-to-date.
5.3	Mandatory Service Provider Privacy Training MPOs must ensure that employees who are service providers or volunteers and who collect, create or access personal information, have completed mandatory privacy training related to the collection, use, disclosure, storage and destruction of personal information. This training must be completed prior to providing services.	Documented tracking of service provider and volunteer training is not conducted.	There is sporadic tracking of service provider or volunteer training and/or there is evidence that some service providers or volunteers have taken mandatory training.	There is a documented process for confirming that service providers who collect, create or access personal information have completed mandatory privacy training prior to providing any service that involves personal information. Personnel who work with an information system or program that involves sensitive or high-risk personal information receive appropriate additional training.	Training for service providers and volunteers is documented, scheduled, timely, consistent and is augmented by regular awareness activities (emails, posters, presentations, etc.).	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the demonstration of a strong privacy culture across the Ministry, that is communicated to all service providers and volunteers and that all training requires service providers and volunteers to complete assignments to validate their understanding prior to providing services. When privacy incidents or breaches occur, remedial training as well as changes to the training curriculum are made in a timely fashion.
5.4	Service provider compliance with privacy requirements There is a process in place for the ongoing monitoring of service provider compliance with privacy requirements(e.g. Section 30 of FOIPPA).	There is a lack of awareness of the need for contractors to comply with privacy requirements as detailed in FOIPPA. There are inadequate mechanisms in place in contracts to ensure contractor compliance with privacy requirements.	There are adequate mechanisms in place in contracts to ensure awareness for contractor compliance to FOIPPA but there are insufficient mechanisms in place to deal with issues of non-compliance.	There is a documented process for the monitoring of service provider compliance with privacy requirements. There are adequate provisions in place to deal with issues of non-compliance.	The MPO monitors service provider compliance with privacy requirements. Corrective actions are discussed with service providers.	Through assessments and the analysis of lessons learned from prior service provider agreements, the MPO is informed of the effectiveness of monitoring service provider compliance with privacy requirements. Such information is analyzed and, where necessary, changes are made to existing and future agreements in order to improve compliance.
6. Personal Information Inventories and Directory						
6.1	Create and Maintain Personal Information Inventory A procedure exists to create and maintain a Personal Information Inventory, and to create it within one year of the Personal Information Inventory Policy being published.	There is no procedure to track personal information at the Ministry through creating and maintaining a Personal Information Inventory.	The MPO has a general understanding of the kinds of personal information under the custody or control of the Ministry; however, there is no documented procedure for creating and maintaining a Personal Information Inventory. The tracking of personal information in the Ministry is informal and not fully documented.	A documented procedure exists to create and maintain a Personal Information Inventory. A Personal Information Inventory is created within one year of the Personal Information Inventory Policy being published.	The MPO monitors and reviews the procedure for the creation and maintenance of the Personal Information Inventory. Any setbacks in inventory creation or gaps in inventory maintenance are remediated.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of the Personal Information Inventory and its maintenance. Such information is analyzed and, where necessary, changes are made to improve accuracy and effectiveness.

6.2	Reporting to CIRMO A procedure exists for the creation and reporting to CIRMO of Personal Information Banks as required.	There is no procedure for the creation and reporting of Personal Information Banks (PIBs) to CIRMO.	Some Personal Information Banks are created within the Ministry, and some PIBs are reported to CIRMO; however, there is no documented procedure for determining how and when a PIB must be created or reported to CIRMO.	A documented procedure exists for the creation and reporting to CIRMO of the Personal Information Banks that result from new enactments, systems, projects, programs or activities of the ministry.	The MPO monitors and reviews the procedure for the creation and reporting of the Personal Information Banks to CIRMO.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of the procedure for the creation and reporting (to CIRMO) of Personal Information Banks. Such information is analyzed and, where necessary, changes are made to improve accuracy and effectiveness.
6.3	Health Information Banks <i>For the Ministry of Health:</i> A procedure exists for the creation and reporting (to CIRMO) of Health Information Banks.	There is no procedure for the creation and reporting of Health Information Banks (HIBs) to CIRMO.	Some Health Information Banks are created within the Ministry and reported to CIRMO; however, there is no documented procedure for determining how and when a HIB must be created or reported to CIRMO.	A documented procedure exists for the creation and reporting of Health Information Banks to CIRMO.	The MPO monitors and reviews the procedure for the creation and reporting of the Health Information Banks to CIRMO.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of the procedure for the creation and reporting (to CIRMO) of Health Information Banks. Such information is analyzed and, where necessary, changes are made to improve accuracy and effectiveness.
6.4	Monitoring of Personal Information Directory (PID) A process is in place to review the PID periodically to ensure all PIAs, ISAs, PIBs and, where applicable, HIBs have been submitted to CIRMO and recorded accurately.	There is no process in place to review the PID to ensure PIAs, ISAs, PIBs, and HIBs have been submitted and recorded accurately.	There is no documented process to ensure the necessary PIAs, ISAs, PIBs, and HIBs have been submitted and recorded, and/or no documented process exists to confirm that PID entries have been submitted and accurately recorded.	There is a documented process in place to review the PID periodically to ensure all PIAs, ISAs, PIBs and, where applicable, HIBs have been submitted and recorded accurately.	The MPO monitors PID reviews and ensures that any issues with the submissions or the accuracy of documentation are remediated.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of PID reviews and any follow up processes. Such information is analyzed and, where necessary, changes are made to improve effectiveness and accuracy.
7. Foreign Demands for Disclosure						
7.1	Reporting Foreign Demands A procedure is in place for reporting foreign demands for disclosure to CIRMO.	There is no procedure for reporting foreign demands for disclosure to CIRMO. Any reports to CIRMO are inconsistent and ad hoc.	Foreign demands for disclosure are informally communicated to CIRMO and there is no documented reporting procedure.	A documented procedure in compliance with FOIPPA, is in place for reporting foreign demands for disclosure to CIRMO.	The MPO monitors and reviews the procedure for reporting foreign demands for disclosure to CIRMO.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of reporting foreign demands for disclosure to CIRMO. Such information is analyzed and, where necessary, changes are made to improve timeliness, accuracy and effectiveness.
8. Information Incident Management						
8.1	Information Incident Management If an information incident occurred in the past 12 months, the incident was reported immediately, all CIRMO instructions were followed and all recommendations were implemented.	Few or no procedures exist to identify and manage information incidents; those that exist are not documented and are applied inconsistently.	The MPO has a general understanding about the need to track and ensure the immediate reporting of information incidents however, incident management occurs informally and a notable proportion of incidents are not reported immediately or at all. There are no documented processes for incident management or for reinforcing the requirement to immediately report, and CIRMO instructions and recommendations are inconsistently tracked and followed.	The ministry has a documented process for supporting the Information Incident Management process, which includes actions by the MPO and others to ensure that staff are aware of the requirement to immediately report all information incidents and to participate in the response to incidents for which the ministry has responsibility. In addition, as part of the response to incidents, ministry staff follow CIRMO instructions and recommendations are tracked by the MPO and implemented.	A walkthrough of the information incident management plan is performed periodically with the relevant staff and management, and updates to the program are made as needed. The MPO monitors ministry incident reporting and ministry processes, analyzes trends and root causes, and identifies remediation steps required.	The internal and external information environments are monitored and evaluated for issues affecting incident risk and response; changes and improvements to the information incident management plan and related procedures are made where necessary.

Records Management		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Governance and Accountability						
1.1	Records Management Accountabilities The Ministry has articulated employees' responsibilities for records management and business areas have clearly assigned accountabilities to employees with additional role specific records management duties, as appropriate. There is a clear understanding of respective roles and responsibilities and the names of such person(s) or group(s) and their responsibilities are communicated to internal personnel.	The Ministry has not articulated responsibility for records management. Records management issues are addressed reactively. Few or no staff members are aware of their individual responsibilities for appropriate records management.	The Ministry has not articulated responsibility for records management and the approaches are often informal and fragmented. There is some, but inconsistent, employee awareness of their individual records management responsibilities and the role of the Government Records Service.	Defined roles and responsibilities have been developed and staff are aware of and understand their records management responsibilities. Staff are aware of and work collaboratively with the Government Records Service.	Management regularly reviews the ministry's records management program and seeks ways to improve the program's performance, including appropriate and adequate resources.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include support being provided by specialist teams and records management duties being devolved to teams and individuals within the ministry. Innovative ideas and continuous improvement are encouraged.
1.2	Ministry-Specific Records Management Policies/Procedures Records management policies and/or procedures have been defined as appropriate for the ministry and any changes to those are communicated to staff.	No Ministry-wide records management policies and/or procedures are in place.	Employees are provided guidance on corporate and ministry specific records management policies and/or procedures but employee awareness remain inconsistent across the Ministry. There may be gaps in the ministry specific policies or procedures that have been developed.	Ministry-specific records management policies and/or procedures have been documented and are communicated to Ministry employees. Changes to such directives are also communicated.	Records management policies and/or procedures are regularly reviewed and updates are communicated shortly after changes are approved. Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include regular communications about the RM program that has led to high visibility and a higher level of awareness for employees or instances where program objectives are being met and new idea generation is common.
2. Education and Awareness						
2.1	Mandatory Employee Training Employees have completed mandatory training related to records management (IM117).	A large proportion of Ministry employees have not completed mandatory records management training, and there is no process for monitoring training completion.	Mandatory records management training has been completed by a majority of Ministry employees, but it is sometimes delayed (beyond the required 6 month window) and/or not consistently delivered or monitored.	Employees receive training when they are hired, and refresher training is provided at least every two years. Training is scheduled, timely, consistent and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.)	A ministry-wide records management awareness program exists (beyond basic training requirements) and there is a process for follow up where training or awareness gaps exist. Training is scheduled, timely, consistent and is augmented by regular awareness activities (emails, posters, presentations, etc.). All employees certify annually that they are aware of, and understand, their records management responsibilities.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the development of innovative methods for training and/or training objectives being based on core organizational goals and specific role-based training being developed to service specific needs.
2.2	Role Specific Training Individuals have received additional, role-specific records management training where appropriate.	There is a general understanding of the need for role-based records management training; however, employees who require such training are not identified. Additional training is provided in an ad hoc, reactive manner.	Employees who require additional training relevant to their roles are identified, but training is sporadic and inconsistent, and completion is not tracked or documented.	There is a documented process in place to identify employees who require additional training. All additional training is scheduled and delivered in a timely and consistent manner.	A Ministry-wide records management awareness and training program, including any additional or role-based training, exists and is monitored.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the demonstration of a strong records management culture across the Ministry, and/or the requirement that all additional training requires employees to complete assignments to validate their understanding specific to their roles and responsibilities.
3. Classification						
3.1	Record Classification The ministry has procedures in place to classify and/or organize records so that the records can be managed according to the function of the information and the approved retention schedules.	Documented procedures are not in place to classify or organize records and an ad-hoc approach is generally taken that does not always align with official and approved retention schedules. Where no schedule exists for certain records no documented procedure exists to help arrange and organize records except an informal business taxonomy.	Procedures for classifying information according to the appropriate retention schedules (or where no schedules exist) have not been developed but some repeatable processes are observed. There is increasing awareness of information classification requirements.	Procedures are documented and cover all required classification and categorization activities, including how to identify, make accessible, and protect information to which no schedule applies. Employees are made aware of the classification requirements and how to meet them, including the use of classification tools.	Procedures are in place and implemented to enable compliant classification activities for records. Automated tools are used for managing information where appropriate. Management monitors compliance with information classification requirements.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the configuration and implementation of auto-classification tools to enable classification of content across repositories.
4. Digitization / Documentary Evidence						
4.1	4.1 Digital Records The ministry has plans, resources, and technology in place to ensure that all non-exemptive government information will be managed digitally in compliance with the Information Management Act and applicable laws, policies, directives, standards, and specifications.	Digitization has not been identified as a ministry priority; digitization happens in an ad-hoc manner and may not adhere to Government policy, specifications, or directives. Records are regularly created and retained in non-digital form.	Digitization and image management procedures, resources, and technology are available to some areas within the ministry but have not been fully deployed or validated for conformance to the relevant laws, policies, directives, standards and specifications. Some records are created digitally but in an ad hoc manner.	Digitization and image management procedures and technologies have been validated for conformance to the relevant legal and policy requirements, and are scalable and available for use. Records are created digitally, and digitization of existing non-digital records takes place.	Compliance with objectives of the digitization program are monitored and achieve compliance with laws, policies, directives, standards, and specifications. Instances of non-compliance are identified and remediated in a timely manner. New records are created and managed digitally and there are plans for the ongoing transition of remaining non-digital records to fully digital format where required.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include a transition to fully digital processes and/or a mandate to use digital processes over analogue record processes.
5. Retention, Holds and Disposition						
5.1	Information Schedule Development and Maintenance The ministry has a process to support and enable the development and implementation of information schedules. The ministry collaborates with GRS to maintain the currency of existing schedules and to develop a procedure to identify records that are not covered by approved schedules.	No process has been established to support and enable the development, implementation, and ongoing maintenance of information schedules.	Processes to support and enable the development, implementation, and ongoing maintenance of information schedules are informal or are not documented. Critical records are not scheduled as a priority.	The ministry has documented its process for supporting the development, implementation, and maintenance of information schedules. The Ministry has adopted and documented a process to identify information not covered by an approved schedule and enable the development of schedules with critical records as a priority.	The ministry's information schedules are regularly reviewed and updated with input from subject matter experts. The ministry regularly monitors the processes and assignments of those responsible for information schedule development and maintenance. Where required, changes and improvements are made in a timely manner.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include committing resources to ensure that information schedules are developed with input from subject matter experts and responsible management so that they are easy to understand, easy to apply to large content sets and are compliant, or efforts to automate and synchronize any changes across systems and repositories.

5.2	Records Retention, Holds and Disposition The ministry has procedures to dispose of, transfer, or archive government information based on official policies, specifications, schedules, guidelines, and procedures published by the Government Records Service. In the case of a legal hold or FOI request, the ministry has processes in place to ensure that such records are not destroyed. Where records are scheduled, retention is limited to the scheduled time period and no longer. Unscheduled records are retained.	Information retention practices across the ministry are inconsistent. Employees retain information based on their own knowledge or interpretation of retention requirements, potentially over-retaining or under-retaining information.	Processes for applying the relevant information schedules to the ministry's information have not been adopted ministry-wide, and do not cover all relevant aspects. Information is held beyond its required retention and is not disposed of as permitted. Employees are generally, but not consistently aware of the importance of suspending disposition.	The ministry has documented and made available its procedures for applying the relevant schedules and retaining information in accordance with those schedules, and no longer. Disposition requests are made in accordance with approved schedules. Where no schedule exists, procedures are in place to ensure that unscheduled records are retained. Procedures for suspending disposition have been documented and communicated to employees. These procedures are followed consistently.	The retention of the ministry's information according to approved information schedules and hold procedures is monitored and periodically assessed for appropriateness. Any discrepancies found are reported and remediated in a timely manner.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This can include automated prompts to track the age of records to ensure no redundant and/or unnecessary retention.
6. Archiving / Preservation / Record Transfers						
6.1	Identify and Protect Digital Records Scheduled for Archiving The ministry has documented procedures for identifying, protecting, and maintaining the usability and integrity of digital records scheduled for transfer to archives.	Procedures to identify and protect digital records scheduled for archiving or long term retention are not defined and processes are inconsistent.	Procedures to identify and protect digital records scheduled for archiving or long term retention are not in place, but some informal processes exist.	The ministry has defined and implemented processes and mechanisms to identify any records that are scheduled for archiving or long term retention to protect the usability and integrity of the records.	The ministry has implemented and monitors processes and mechanisms to identify any records that are scheduled for archiving or long term retention to protect the usability and integrity of the records.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the implementation of processes and mechanisms to identify any digital records that are scheduled for archiving or long term retention or systematic monitoring of formats and record repositories to help ensure long term usability.
6.2	Records Transfers to IMA Bodies The ministry has agreements and procedures in place to maintain chain of custody and continuity of control for records during transfers to other bodies covered by the Information Management Act. This includes procedures to monitor such transfers.	Procedures for records transfers to other government bodies are not in place. Limited monitoring of transfers is taking place.	Procedures for records transfers to other government bodies are informal and not documented. Best efforts are made to monitor the transfers but it is not formalized.	Procedures for records transfers to other government bodies and for monitoring of such transfers have been documented and implemented.	Monitoring of all transfers has been implemented, and where issues are encountered they are remediated.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the incorporation of such procedures into existing business processes.
6.3	Records Transfers to Non-IMA Bodies The ministry has documented procedures in place to ensure that records transfers to bodies not covered by the Information Management Act are completed in accordance with an appropriate legal instrument.	Procedures for records transfers outside of government are not in place and such transfers are inconsistent and may not be compliant.	Some procedures for records transfers outside of government are in place, but not consistently followed.	Procedures for records transfers outside of government have been documented. Legal instruments and associated processes have also been defined and implemented where appropriate.	There is a process in place to monitor transfers to non-IMA bodies and any incidents of non-compliance are remediated.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion.
7. Records Maintenance and Storage						
7.1	Manage Information in Recordkeeping Systems The ministry manages government information through its lifecycle using recordkeeping system(s) as appropriate. Systems are used to meet records management requirements, including schedules as mandated in the IMA.	Recordkeeping systems are not implemented and/or procedures are not communicated to employees.	The ministry maintains some but not all of the appropriate records in recordkeeping system(s). The overall management of records is not consistent and/or requirements for lifecycle management of those records are not communicated to employees.	The ministry has established procedures and communicated to employees the processes needed to manage information appropriately in recordkeeping system(s). Ministry records are managed throughout their lifecycle and information schedules are applied but disposition may not be consistently performed.	The Ministry monitors the use of its recordkeeping system(s) and, where instances of non-compliance are identified, steps are taken to remediate as appropriate. The use of systems is periodically reviewed for alignment to Ministry government recordkeeping requirements. Lifecycle management using automated scheduling systems of ministry records is configured and operational. Information schedules are consistently applied to content and routine disposition is in force.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include: * mechanisms and strategies to reduce transitory information; * mechanisms and strategies to identify other repositories of ministry content and encourage the capture of government information within recordkeeping systems; * the establishment and consolidation of recordkeeping system(s) to allow uniform lifecycle management to be applied; and/or * the optimization of information schedules to enable easy classification across disparate systems and platforms.
7.2	Manage Physical Records Documented procedures exist regarding the management and storage of physical records in appropriate onsite storage (commensurate with degree of information sensitivity) and/or approved offsite storage facilities.	Record handling practices are inconsistent and Ministry procedures related to physical record storage are not developed and/or not communicated to employees.	Practices for the handling of physical records are consistent but procedures are not documented and/or communicated to employees.	Physical records procedures are documented and records are managed and stored in appropriate onsite storage (commensurate with information sensitivity) and/or approved offsite storage facilities. Physical records are tracked and access is closely monitored and only authorized use is allowed.	The ministry has documented procedures in place for transferring physical records scheduled for semi-active retention or for archiving to approved offsite storage facilities in accordance with the schedule. Physical record management is monitored and instances of non-compliance are remediated.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include regular monitoring of service agreements to ensure quick retrieval, adequate protective measures and regular audits.

Information Access		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Accountability						
1.1	Information Access Procedures and the Duty to Assist Information Access and Duty to Assist procedures have been clearly defined and have been communicated to all staff. Ministry staff are informed and aware of the appropriate response to FOI requests (e.g., how to conduct a comprehensive and timely search for responsive records, seeking clarification, and execute these steps in accordance to defined procedures).	There are no processes or procedures in place for staff to follow when responding to FOI requests, staff are unaware of their obligations under FOIPPA, and do not respond to FOI requests as required.	Staff responses to FOI requests are ad hoc and inconsistent. There are no documented processes or procedures for staff to follow, and staff knowledge regarding their obligations under FOIPPA is inconsistent.	There are established processes and procedures in place for staff to follow in responding adequately and in a timely fashion to FOI requests. Staff are aware of their obligations under FOIPPA to conduct adequate searches for responsive records and consistently do so in a timely fashion.	The Ministry consistently responds in a timely fashion to FOI requests, adheres to the principles of sound information access management and maintains clear and ongoing communications with its executive on the status of each request. Information access procedures are reviewed at least annually (or upon significant changes to policy or regulatory requirements) and updated as required. Compliance with procedures is regularly monitored and reported to senior leadership.	Level 4 has been obtained and the Ministry strives for continuous improvement in providing comprehensive and timely responses.
1.2	Information Access Accountability Accountabilities for FOI requests are assigned, and roles and responsibilities are clearly defined.	Accountabilities for FOI requests have not been defined or assigned. Resources are assigned reactively as requests are received.	Accountabilities have not been defined, but there is informal recognition of individual responsibility for FOI requests and related processes. The same individuals are commonly involved in these processes but there is no documented description of their responsibilities.	Responsibilities for FOI requests have been defined and are also included in job descriptions for all aspects of the FOI process, at all levels in the organization.	FOI accountabilities are reviewed at least annually and updated as required.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion.
2. Education and Awareness						
2.1	Employee Training Employees have completed mandatory (IM117) training related to FOI/ Information Access.	A large proportion of Ministry employees have not completed mandatory privacy training, and there is no process for monitoring training completion.	Mandatory training for access has been completed by a majority of Ministry employees, but it is sometimes delayed (beyond the required 6 month window) and/or not consistently delivered or monitored.	Employees receive training when they are hired, and refresher training is provided at least every two years. Training is scheduled, timely, consistent and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.)	A Ministry-wide privacy awareness and training program exists and is monitored by the MPO. Training activities are monitored, regularly scheduled to provide timely and consistent privacy awareness (e.g., emails, posters, presentations, etc.) All Employees certify that they are aware of, and understand, their responsibilities under FOIPPA regarding the sharing and protection of personal information in their care.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion.
2.2	Role Specific Training Individuals have received additional, role-specific FOI/Information Access training where appropriate (e.g. ministerial staff, FOI co-ordinators).	There is a general understanding of the need for role-based FOI training; however, employees who require such training are not identified. Additional training is provided in an ad hoc, reactive manner.	Employees who require additional training relevant to their job are identified, but implementation is sporadic and inconsistent, and completion is not tracked or documented.	There is a documented process in place to identify employees who require additional training. All additional training is scheduled and delivered in a timely and consistent fashion.	A Ministry-wide records management awareness and training program, including any additional or role-based training, exists and is monitored.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the requirement that all additional training requires employees to complete assignments to validate their understanding specific to their roles and responsibilities.
3. Minister's Offices & Ministerial Staff						
3.1	Dedicated Public Servant A dedicated Public Servant is designated as the person in charge of all requests involving a Minister's office. This person is accountable for contacting all staff directly, in writing, with the details of the request and directing that staff search for responsive records and respond within a set time period. This individual must also retain a current list of all Ministerial staff that is shared on an ongoing basis with IAO.	A public servant has not been designated as the person in charge of all requests involving a Minister's office.	Accountability has not been assigned to a dedicated Public Servant for these processes, but this role is informally in place and supports FOI requests as they are received.	A dedicated Public Servant has been assigned this role. Responsibilities are formally defined and are also included in this person's job description. This individual retains a current list of all Ministerial staff that is shared on an ongoing basis with IAO.	Accountabilities are reviewed at least annually (or when there are significant changes to policy or regulatory requirements) and updated as required.	FOI request performance is tied to personal performance ratings and continual improvement is supported.
4. Monitoring						
4.1	Monitoring of FOI Requests A documented process is in place to track and monitor all active FOI requests. This includes regular reporting to Ministry leadership and escalation processes to ensure compliance with timeliness and/or "duty to assist" requirements.	No documented monitoring or reporting of FOI requests takes place within the Ministry. No escalation processes or triggers exist to assess the risk of non-compliance with timeliness and duty to assist requirements.	FOI requests are informally monitored by those managing the process but this information is not reported or acted upon. Some escalation processes exist but are used in an ad hoc fashion.	There is a documented process for the monitoring of compliance with FOI /access requirements. There is an escalation process if there is a risk of non-compliance with timeliness and/or "duty to assist".	There is regular monitoring of, and reporting on FOI requests to Ministry leadership. The process ensures that issues are identified and addressed proactively to support completion of requests within the allotted timeframe.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion.
4.2	Monitoring Service Provider Compliance with FOI Requests There is a process in place for the monitoring of service provider compliance with ministry requirements related to FOI requests.	There is no process in place for monitoring service provider compliance with ministry requirements for FOI requests.	The Ministry communicates FOI request compliance requirements to service providers but the requirements are not documented, and there is no process to track compliance.	There is a documented process for the monitoring of service provider compliance with FOI requests and there is an escalation process to mitigate risks of non-compliance with timeliness or "duty to assist" requirements.	The MPO monitors and reviews service provider compliance with processes related to FOI. Corrective actions are addressed with service providers and remediated.	Through assessments and the analysis of lessons learned from prior service provider agreements, the MPO is informed of the effectiveness of monitoring service provider compliance with FOI requirements. Such information is analyzed and, where necessary, changes are made to existing and future agreements in order to improve compliance.

Information Protection		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Information Protection						
1.1	Security Program An Information Security Program has been developed, documented, approved, and implemented based on the Information Security Policy (ISP) developed by the Office of the Government Chief Information Officer (OCIO) and Corporate Information and Records Management Office (CIRMO) with respect to security of personal information. Responsibilities for the Information Security Program are documented and assigned.	No documented security policy or procedures exist and formal accountability for security has not been assigned. Security is managed in an ad-hoc manner.	Security policies or procedures do not exist, but some security processes are in place and operating. Processes may be inconsistent and accountability has not been formally defined.	A security program (aligned with ISP) has been documented in the form of policies and procedures. Formal accountability has been assigned for information security.	The security program is regularly reviewed and updated. Security performance is monitored and reported to Ministry leadership on a regular basis.	Level 4 has been attained and additional measures are in place related to the security program. This could include regular benchmarking of security program performance, or adoption of other leading practices.
1.2	Employee Training Employees have completed training related to the protection of government information (IM117 and IM118).	A large proportion of Ministry employees have not completed mandatory privacy training, and there is no process for monitoring training completion.	Mandatory training has been completed by a majority of Ministry employees, but it is sometimes delayed and/or not consistently delivered or monitored.	Employees receive training when they are hired, and refresher training is provided at least every two years. Training is scheduled, timely, consistent and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.)	A Ministry-wide privacy and security awareness and training program exists and is monitored by the MPO and the MISO. Training activities are monitored, regularly scheduled to provide timely and consistent privacy awareness (e.g., emails, posters, presentations, etc.). All Employees certify annually that they are aware of, and understand, their responsibilities under FOIPPA regarding the sharing and protection of personal information in their care.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to training and awareness. This could include advanced training methodologies (gamification, etc.), coordination of training program development with the OCIO and other Ministries, regular testing of employee knowledge, etc.
1.3	Role Based Training A process is in place to develop and deliver additional training (beyond IM117 and IM118) on Information Protection to employees	There is a general understanding of the need for role-based information protection training; however, employees who require such training are not identified. Additional training is provided in an ad hoc, reactive manner.	Employees who require additional training relevant to their job are identified, but implementation is sporadic and inconsistent, and completion is not tracked or documented.	There is a documented process in place to identify employees who require additional training. Additional training is scheduled and delivered in a timely and consistent fashion.	A Ministry-wide information protection awareness and training program, including any additional or role-based training, exists and is monitored.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the requirement that all additional training requires employees to complete assignments to validate their understanding specific to their roles and responsibilities.
1.4	External Parties Assessment of risks from external party access to government information, information systems or information processing facilities are performed and appropriate security controls implemented prior to granting access.	No process exists for assessing risks associated with access by third parties, and risk assessments are not conducted.	No process exists for risk assessments, but risk assessments are conducted in some cases. Where conducted, these assessments result in the identification and implementation of appropriate mitigating controls.	A documented risk assessment process exists and is communicated to Ministry staff. Reviews are conducted for all external party access.	Risks associated with third-party access are monitored and reported on regularly. Controls are updated to reflect changes to risks on an ongoing basis.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to risk management and external access.
1.5	Asset Management An inventory of information assets and systems exists and is maintained. Ownership of assets is assigned and accountabilities associated with ownership are defined.	No inventory of information assets or systems exists and no ownership has been assigned or is in place.	A basic inventory exists, but there is no documented process for information asset management. Some ownership exists for assets and systems wherein functions related to the protection and management of these assets are fulfilled.	An asset management process is in place and a formal inventory of information assets and systems is maintained. Accountabilities for ownership are clearly defined and implemented.	An inventory of information assets and systems is maintained and actively monitored, and the inventory is updated periodically. Ownership of assets is regularly reviewed and accountabilities are monitored.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to asset management. This could include incorporating ownership accountabilities and performance into personal performance ratings.
1.6	Employee Accountabilities Information protection roles and accountabilities for employees are documented, and employees acknowledge their responsibilities for the protection of personal and sensitive information prior to employment and periodically.	No accountabilities related to security or information protection are documented.	Accountabilities are not documented; however, there is a demonstrated awareness of fundamental security responsibilities. There is no formal acknowledgement or attestation process in place.	Accountabilities for security and information protection are documented and/or included in job descriptions. Ministry staff are required to sign off periodically (i.e., annually) to acknowledge their accountabilities with respect to security and information protection.	Accountabilities for security are defined and regularly updated to reflect changes in Ministry programs and/or compliance requirements. Performance is monitored and reported regularly and there is a process to verify that all staff complete their periodic sign-off.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to human resources security. This could include incorporating security and information protection accountabilities in annual employee performance ratings.
1.7	Physical and Environmental Protection Equipment containing personal or sensitive information must be protected throughout its lifecycle, including secure disposal, to reduce the risks from unauthorized access or loss.	No physical/environmental protection program is documented.	Physical/environmental controls are not documented, but some practices are informally conducted.	Controls are documented regarding equipment protection, including asset disposal.	Controls related to physical/environmental protection are documented and monitored for effectiveness. They are reviewed and updated on a regular basis.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to equipment protection.
1.8	Protection Against Malicious Code There an established process in place to prevent, detect, and resolve malicious code infections on information systems and infrastructure.	No process is in place to prevent, detect and/or resolve malicious code.	No processes related to malicious code are defined, but some informal practices are in place.	Processes related to malicious code are defined and implemented.	Controls related to malicious code are regularly monitored and updated to reflect changes in risk, Ministry operations or compliance requirements. Incidents related to malicious code are reported and followed up on.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to malicious code management. This could include actively monitoring and acting on threat intelligence.
1.9	Security Classification Records are organized so that security classifications can be applied to protect different classes of information based on their sensitivity.	No process is in place for security classification, and classification is not practiced.	No documented process is in place for security classification; however, information is protected based on sensitivity in some cases and/or classification has been accomplished for some data repositories or information systems.	Information security classification processes are formalized and information assets and systems are classified according to the OCIO data security classification standard (or similar). Assets are managed according to their security classification.	Data security classification processes and ratings are regularly reviewed and updated.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to security classification.
1.10	Portable Media A formal inventory of portable media devices is maintained. Where devices are used, they comply with OCIO standards, are encrypted, and are managed with controls appropriate for the sensitivity of the data contained on the media, including logging/tracking and secure storage, transfer and disposal.	No inventory of portable media is maintained. No assessment of compliance of portable media to applicable standards is conducted.	An inventory of portable media is not maintained, but efforts are made informally to minimize and control the use of portable media. In certain cases, the use of portable media is logged/tracked with secure storage, transfer and disposal, but this is not formalized or consistently applied.	An inventory of portable media is in place, an approval process for the use of portable media exists, and the use of portable media is tracked/logged. Appropriate steps are taken to ensure that portable media devices in use comply with applicable OCIO standards and devices are managed with controls appropriate for the sensitivity of the data they contain.	The inventory and tracking/logging of portable media devices is actively maintained and reviewed.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to portable media management. This could include providing more secure mechanisms for data transfer to eliminate the need for portable media.
1.11	User Access and Responsibilities - Users must only access information permitted by their assigned roles and responsibilities -Users must ensure unattended equipment has appropriate protection. -Users must ensure the safety of sensitive information from unauthorized access, loss or damage.	Documented processes for user access, system privileges and review of access privileges are not in place. User awareness of their responsibilities is sporadic and they may be unaware of their responsibilities for maintaining a clean desk and protecting equipment and information while not at their workstations.	There are no documented processes in place, but repeatable practices for access and protection of unattended equipment and information are observed.	Documented processes are in place for user responsibilities and access. Staff is aware of and adheres to the clean desk policy and the need to protect unattended equipment and access to government information.	User responsibilities are up to date and monitored. Access and user controls are kept up to date and are regularly monitored for accuracy and currency.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to access control and user responsibilities.

1.12	Access Control Logical access to personal information is restricted by procedures that address the following matters: - Authorizing and registering internal personnel and individuals - Identifying and authenticating internal personnel and individuals - Access privilege change requests and permissions - Granting system access privileges and permissions - The access rights to information systems must be removed upon termination or change of employment/position of staff. Access rights should be reviewed and monitored at regular intervals, depending on the sensitivity of the information.	Access control processes are not in place and no repeatable processes are observed.	Documented processes are not in place, but repeatable access control practices are observed.	Documented access control processes are in place covering the full range of access management (granting, reviewing, removing, changing, etc.) and they apply to both employees and contractors.	Access controls are regularly monitored, reported on and updated on a regular basis.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to access control. This could include the assessment of instances of inappropriate access attempts to determine root causes and potential exposures and the development of remedial action plans.
1.13	Security requirements for information systems Security controls are identified as part of the business requirements for new information systems or enhancements to existing information systems through the information security risk assessment (the former STRA) process, and controls are implemented and reviewed prior to implementation.	No formal information security risk assessment (ISRA) process exists or is followed. ISRAs are not conducted for all new systems or enhancements to existing systems.	A formal ISRA process does not exist within the Ministry, but ISRAs are conducted on a majority of new systems or system enhancements.	A formal ISRA process is in place in the Ministry. ISRAs are completed for all new systems and system enhancements. Accountabilities for ISRAs are clearly defined.	An inventory of ISRAs (complete and ongoing) is maintained and regularly reviewed. Outstanding items are tracked and monitored to confirm completion.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to security requirements for information systems. This could include taking a "privacy by design" and/or a "security by design" approach that looks to formalize all relevant compliance requirements during the design phase and includes formal testing of security controls prior to, and after, go-live.
1.14	Technical Vulnerability Management - A Vulnerability and Risk Management (VRM) Program has been developed, documented, approved, and implemented by the Office of the Government Chief Information Officer (OCIO). Ministries should identify the criticality of information systems and regularly assess and evaluate information security vulnerabilities, potential risks evaluated, and vulnerabilities mitigated or remediated.	Vulnerability assessments have not been conducted and are not planned.	Vulnerability assessments are conducted in an inconsistent manner. Risks arising from vulnerability assessments are remediated.	Vulnerability assessments are planned and conducted on a regular basis (based on risk). Vulnerabilities are risk ranked and remediated in priority order.	Remediation activities are planned, tracked and verified, and escalation takes place in cases where remediation is not completed.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to vulnerability management. This could include active monitoring of relevant threat intelligence to inform the Ministry's vulnerability management approach and priorities.
1.15	Logging and Monitoring Audit logs recording user and privileged user activities, exceptions, and information security events are kept and protected for an appropriate period of time to assist in monitoring and future investigations. Logs are monitored and the result of the monitoring activities are regularly reviewed and acted upon as necessary.	No audit logs are retained for key systems. No monitoring of access or exceptions is possible.	No logging or monitoring program is in place. Logging is enabled on some key systems. Logs are not monitored, but can be accessed for retrospective review.	Logging is enabled on key systems (based on risk and security classification). Logs are maintained and controls are in place to limit access to these logs. Manual monitoring or basic automated monitoring is in place for critical/high-risk systems.	Log monitoring and correlation capabilities are in place and exceptions are reviewed and acted upon as necessary. Results of monitoring activities are reported and are used to enhance access and security controls on an ongoing basis.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to logging and monitoring. This could include advanced monitoring analytics and/or the use of threat intelligence to regularly update the configuration of monitoring tools.
1.16	Business Continuity Management Business continuity management processes and plans have been developed tested, maintained, updated and they include provisions to maintain security and information protection in the case of an incident.	No business continuity plan has been defined.	No business continuity plan has been defined, but recovery procedures have been defined for some key systems. Security is not addressed formally in these procedures.	A documented business continuity plan exists. The plan includes an assessment of risk and information sensitivity and incorporates appropriate controls to address information protection.	The business continuity plan is regularly reviewed and exercises are conducted on a periodic basis to test and improve the plan.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to business continuity management. This could include regular independent or external reviews of the business continuity plan and involvement of related third parties in exercises and tests.
1.17	Monitoring Service Provider Compliance with Information Protection requirements The Ministry has a process to monitor service provider compliance for information protection requirements	There is a lack of awareness of the need for contractors to comply with government information protection requirements. There are inadequate mechanisms in place in contracts to ensure contractor compliance with information protection requirements	There are adequate provisions in contracts to reinforce compliance with information protection requirements. Contractors are aware of their obligations, but there are insufficient mechanisms in place to deal with issues of non-compliance.	There is a documented process for the monitoring of service provider compliance with information protection requirements. There are adequate provisions in place to deal with issues of non-compliance.	The ministry monitors service provider compliance with information protection requirements. Corrective actions are addressed with service providers and remediated.	Through assessments and the analysis of lessons learned from prior service provider agreements, the ministry is informed of the effectiveness of monitoring service provider compliance with information protection requirements. Such information is analyzed and, where necessary, changes are made to existing and future agreements in order to improve compliance.

RE: Self-Assessment Guidance Material (DRAFT)

From: Thibault, Sarah FIN:EX <Sarah.Thibault@gov.bc.ca>
To: Jackson, Brittany CITZ:EX <Brittany.Jackson@gov.bc.ca>
Cc: Grover, Brent CITZ:EX <Brent.Grover@gov.bc.ca>, Linkletter, Lynette FIN:EX <Lynette.Linkletter@gov.bc.ca>, Thibault, Sarah FIN:EX <Sarah.Thibault@gov.bc.ca>
Sent: August 2, 2018 9:00:24 AM PDT
Attachments: SA Self Assessment Guide - CURRENT_feedback.docx

Hi Brittany,

Thank you so much for sharing. The documents are very helpful!

First, I was happy to see that what we have done so far aligns with the Self Assessment (SA). At a glance you could say we are doing a self assessment; however, to identify and understand our current state, we are completing an inventory which includes our information holdings (data about our information that is under our custody and control).

Second, I am, again, on the edge of my seat until the resources/templates are made available. I particularly liked the 'document log' and 'interview log', and so I have created such documents for the inventory.

Third, I noticed the questions were mainly open-ended. In our case - divisionally, it might be difficult to compile data with mostly open-ended questions, where we drill down into details. However I see the need/benefit for implementing some open-ended questions, particularly when it comes to understanding program area's practices - I have brought this point forward for our inventory.

Few questions so I understand...

1. Why is 7.1, 7.2, 7.3, and 8.3 'N/A' in the Sample Interview Question?
2. Why are documents requested before interviews? Is it so they can be discussed during interviews?

Lastly, you mentioned feedback, and as I am a huge fan of feedback, I have brought some forward.

1. I really liked the walkthrough of the SA, well designed and colourful. I also like that it is only one page.
2. I wrote some notes for the guide - attached below.

Thank you both for giving me this opportunity to learn and gather all the info I need to make our inventory a success. I will keep you posted throughout major milestones and share some of the documents we will have created.

Respectfully,

Sarah Thibault
Divisional Information Management Analyst
Tel: 778.698.4808

RD Information Management Inquiries: FIN.REV.RIM@gov.bc.ca <mailto:FIN.REV.RIM@gov.bc.ca>

From: Jackson, Brittany CITZ:EX
Sent: Monday, July 30, 2018 10:23 AM
To: Thibault, Sarah FIN:EX
Cc: Grover, Brent CITZ:EX
Subject: Self-Assessment Guidance Material (DRAFT)

Hi Sarah,

Attached below is our current, draft guidance material for ministry self-assessments:

<< File: SA Self Assessment Guide - CURRENT.docx >> << File: Sample Interview Questions.docx >> << File: SA IMPR Walkthrough - CURRENT.pptx >>

We are in the midst of approving final versions of these documents – please note that the versions above may become out-of-date within the next few months.

In addition, there are several resources/templates noted within the guide – these resources will be available once the guidance material is finalized.

Please review the attached documents and let me know if you have any questions or feedback.

Brittany

Brittany Jackson | Senior Auditor | Privacy, Compliance and Training Branch
Ministry of Citizens' Services | T: (250) 356-9639

From: Thibault, Sarah FIN:EX
Sent: Friday, July 27, 2018 11:32 AM
To: Jackson, Brittany CITZ:EX
Cc: Thibault, Sarah FIN:EX
Subject: RE: Meeting Follow-up

I'm on the edge of my seat!

Respectfully,

Sarah Thibault
Divisional Information Management Analyst
Tel: 778.698.4808

RD Information Management Inquiries: FIN.REV.RIM@gov.bc.ca <<mailto:FIN.REV.RIM@gov.bc.ca>>

From: Jackson, Brittany CITZ:EX
Sent: Friday, July 27, 2018 10:53 AM
To: Thibault, Sarah FIN:EX
Subject: RE: Meeting Follow-up

Hi Sarah,

Just to follow up – Brent is amending a few of the guidance documents before I pass them on to you.

I should be able to email you the draft material either today or early next week.

Thanks for your patience,
Britt

Brittany Jackson | Senior Auditor | Privacy, Compliance and Training Branch
Ministry of Citizens' Services | T: (250) 356-9639

From: Thibault, Sarah FIN:EX
Sent: Wednesday, July 25, 2018 2:04 PM
To: Jackson, Brittany CITZ:EX
Cc: Thibault, Sarah FIN:EX
Subject: RE: Meeting Follow-up

That is great news! Thanks for the follow-up Brittany.

Respectfully,

Sarah Thibault
Divisional Information Management Analyst
Tel: 778.698.4808

RD Information Management Inquiries: FIN.REV.RIM@gov.bc.ca <<mailto:FIN.REV.RIM@gov.bc.ca>>

From: Jackson, Brittany CITZ:EX
Sent: Wednesday, July 25, 2018 1:52 PM
To: Thibault, Sarah FIN:EX
Subject: RE: Meeting Followup

Hi Sarah,

Sorry for the late response - our team is meeting tomorrow to discuss our draft versions of the self-assessment guidance documentation.

We will also be discussing the possibility of providing sample interview questions within the guidance documentation.

I will connect with you after the meeting and send you any material we are able to (somewhat) finalize during our meeting.

Britt

Brittany Jackson | Senior Auditor | Privacy, Compliance and Training Branch
Ministry of Citizens' Services | T: (250) 356-9639

From: Thibault, Sarah FIN:EX
Sent: Wednesday, July 18, 2018 1:01 PM
To: Jackson, Brittany CITZ:EX
Cc: Thibault, Sarah FIN:EX
Subject: RE: Meeting Followup

Hi Brittany,

Thank you for your response and for reviewing the Executive Summary – I want to make sure I speak about the assessment accurately, especially at an executive level.

A few more questions if you don't mind:

- I believe either Brent or you were able to provide some questions (not the results) for questions that are typically asked during an assessment –referencing the CIRMO pilot assessment. The questions would be helpful in formatting my questions for the inventory.
- Are you able to share the tools used when conducting a self-assessment?

Much appreciated, thank you

Respectfully,

Sarah Thibault
Divisional Information Management Analyst
Tel: 778.698.4808

RD Information Management Inquiries: FIN.REV.RIM@gov.bc.ca <<mailto:FIN.REV.RIM@gov.bc.ca>>

From: Jackson, Brittany CITZ:EX
Sent: Wednesday, July 11, 2018 3:51 PM
To: Thibault, Sarah FIN:EX
Cc: Grover, Brent CITZ:EX
Subject: RE: Meeting Followup

Hi Sarah,

In order to obtain training stats for your division, please connect with your Ministry Privacy Officer (Richard Barlow).

Your executive summary looks great to me – please let us know if you need any assistance while completing your self-assessment.

Thanks,
Brittany

Brittany Jackson | Senior Auditor | Privacy, Compliance and Training Branch
Ministry of Citizens' Services | T: (250) 356-9639

From: Thibault, Sarah FIN:EX
Sent: Monday, July 9, 2018 8:24 AM
To: Jackson, Brittany CITZ:EX
Cc: Grover, Brent CITZ:EX; Thibault, Sarah FIN:EX
Subject: RE: Meeting Followup

Thank you Brittany, much appreciated – looking forward to your reply.

On another note:

Attached is a draft of an Executive Summary for the Information Management Inventory (one pager). Would you/Brent be able to read through and provide some feedback from the lenses of a records professional? Wondering if the document makes sense and if I've interpreted and described the assessment correctly. If you both have some time to do so:, any comments or suggestions is most welcome.

Thank you

Respectfully,

Sarah Thibault
Divisional Information Management Analyst
Tel: 778.698.4808

RD Information Management Inquiries: FIN.REV.RIM@gov.bc.ca <<mailto:FIN.REV.RIM@gov.bc.ca>>

From: Jackson, Brittany CITZ:EX
Sent: Friday, July 6, 2018 3:13 PM
To: Thibault, Sarah FIN:EX; Grover, Brent CITZ:EX
Subject: RE: Meeting Followup

Hi Sarah,

It was nice to meet you today – thanks for asking such great questions, I learned a lot alongside you :)

Our branch's contact for training stats is currently away until July 11 – I will be able to get you the stats shortly after this date.

Thanks,

Britt

Brittany Jackson | Senior Auditor | Privacy, Compliance and Training Branch
Ministry of Citizens' Services | T: (250) 356-9639

From: Thibault, Sarah FIN:EX
Sent: Friday, July 6, 2018 1:29 PM
To: Grover, Brent CITZ:EX
Cc: Jackson, Brittany CITZ:EX
Subject: RE: Meeting Followup

Brent and Brittany,

Thank you both for meeting with me today, and for your openness to share information. I learned a lot and gained some confidence in our inventory direction.

As discussed, please find attached a draft of our information collection for our inventory. As per your feedback, I've added a bullet point regarding "Authorized accessibility/Monitoring list" for digital records. Should you have any other feedback, I welcome it with open arms. I truly value feedback – it's the best way for me to improve on my skills.

Have a great weekend!

Respectfully,

Sarah Thibault
Divisional Information Management Analyst
Tel: 778.698.4808

RD Information Management Inquiries: FIN.REV.RIM@gov.bc.ca <<mailto:FIN.REV.RIM@gov.bc.ca>>

From: Grover, Brent CITZ:EX
Sent: Friday, July 6, 2018 12:42 PM
To: Thibault, Sarah FIN:EX
Cc: Jackson, Brittany CITZ:EX
Subject: Meeting Followup

Hi Sarah, it was nice meeting you today s.22

The document on Office Recordkeeping Systems is on the GRS Intranet (this is the link).
<<https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/records-management/guides/officerecordkeepingsystem.pdf>>

Brittany will forward the link to the training stats shortly.

Thanks

Brent Grover, MPA|Senior Auditor (Practice Reviews)
Investigations and Reviews|Privacy, Compliance and Training Branch|Ministry of Citizens' Services
Ph: 778-698-4992|M: PO Box 9406, Stn Prov Gov, Victoria BC V8W 9V1

The dogmas of the quiet past are inadequate to the stormy present - Lincoln

Government confidentiality and privilege requirements apply to this message and any attachments. If you are not the intended recipient, you are hereby notified that any review, retransmission, conversion to hard copy, copying, circulation or other use is strictly prohibited. If you are not the intended recipient, please notify the sender immediately, and delete this message and any attachments from both your inbox and deleted items folder. Thank You.

Page 081 of 142 to/à Page 098 of 142

Withheld pursuant to/removed as

s.13

2018 Practice Review Framework

Criteria	
Domain	# of Assessment Criteria
Privacy	23
Records Management	14
Information Access	7
Information Protection	17
	61

NOTE: Criteria that are grayed out within the domain tabs of the Practice Review Framework relate to requirements that are not yet in force. Staff will gather information about the criteria to raise awareness and encourage development of work processes but will not score ministries on these criteria until those requirements are fully implemented.

Sources

The criteria are based on existing legislative and policy requirements which include the following sources.

PMAP	Privacy Management and Accountability Policy
FOIPPA	Freedom of Information and Protection of Privacy Act
ETA	Electronic Transactions Act
CPC12	Core Policy Chapter 12
AUP	Appropriate Use Policy
WOWP	Working Outside the Workplace Policy
ISP	Information Security Policy
RIM	Recorded Information Management (RIM) Manual
IMA	Information Management Act
Loukidelis	Loukidelis Report
OIPC	OIPC Recommendations

Privacy					Maturity Scale				
#	Criteria	Maturity Ranking	Rationale	Variance	Initial (1)	Repeatable (2)	Defined (3)	Managed (4)	Optimized (5)
1. Accountability for Privacy Management		#DIV/0!							
1.1	Designated Ministry Privacy Officer The Deputy Minister has named a Ministry Privacy Officer and roles and responsibilities related to privacy in the ministry have been defined.	Enter the maturity ranking (number) applicable for this criteria	Describe the key factors that resulted in the assessed maturity ranking	Where there is a wide range of IM practices note areas that warrant special attention by identifying leading practices or areas that require attention to basic practices	A Ministry Privacy Officer (MPO) has not been named and privacy matters are addressed reactively in an informal and/or ad hoc manner.	An MPO has been identified and is accountable for privacy management, but no documentation regarding roles and responsibilities exists. The responsibilities of the role are not captured in the MPO's job description.	The responsibilities of the MPO have been documented and included in the MPO's job description.	The Deputy Minister (or delegate) monitors the performance of the MPO's duties to confirm that responsibilities are being addressed and support continual improvement over time. Privacy initiatives are supported by the Deputy Minister.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include defining roles and responsibilities related to privacy throughout the Ministry (beyond the MPO), privacy performance is regularly assessed internally, and where appropriate, by independent reviewers, and a formal process of continual improvement is in place.
1.2	Deputy Delegation of Duties If the Deputy Minister has delegated any duties, powers or functions a delegation instrument is in place and all privacy related delegation instruments are maintained and communicated to CIRMO.				The Deputy Minister has not delegated any duties, powers, or functions or assigned responsibilities or has done so without proper documentation. Privacy issues and the delegation of activities are addressed reactively, on a case-by-case basis.	No delegation is documented, but there is informal recognition that there are individual(s) with accountability for certain duties, powers or functions.	The Deputy Minister documents the delegation of any duties, powers, or functions to the MPO using a FOIPPA Delegation Instrument.	The MPO maintains and monitors all FOIPPA Delegation Instruments and assists CIRMO in documenting and monitoring the delegation process.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the MPO working with CIRMO to analyse the delegation process and assignment of responsibilities to determine its effectiveness and compliance with PMAP and FOIPPA. Where required, changes and improvements are made in a timely and effective fashion. The MPO ensures that all changes are documented, Instruments remain current, and all updates are sent to CIRMO.
1.3	MPO Delegation of Duties If the MPO has delegated any duties, powers or functions (such as MPO delegating to an Analyst the review and sign off of PIAs), a formal PMAP delegation instrument is documented, in place, and current. Delegation instruments are maintained and communicated to CIRMO.				The MPO has not delegated any duties, powers, or functions or assigned responsibilities. Privacy issues and the delegation of activities are addressed reactively.	No delegation is documented, but there is informal recognition that there are individual(s) with accountability for certain duties, powers or functions.	The MPO documents the delegation of roles and responsibilities using a PMAP Delegation Instrument to delegate any roles and responsibilities assigned to them. Roles and responsibilities are developed, assigned and documented. Delegation instruments have been communicated to CIRMO.	The MPO maintains and monitors all PMAP Delegation Instruments and assists CIRMO in documenting, keeping updated copies, and monitoring the delegation process.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the MPO working with CIRMO, to analyse the delegation process and assignment of responsibilities to determine its effectiveness and compliance with PMAP and FOIPPA. Where required, changes and improvements are made in a timely and effective fashion. The MPO ensures that all changes are documented, Instruments remain current, and all updates are sent to CIRMO.
1.4	Privacy Policies/Procedures Ministry-specific privacy policies and procedures, incorporating Ministry-specific privacy requirements, have been developed and deployed, where appropriate.				If needed, no documented ministry-specific privacy policies exist. Privacy-related practices across the Ministry are variable and reactive.	No documented Ministry-specific privacy policies are in place, but Ministry-specific privacy practices have been developed. These practices are inconsistent across the Ministry.	Ministry-specific privacy policies have been developed and documented where appropriate.	Ministry-specific privacy policies have been developed and are regularly reviewed and updated to reflect changes in policy and/or privacy risks in the Ministry (e.g., arising from new programs or information systems).	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include having the MPO assist CIRMO with the monitoring and compliance review of policies and procedures concerning personal information and/or the identification of issues of non-compliance and implementation of remedial action to ensure compliance in a timely fashion, and update policies where necessary.
2. Education and Awareness		#DIV/0!							

2.1	Mandatory Employee Training Employees have completed mandatory training related to privacy (IM117 or equivalent) within an appropriate amount of time and updated periodically.				A large proportion of Ministry employees have not completed mandatory privacy training, and there is no process for monitoring training completion.	Mandatory privacy training has been completed by a majority of Ministry employees, but it is not consistently delivered or monitored.	Employees receive training when they are hired, and refresh training at least every two years. Training is scheduled, timely, consistent and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.)	A Ministry-wide privacy awareness and training program exists and is monitored by the MPO. Mandatory training requirements are tracked and monitored. Additional training activities are regularly scheduled to provide timely and consistent privacy awareness (e.g., emails, posters, presentations, etc.) Employees certify that they are aware of, and understand, their responsibilities under FOIPPA regarding the sharing and protection of personal information in their care.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include demonstration of a strong privacy culture across the Ministry, the requirement that employees complete assignments to validate their understanding, and when privacy incidents or breaches occur, remedial training and awareness activities are conducted and changes to the training curriculum are made in a timely fashion.
2.2	Role Based Privacy Training A process is in place to develop and deliver additional privacy training (beyond IM117) to employees.				There is a general understanding of the need for role-based privacy training, however, employees who require additional privacy training are not identified. Additional training is provided in an ad hoc, reactive manner.	Employees who require additional training relevant to their job are identified by the MPO, but implementation is sporadic and inconsistent, and completion is not tracked or documented.	The MPO has documented a process to identify employees who require additional training and that training is scheduled and delivered in a timely and consistent fashion.	A Ministry-wide privacy awareness and training program, including any additional or role-based training, exists and is monitored by the MPO.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the demonstration of a strong privacy culture across the Ministry, and/or the requirement that all additional training requires employees to complete assignments to validate their understanding specific to their roles and responsibilities. When privacy incidents or breaches occur, remedial training as well as changes to the training curriculum take into account role-based training, and are made in a timely fashion.
3. Privacy Impact Assessments		#DIV/0!							
3.1	Process for PIAs The MPO has developed and communicated Ministry processes for the completion of PIAs within their Ministry, and these are easily accessible by all employees.				The MPO has not developed an internal process regarding assessing privacy impacts within their Ministry. Privacy impacts are assessed in an ad hoc, reactionary manner.	Privacy impacts are considered during some changes to business processes and/or supporting application systems; however, these processes are not documented, and the procedures are inconsistently applied.	The MPO has developed, maintained, and made available processes regarding the completion of PIAs within their Ministry, and these are easily accessible by all employees.	The MPO monitors and reviews compliance with policies and procedures regarding the completion of, and access to, privacy impact assessments.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of PIA processes within the Ministry. Such information is analyzed and, where necessary, changes are made to improve effectiveness and accessibility.
3.2	Inventory of PIAs The MPO has a current inventory of PIAs completed and in progress, and a process to follow up on outstanding items.				The MPO has not developed an inventory of completed or in-progress PIAs, and there is not a process to follow up on outstanding items.	The MPO has an understanding of which PIAs have been completed by the Ministry and where there are outstanding items; however, tracking is done informally and is not fully documented or complete.	The MPO has developed, maintained and published a PIA inventory to track which PIAs are completed or are in progress. The MPO has established a documented process to follow up on outstanding items.	The MPO monitors and reviews all updates to the PIA inventory, and monitors the completion of outstanding items.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include conducting regular quality reviews and other assessments to determine the effectiveness of the PIA inventory and any formalized follow up processes, and the incorporation of findings into process improvements where necessary.

3.3	Requirement to Complete PIAs There is a process in place to ensure that PIAs are completed prior to the start of any proposed enactment, system, project, program or activity. This process includes the sharing of PIAs with CIRMO and follow up to ensure CIRMO feedback is addressed prior to the PIA being finalized. Once complete, PIAs are sent to CIRMO for retention and entry into the Personal Information Directory (PID).				The MPO has not developed a process to ensure compliance with the requirement to complete PIAs prior to the start of any proposed enactment, system, project, program or activity. There is little to no communication with CIRMO during impact assessments prior to their finalization.	The MPO has not documented a process to ensure compliance with the requirement to complete PIAs prior to the start of any proposed enactment, system, project, program or activity. There is some communication with CIRMO during impact assessments prior to their finalization; however, these processes are not documented, and are inconsistent in practice.	There is a documented process in place to ensure that PIAs are completed prior to the start of any proposed enactment, system, project, program or activity. This process includes sharing PIAs with CIRMO and following up to ensure CIRMO feedback is addressed prior to the PIA being finalized. Once complete, PIAs are sent to CIRMO for retention and to be entered into the Personal Information Directory (PID).	The MPO monitors and reviews compliance with the internal policies and procedures for ensuring the timing of completed PIAs, sharing PIAs with CIRMO and following up with feedback, and sending the PIA to CIRMO within 30 days.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include conducting regular quality reviews and other assessments to assess the effectiveness of internal processes to track PIA completion timing and engagement with CIRMO prior to finalization, and updates to processes to address findings where necessary.
4. Agreements		#DIV/0!							
4.1	Completion and updating of ISAs, RAs, CPAs and IPAs The MPO has a process to identify when ISAs, RAs, CPAs, and IPAs need to be developed and/or updated. This process includes engagement by the MPO as part of the development or updating of the agreement to ensure the agreements are completed as required.				The MPO has not developed a process to identify instances when ISAs, RAs, CPAs and IPAs must be completed or updated. Agreements are not reviewed by the MPO, and any reviews that do occur are ad hoc and reactionary.	The MPO has developed a process to track the completion and update of ISAs, RAs, CPAs and IPAs. Employee awareness of, and adherence to, these processes is sporadic and inconsistent. The MPO is sporadically engaged in the completion of the agreements.	The MPO has documented processes regarding the completion and updating of ISAs, RAs, CPAs and IPAs and these agreements are completed as required. The MPO is consulted during the development or updating of agreements.	The MPO proactively and regularly engages with ministry employees to inform them about when ISAs, RAs, CPAs and IPAs are to be completed, updated and reviewed.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include conducting regular reviews to determine the effectiveness of the process for identifying when the completion, update, or review of ISAs, RAs, CPAs and IPAs is needed and the updating of processes based on the results of such reviews.
4.2	ISAs are reported to CIRMO The MPO has a process in place to ensure ISAs are reported to CIRMO for entry into the Personal Information Directory (PID) once completed.				The MPO has not developed a process to ensure that ISAs are reported to CIRMO once completed. Any reports to CIRMO are done in an ad hoc and reactionary manner, such as in response to specific requests.	The MPO understands that ISAs should be reported to CIRMO for entry into the PID; however, there is no documented process to ensure this occurs.	The MPO has a documented process to ensure that ISAs are reported to CIRMO for entry into the PID as soon as they are completed.	The MPO monitors and reviews the ISA reporting process to ensure process compliance.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include conducting regular quality reviews to determine the effectiveness of the process for ensuring ISAs are reported to CIRMO and updating the process based on the results of such reviews.
4.3	Inventory of all Research Agreements The MPO has a current inventory of all RAs completed and in progress, and a process to follow up on outstanding items.				The MPO has not developed an inventory of RAs that are completed or in progress, and there is no documented process to follow up on outstanding items.	The MPO understands which RAs have been completed and where there are outstanding items; however, tracking processes are informal and not documented.	The MPO has a documented agreement inventory to track which RAs are completed and in progress. The MPO has established a documented process to follow up on outstanding items.	The MPO monitors and reviews updates to the RA inventory, and monitors and documents the completion of outstanding items.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of the RA inventory and any formalized follow up processes. Such information is analyzed and, where necessary, changes are made to improve effectiveness.
4.4	Monitoring compliance with privacy and security requirements in agreements There is a process in place for the ongoing monitoring of compliance with privacy requirements (e.g. section 30 of FOIPPA) outlined in agreements.				There is no process in place for monitoring counterparty compliance with privacy requirements.	The MPO communicates certain privacy requirements to counterparties; however, the requirements are not documented, and there is no formal process to track compliance.	There is a documented process for the ongoing monitoring of counterparty compliance with privacy requirements.	The MPO monitors and reviews the process for monitoring counterparty compliance with privacy requirements. Corrective actions are discussed with counterparties.	Through review of prior agreements, the MPO is kept current on the effectiveness of the monitoring process. Where necessary, changes are made to existing and future agreements in order to improve compliance.
5. Service Provider Management		#DIV/0!							
5.1	Privacy Protection Schedules Privacy Protection Schedules are included for contracts containing personal information, and the MPO is made aware of all such contracts.				The MPO has little or no awareness about which contracts contain personal information and Privacy Protection Schedules are often not included in contracts containing personal information.	The MPO has some understanding about which contracts contain personal information, but there is no documented process for ensuring that the MPO is aware of such contracts. Privacy Protection Schedules are sometimes included in contracts containing personal information, but are incomplete or inconsistently applied.	Privacy Protection Schedules are included for contracts containing personal information, and the MPO is made aware of all such contracts.	The MPO monitors and reviews contracts containing personal information to ensure that Privacy Protection Schedules are included and accurate.	Through assessments and the analysis of lessons learned from prior contracts, the MPO is informed of the effectiveness of including and reviewing Privacy Protection Schedules in contracts containing personal information. Such information is analyzed and, where necessary, changes are made to existing and future contracts.

5.2	Inventory of Access to Personal Information The MPO maintains an up to date inventory of service providers or volunteers with access to personal information within the Ministry's custody and control.				The MPO has not developed an inventory of service providers or volunteers with access to personal information.	The MPO has an understanding of which service providers and volunteers have access to personal information however, tracking processes are informal and not documented.	The MPO maintains an inventory of service providers or volunteers with access to personal information, and the inventory is up to date.	The MPO monitors and reviews updates to the inventory of service providers and volunteers with access to Personal Information, including monitoring any relevant changes to access privileges.	Through regular review of the monitoring process, the MPO is kept current on its effectiveness. Where necessary, changes are made to ensure the inventory is accurate and up-to-date.
5.3	Mandatory Service Provider Privacy Training MPOs must ensure that employees who are service providers or volunteers and who collect, create or access personal information, have completed mandatory privacy training related to the collection, use, disclosure, storage and destruction of personal information. This training must be completed prior to providing services.				Documented tracking of service provider and volunteer training is not conducted.	There is sporadic tracking of service provider or volunteer training and/or there is evidence that some service providers or volunteers have taken mandatory training.	There is a documented process for confirming that service providers who collect, create or access personal information have completed mandatory privacy training prior to providing any service that involves personal information. Personnel who work with an information system or program that involves sensitive or high-risk personal information receive appropriate additional training.	Training for service providers and volunteers is documented, scheduled, timely, consistent and is augmented by regular awareness activities (emails, posters, presentations, etc.).	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the demonstration of a strong privacy culture across the Ministry, that is communicated to all service providers and volunteers and that all training requires service providers and volunteers to complete assignments to validate their understanding prior to providing services. When privacy incidents or breaches occur, remedial training as well as changes to the training curriculum are made in a timely fashion.
5.4	Service provider compliance with privacy requirements There is a process in place for the ongoing monitoring of service provider compliance with privacy requirements(e.g. Section 30 of FOIPPA).				There is a lack of awareness of the need for contractors to comply with privacy requirements as detailed in FOIPPA. There are inadequate mechanisms in place in contracts to ensure contractor compliance with privacy requirements.	There are adequate mechanisms in place in contracts to ensure awareness for contractor compliance to FOIPPA but there are insufficient mechanisms in place to deal with issues of non-compliance.	There is a documented process for the monitoring of service provider compliance with privacy requirements. There are adequate provisions in place to deal with issues of non-compliance.	The MPO monitors service provider compliance with privacy requirements. Corrective actions are discussed with service providers.	Through assessments and the analysis of lessons learned from prior service provider agreements, the MPO is informed of the effectiveness of monitoring service provider compliance with privacy requirements. Such information is analyzed and, where necessary, changes are made to existing and future agreements in order to improve compliance.
6. Personal Information Inventories and Di #DIV/0!									
6.1	Create and Maintain Personal Information Inventory A procedure exists to create and maintain a Personal Information Inventory, and to create it within one year of the Personal Information Inventory Policy being published.				There is no procedure to track personal information at the Ministry through creating and maintaining a Personal Information Inventory.	The MPO has a general understanding of the kinds of personal information under the custody or control of the Ministry; however, there is no documented procedure for creating and maintaining a Personal Information Inventory. The tracking of personal information in the Ministry is informal and not fully documented.	A documented procedure exists to create and maintain a Personal Information Inventory. A Personal Information Inventory is created within one year of the Personal Information Inventory Policy being published.	The MPO monitors and reviews the procedure for the creation and maintenance of the Personal Information Inventory. Any setbacks in inventory creation or gaps in inventory maintenance are remediated.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of the Personal Information Inventory and its maintenance. Such information is analyzed and, where necessary, changes are made to improve accuracy and effectiveness.
6.2	Reporting to CIRMO A procedure exists for the creation and reporting to CIRMO of Personal Information Banks as required.				There is no procedure for the creation and reporting of Personal Information Banks (PIBs) to CIRMO.	Some Personal Information Banks are created within the Ministry, and some PIBs are reported to CIRMO; however, there is no documented procedure for determining how and when a PIB must be created or reported to CIRMO.	A documented procedure exists for the creation and reporting to CIRMO of the Personal Information Banks that result from new enactments, systems, projects, programs or activities of the ministry.	The MPO monitors and reviews the procedure for the creation and reporting of the Personal Information Banks to CIRMO.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of the procedure for the creation and reporting (to CIRMO) of Personal Information Banks. Such information is analyzed and, where necessary, changes are made to improve accuracy and effectiveness.
6.3	Health Information Banks <i>For the Ministry of Health:</i> A procedure exists for the creation and reporting (to CIRMO) of Health Information Banks.				There is no procedure for the creation and reporting of Health Information Banks (HIBs) to CIRMO.	Some Health Information Banks are created within the Ministry and reported to CIRMO; however, there is no documented procedure for determining how and when a HIB must be created or reported to CIRMO.	A documented procedure exists for the creation and reporting of Health Information Banks to CIRMO.	The MPO monitors and reviews the procedure for the creation and reporting of the Health Information Banks to CIRMO.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of the procedure for the creation and reporting (to CIRMO) of Health Information Banks. Such information is analyzed and, where necessary, changes are made to improve accuracy and effectiveness.
6.4	Monitoring of Personal Information Directory (PID) A process is in place to review the PID periodically to ensure all PIAs, ISAs, PIBs and, where applicable, HIBs have been submitted to CIRMO and recorded accurately.				There is no process in place to review the PID to ensure PIAs, ISAs, PIBs, and HIBs have been submitted and recorded accurately.	There is no documented process to ensure the necessary PIAs, ISAs, PIBs, and HIBs have been submitted and recorded, and/or no documented process exists to confirm that PID entries have been submitted and accurately recorded.	There is a documented process in place to review the PID periodically to ensure all PIAs, ISAs, PIBs and, where applicable, HIBs have been submitted and recorded accurately.	The MPO monitors PID reviews and ensures that any issues with the submissions or the accuracy of documentation are remediated.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of PID reviews and any follow up processes. Such information is analyzed and, where necessary, changes are made to improve effectiveness and accuracy.

7. Foreign Demands for Disclosure		#DIV/0!							
7.1	Reporting Foreign Demands A procedure is in place for reporting foreign demands for disclosure to CIRMO.				There is no procedure for reporting foreign demands for disclosure to CIRMO. Any reports to CIRMO are inconsistent and ad hoc.	Foreign demands for disclosure are informally communicated to CIRMO and there is no documented reporting procedure.	A documented procedure in compliance with FOIPPA, is in place for reporting foreign demands for disclosure to CIRMO.	The MPO monitors and reviews the procedure for reporting foreign demands for disclosure to CIRMO.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of reporting foreign demands for disclosure to CIRMO. Such information is analyzed and, where necessary, changes are made to improve timeliness, accuracy and effectiveness.
8. Information Incident Management		#DIV/0!							
8.1	Information Incident Management If an information incident occurred in the past 12 months, the incident was reported immediately, all CIRMO instructions were followed and all recommendations were implemented.				Few or no procedures exist to identify and manage information incidents; those that exist are not documented and are applied inconsistently.	The MPO has a general understanding about the need to track and ensure the immediate reporting of information incidents however, incident management occurs informally and a notable proportion of incidents are not reported immediately or at all. There are no documented processes for incident management or for reinforcing the requirement to immediately report, and CIRMO instructions and recommendations are inconsistently tracked and followed.	The ministry has a documented process for supporting the Information Incident Management process, which includes actions by the MPO and others to ensure that staff are aware of the requirement to immediately report all information incidents and to participate in the response to incidents for which the ministry has responsibility. In addition, as part of the response to incidents, ministry staff follow CIRMO instructions and recommendations are tracked by the MPO and implemented.	A walkthrough of the information incident management plan is performed periodically with the relevant staff and management, and updates to the program are made as needed. The MPO monitors ministry incident reporting and ministry processes, analyzes trends and root causes, and identifies remediation steps required.	The internal and external information environments are monitored and evaluated for issues affecting incident risk and response; changes and improvements to the information incident management plan and related procedures are made where necessary.

Records Management					Maturity Scale				
#	Criteria	Maturity Ranking	Rationale	Variance	Initial (1)	Repeatable (2)	Defined (3)	Managed (4)	Optimized (5)
1. Governance and Accountability		#DIV/0!							
1.1	Records Management Accountabilities The Ministry has articulated employees' responsibilities for records management and business areas have clearly assigned accountabilities to employees with additional role specific records management duties, as appropriate. There is a clear understanding of respective roles and responsibilities and the names of such person(s) or group(s) and their responsibilities are communicated to internal personnel.	<i>The assessed maturity ranking for this criteria</i>	<i>Describe the key factors that resulted in the assessed maturity ranking</i>	<i>Where there is a wide range of IM practices note areas that warrant special attention by identifying leading practices or areas that require attention to basic practices</i>	The Ministry has not articulated responsibility for records management. Records management issues are addressed reactively. Few or no staff members are aware of their individual responsibilities for appropriate records management.	The Ministry has not articulated responsibility for records management and the approaches are often informal and fragmented. There is some, but inconsistent, employee awareness of their individual records management responsibilities and the role of the Government Records Service.	Defined roles and responsibilities have been developed and staff are aware of and understand their records management responsibilities. Staff are aware of and work collaboratively with the Government Records Service.	Management regularly reviews the ministry's records management program and seeks ways to improve the program's performance, including appropriate and adequate resources.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include support being provided by specialist teams and records management duties being devolved to teams and individuals within the ministry. Innovative ideas and continuous improvement are encouraged.
1.2	Ministry-Specific Records Management Policies/Procedures Records management policies and/or procedures have been defined as appropriate for the ministry and any changes to those are communicated to staff.				No Ministry-wide records management policies and/or procedures are in place.	Employees are provided guidance on corporate and ministry specific records management policies and/or procedures but employee awareness remain inconsistent across the Ministry. There may be gaps in the ministry specific policies or procedures that have been developed.	Ministry-specific records management policies and/or procedures have been documented and are communicated to Ministry employees. Changes to such directives are also communicated.	Records management policies and/or procedures are regularly reviewed and updates are communicated shortly after changes are approved. Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include regular communications about the RM program that has led to high visibility and a higher level of awareness for employees or instances where program objectives are being met and new idea generation is common.
2. Education and Awareness		#DIV/0!							
2.1	Mandatory Employee Training Employees have completed mandatory training related to records management (IM117).				A large proportion of Ministry employees have not completed mandatory records management training, and there is no process for monitoring training completion.	Mandatory records management training has been completed by a majority of Ministry employees, but it is sometimes delayed (beyond the required 6 month window) and/or not consistently delivered or monitored.	Employees receive training when they are hired, and refresher training is provided at least every two years. Training is scheduled, timely, consistent and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.)	A ministry-wide records management awareness program exists (beyond basic training requirements) and there is a process for follow up where training or awareness gaps exist. Training is scheduled, timely, consistent and is augmented by regular awareness activities (emails, posters, presentations, etc.). All employees certify annually that they are aware of, and understand, their records management responsibilities.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the development of innovative methods for training and/or training objectives being based on core organizational goals and specific role-based training being developed to service specific needs.
2.2	Role Specific Training Individuals have received additional, role-specific records management training where appropriate.				There is a general understanding of the need for role-based records management training; however, employees who require such training are not identified. Additional training is provided in an ad hoc, reactive manner.	Employees who require additional training relevant to their roles are identified, but training is sporadic and inconsistent, and completion is not tracked or documented.	There is a documented process in place to identify employees who require additional training. All additional training is scheduled and delivered in a timely and consistent manner.	A Ministry-wide records management awareness and training program, including any additional or role-based training, exists and is monitored.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the demonstration of a strong records management culture across the Ministry, and/or the requirement that all additional training requires employees to complete assignments to validate their understanding specific to their roles and responsibilities.
3. Classification		#DIV/0!							
3.1	Record Classification The ministry has procedures in place to classify and/or organize records so that the records can be managed according to the function of the information and the approved retention schedules.				Documented procedures are not in place to classify or organize records and an ad hoc approach is generally taken that does not always align with official and approved retention schedules. Where no schedule exists for certain records no documented procedure exists to help arrange and organize records except an informal business taxonomy.	Procedures for classifying information according to the appropriate retention schedules (or where no schedules exist) have not been developed but some repeatable processes are observed. There is increasing awareness of information classification requirements.	Procedures are documented and cover all required classification and categorization activities, including how to identify, make accessible, and protect information to which no schedule applies. Employees are made aware of the classification requirements and how to meet them including the use of classification tools.	Procedures are in place and implemented to enable compliant classification activities for records. Automated tools are used for managing information where appropriate. Management monitors compliance with information classification requirements.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the configuration and implementation of auto-classification tools to enable classification of content across repositories.
4. Digitization / Documentary Evidence		#DIV/0!							
4.1	4.1 Digital Records The ministry has plans, resources, and technology in place to ensure that all non-exemptive government information will be managed digitally in compliance with the Information Management Act and applicable laws, policies, directives, standards, and specifications.				Digitization has not been identified as a ministry priority; digitization happens in an ad-hoc manner and may not adhere to Government policy, specifications, or directives. Records are regularly created and retained in non-digital form.	Digitization and image management procedures, resources, and technology are available to some areas within the ministry but have not been fully deployed or validated for conformance to the relevant laws, policies, directives, standards and specifications. Some records are created digitally but in an ad hoc manner.	Digitization and image management procedures and technologies have been validated for conformance to the relevant legal and policy requirements, and are scalable and available for use. Records are created digitally, and digitization of existing non-digital records takes place.	Compliance with objectives of the digitization program are monitored and achieve compliance with laws, policies, directives, standards, and specifications. Instances of non-compliance are identified and remediated in a timely manner. New records are created and managed digitally and there are plans for the ongoing transition of remaining non-digital records to fully digital format where required.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include a transition to fully digital processes and/or a mandate to use digital processes over analogue record processes.
5. Retention, Holds and Disposition		#DIV/0!							
5.1	Information Schedule Development and Maintenance The ministry has a process to support and enable the development and implementation of information schedules. The ministry collaborates with GRS to maintain the currency of existing schedules and to develop a procedure to identify records that are not covered by approved schedules.				No process has been established to support and enable the development, implementation, and ongoing maintenance of information schedules.	Processes to support and enable the development, implementation, and ongoing maintenance of information schedules are informal or are not documented. Critical records are not scheduled as a priority.	The ministry has documented its process for supporting the development, implementation, and maintenance of information schedules. The Ministry has adopted and documented a process to identify information not covered by an approved schedule and enable the development of schedules with critical records as a priority.	The ministry's information schedules are regularly reviewed and updated with input from subject matter experts. The ministry regularly monitors the processes and assignments of those responsible for information schedule development and maintenance. Where required, changes and improvements are made in a timely manner.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include committing resources to ensure that information schedules are developed with input from subject matter experts and responsible management so that they are easy to understand, easy to apply to large content sets and are compliant, or efforts to automate and synchronize any changes across systems and repositories.
5.2	Records Retention, Holds and Disposition The ministry has procedures to dispose of, transfer, or archive government information based on official policies, specifications, schedules, guidelines, and procedures published by the Government Records Service. In the case of a legal hold or FOI request, the ministry has processes in place to ensure that such records are not destroyed. Where records are scheduled, retention is limited to the scheduled time period and no longer. Unscheduled records are retained.				Information retention practices across the ministry are inconsistent. Employees retain information based on their own knowledge or interpretation of retention requirements, potentially over-retaining or under-retaining information.	Processes for applying the relevant information schedules to the ministry's information have not been adopted ministry-wide, and do not cover all relevant aspects. Information is held beyond its required retention and is not disposed of as permitted. Employees are generally, but not consistently aware of the importance of suspending disposition.	The ministry has documented and made available its procedures for applying the relevant schedules and retaining information in accordance with those schedules, and no longer. Disposition requests are made in accordance with approved schedules. Where no schedule exists, procedures are in place to ensure that unscheduled records are retained. Procedures for suspending disposition have been documented and communicated to employees. These procedures are followed consistently.	The retention of the ministry's information according to approved information schedules and hold procedures is monitored and periodically assessed for appropriateness. Any discrepancies found are reported and remediated in a timely manner.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This can include automated prompts to track the age of records to ensure no redundant and/or unnecessary retention.
6. Archiving / Preservation / Record Transfers		#DIV/0!							

6.1	Identify and Protect Digital Records Scheduled for Archiving The ministry has documented procedures for identifying, protecting, and maintaining the usability and integrity of digital records scheduled for transfer to archives.				Procedures to identify and protect digital records scheduled for archiving or long term retention are not defined and processes are inconsistent.	Procedures to identify and protect digital records scheduled for archiving or long term retention are not in place, but some informal processes exist.	The ministry has defined and implemented processes and mechanisms to identify any records that are scheduled for archiving or long term retention to protect the usability and integrity of the records.	The ministry has implemented and monitors processes and mechanisms to identify any records that are scheduled for archiving or long term retention to protect the usability and integrity of the records.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the implementation of processes and mechanisms to identify any digital records that are scheduled for archiving or long term retention or systematic monitoring of formats and record repositories to help ensure long term usability.
6.2	Records Transfers to IMA Bodies The ministry has agreements and procedures in place to maintain chain of custody and continuity of control for records during transfers to other bodies covered by the Information Management Act. This includes procedures to monitor such transfers.				Procedures for records transfers to other government bodies are not in place. Limited monitoring of transfers is taking place.	Procedures for records transfers to other government bodies are informal and not documented. Best efforts are made to monitor the transfers but it is not formalized.	Procedures for records transfers to other government bodies and for monitoring of such transfers have been documented and implemented.	Monitoring of all transfers has been implemented, and where issues are encountered they are remediated.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the incorporation of such procedures into existing business processes.
6.3	Records Transfers to Non-IMA Bodies The ministry has documented procedures in place to ensure that records transfers to bodies not covered by the Information Management Act are completed in accordance with an appropriate legal instrument.				Procedures for records transfers outside of government are not in place and such transfers are inconsistent and may not be compliant.	Some procedures for records transfers outside of government are in place, but not consistently followed.	Procedures for records transfers outside of government have been documented. Legal instruments and associated processes have also been defined and implemented where appropriate.	There is a process in place to monitor transfers to non-IMA bodies and any incidents of non-compliance are remediated.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion.
7. Records Maintenance and Storage		#DIV/0!							
7.1	Manage Information in Recordkeeping Systems The ministry manages government information through its lifecycle using recordkeeping system(s) as appropriate. Systems are used to meet records management requirements, including schedules as mandated in the IMA.				Recordkeeping systems are not implemented and/or procedures are not communicated to employees.	The ministry maintains some but not all of the appropriate records in recordkeeping system(s). The overall management of records is not consistent and/or requirements for lifecycle management of those records are not communicated to employees.	The ministry has established procedures and communicated to employees the processes needed to manage information appropriately in recordkeeping system(s). Ministry records are managed throughout their lifecycle and information schedules are applied but disposition may not be consistently performed.	The Ministry monitors the use of its recordkeeping system(s) and, where instances of non-compliance are identified, steps are taken to remediate as appropriate. The use of systems is periodically reviewed for alignment to Ministry government recordkeeping requirements. Lifecycle management using automated scheduling systems of ministry records is configured and operational. Information schedules are consistently applied to content and routine disposition is in force.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include: * mechanisms and strategies to reduce transitory information; * mechanisms and strategies to identify other repositories of ministry content and encourage the capture of government information within recordkeeping systems; * the establishment and consolidation of recordkeeping system(s) to allow uniform lifecycle management to be applied; and/or * the optimization of information schedules to enable easy classification across disparate systems and platforms.
7.2	Manage Physical Records Documented procedures exist regarding the management and storage of physical records in appropriate onsite storage (commensurate with degree of information sensitivity) and/or approved offsite storage facilities.				Record handling practices are inconsistent and Ministry procedures related to physical record storage are not developed and/or not communicated to employees.	Practices for the handling of physical records are consistent but procedures are not documented and/or communicated to employees.	Physical records procedures are documented and records are managed and stored in appropriate onsite storage (commensurate with information sensitivity) and/or approved offsite storage facilities. Physical records are tracked and access is closely monitored and only authorized use is allowed.	The ministry has documented procedures in place for transferring physical records scheduled for semi-active retention or for archiving to approved offsite storage facilities in accordance with the schedule. Physical record management is monitored and instances of non-compliance are remediated.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include regular monitoring of service agreements to ensure quick retrieval, adequate protective measures and regular audits.

Information Access									
#	Criteria	Maturity Ranking	Rationale	Variance	Initial (1)	Repeatable (2)	Maturity Scale		
1. Accountability		#DIV/0!					Defined (3)	Managed (4)	Optimized (5)
1.1	Information Access Procedures and the Duty to Assist Information Access and Duty to Assist procedures have been clearly defined and have been communicated to all staff. Ministry staff are informed and aware of the appropriate response to FOI requests (e.g., how to conduct a comprehensive and timely search for responsive records, seeking clarification, and execute these steps in accordance to defined procedures).	<i>The assessed maturity ranking for this criteria</i>	<i>Describe the key factors that resulted in the assessed maturity ranking</i>	<i>Where there is a wide range of IM practices note areas that warrant special attention by identifying leading practices or areas that require attention to basic practices</i>	There are no processes or procedures in place for staff to follow when responding to FOI requests, staff are unaware of their obligations under FOIPPA, and do not respond to FOI requests as required.	Staff responses to FOI requests are ad hoc and inconsistent. There are no documented processes or procedures for staff to follow, and staff knowledge regarding their obligations under FOIPPA is inconsistent.	There are established processes and procedures in place for staff to follow in responding adequately and in a timely fashion to FOI requests. Staff are aware of their obligations under FOIPPA to conduct adequate searches for responsive records and consistently do so in a timely fashion.	The Ministry consistently responds in a timely fashion to FOI requests, adheres to the principles of sound information access management and maintains clear and ongoing communications with its executive on the status of each request. Information access procedures are reviewed at least annually (or upon significant changes to policy or regulatory requirements) and updated as required. Compliance with procedures is regularly monitored and reported to senior leadership.	Level 4 has been obtained and the Ministry strives for continuous improvement in providing comprehensive and timely responses.
1.2	Information Access Accountability Accountabilities for FOI requests are assigned, and roles and responsibilities are clearly defined.				Accountabilities for FOI requests have not been defined or assigned. Resources are assigned reactively as requests are received.	Accountabilities have not been defined, but there is informal recognition of individual responsibility for FOI requests and related processes. The same individuals are commonly involved in these processes but there is no documented description of their responsibilities.	Responsibilities for FOI requests have been defined and are also included in job descriptions for all aspects of the FOI process, at all levels in the organization.	FOI accountabilities are reviewed at least annually and updated as required.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion.
2. Education and Awareness		#DIV/0!							
2.1	Employee Training Employees have completed mandatory (IM117) training related to FOI/ Information Access.				A large proportion of Ministry employees have not completed mandatory privacy training, and there is no process for monitoring training completion.	Mandatory training for access has been completed by a majority of Ministry employees, but it is sometimes delayed (beyond the required 6 month window) and/or not consistently delivered or monitored.	Employees receive training when they are hired, and refresher training is provided at least every two years. Training is scheduled, timely, consistent and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.)	A Ministry-wide privacy awareness and training program exists and is monitored by the MPO. Training activities are monitored, regularly scheduled to provide timely and consistent privacy awareness (e.g., emails, posters, presentations, etc.) All Employees certify that they are aware of, and understand, their responsibilities under FOIPPA regarding the sharing and protection of personal information in their care.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion.
2.2	Role Specific Training Individuals have received additional, role-specific FOI/Information Access training where appropriate (e.g. ministerial staff, FOI co-ordinators).				There is a general understanding of the need for role-based FOI training; however, employees who require such training are not identified. Additional training is provided in an ad hoc, reactive manner.	Employees who require additional training relevant to their job are identified, but implementation is sporadic and inconsistent, and completion is not tracked or documented.	There is a documented process in place to identify employees who require additional training. All additional training is scheduled and delivered in a timely and consistent fashion.	A Ministry-wide records management awareness and training program, including any additional or role-based training, exists and is monitored.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the requirement that all additional training requires employees to complete assignments to validate their understanding specific to their roles and responsibilities.
3. Minister's Offices & Ministerial Staff		#DIV/0!							
3.1	Dedicated Public Servant A dedicated Public Servant is designated as the person in charge of all requests involving a Minister's office. This person is accountable for contacting all staff directly, in writing, with the details of the request and directing that staff search for responsive records and respond within a set time period. This individual must also retain a current list of all Ministerial staff that is shared on an ongoing basis with IAO.				A public servant has not been designated as the person in charge of all requests involving a Minister's office.	Accountability has not been assigned to a dedicated Public Servant for these processes, but this role is informally in place and supports FOI requests as they are received.	A dedicated Public Servant has been assigned this role. Responsibilities are formally defined and are also included in this person's job description. This individual retains a current list of all Ministerial staff that is shared on an ongoing basis with IAO.	Accountabilities are reviewed at least annually (or when there are significant changes to policy or regulatory requirements) and updated as required.	FOI request performance is tied to personal performance ratings and continual improvement is supported.
4. Monitoring		#DIV/0!							
4.1	Monitoring of FOI Requests A documented process is in place to track and monitor all active FOI requests. This includes regular reporting to Ministry leadership and escalation processes to ensure compliance with timeliness and/or "duty to assist" requirements.				No documented monitoring or reporting of FOI requests takes place within the Ministry. No escalation processes or triggers exist to assess the risk of non-compliance with timeliness and duty to assist requirements.	FOI requests are informally monitored by those managing the process but this information is not reported or acted upon. Some escalation processes exist but are used in an ad hoc fashion.	There is a documented process for the monitoring of compliance with FOI/access requirements. There is an escalation process if there is a risk of non-compliance with timeliness and/or "duty to assist".	There is regular monitoring of, and reporting on FOI requests to Ministry leadership. The process ensures that issues are identified and addressed proactively to support completion of requests within the allotted timeframe.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion.
4.2	Monitoring Service Provider Compliance with FOI Requests There is a process in place for the monitoring of service provider compliance with ministry requirements related to FOI requests.				There is no process in place for monitoring service provider compliance with ministry requirements for FOI requests.	The Ministry communicates FOI request compliance requirements to service providers but the requirements are not documented, and there is no process to track compliance.	There is a documented process for the monitoring of service provider compliance with FOI requests and there is an escalation process to mitigate risks of non-compliance with timeliness or "duty to assist" requirements.	The MPO monitors and reviews service provider compliance with processes related to FOI. Corrective actions are addressed with service providers and remediated. Such information is analyzed and, where necessary, changes are made to existing and future agreements in order to improve compliance.	

Information Protection						Maturity Scale			
#	Criteria	Maturity Ranking	Rationale	Variance	Initial (1)	Repeatable (2)	Defined (3)	Managed (4)	Optimized (5)
1. Information Protection		The assessed maturity ranking for this criteria							
1.1	Security Program An Information Security Program has been developed, documented, approved, and implemented based on the Information Security Policy (ISP) developed by the Office of the Government Chief Information Officer (OCIO) and Corporate Information and Records Management Office (CIRMO) with respect to security of personal information. Responsibilities for the Information Security Program are documented and assigned.		<i>Describe the key factors that resulted in the assessed maturity ranking</i>	<i>Where there is a wide range of IM practices note areas that warrant special attention by identifying leading practices or areas that require attention to basic practices</i>	No documented security policy or procedures exist and formal accountability for security has not been assigned. Security is managed in an ad-hoc manner.	Security policies or procedures do not exist, but some security processes are in place and operating. Processes may be inconsistent and accountability has not been formally defined.	A security program (aligned with ISP) has been documented in the form of policies and procedures. Formal accountability has been assigned for information security.	The security program is regularly reviewed and updated. Security performance is monitored and reported to Ministry leadership on a regular basis.	Level 4 has been attained and additional measures are in place related to the security program. This could include regular benchmarking of security program performance, or adoption of other leading practices.
1.2	Employee Training Employees have completed training related to the protection of government information (IM117 and IM118).				A large proportion of Ministry employees have not completed mandatory privacy training, and there is no process for monitoring training completion.	Mandatory training has been completed by a majority of Ministry employees, but it is sometimes delayed and/or not consistently delivered or monitored.	Employees receive training when they are hired, and refresher training is provided at least every two years. Training is scheduled, timely, consistent and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.)	A Ministry-wide privacy and security awareness and training program exists and is monitored by the MPO and the MISQ. Training activities are monitored, regularly scheduled to provide timely and consistent privacy awareness (e.g., emails, posters, presentations, etc.). All Employees certify annually that they are aware of, and understand, their responsibilities under FOIPPA regarding the sharing and protection of personal information in their care.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to training and awareness. This could include advanced training methodologies (gamification, etc.), coordination of training program development with the OCIO and other Ministries, regular testing of employee knowledge, etc.
1.3	Role Based Training A process is in place to develop and deliver additional training (beyond IM117 and IM118) on Information Protection to employees				There is a general understanding of the need for role-based information protection training; however, employees who require such training are not identified. Additional training is provided in an ad hoc, reactive manner.	Employees who require additional training relevant to their job are identified, but implementation is sporadic and inconsistent, and completion is not tracked or documented.	There is a documented process in place to identify employees who require additional training. Additional training is scheduled and delivered in a timely and consistent fashion.	A Ministry-wide information protection awareness and training program, including any additional or role-based training, exists and is monitored.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the requirement that all additional training requires employees to complete assignments to validate their understanding specific to their roles and responsibilities.
1.4	External Parties Assessment of risks from external party access to government information, information systems or information processing facilities are performed and appropriate security controls implemented prior to granting access.				No process exists for assessing risks associated with access by third parties, and risk assessments are not conducted.	No process exists for risk assessments, but risk assessments are conducted in some cases. Where conducted, these assessments result in the identification and implementation of appropriate mitigating controls.	A documented risk assessment process exists and is communicated to Ministry staff. Reviews are conducted for all external party access.	Risks associated with third-party access are monitored and reported on regularly. Controls are updated to reflect changes to risks on an ongoing basis.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to risk management and external access.
1.5	Asset Management An inventory of information assets and systems exists and is maintained. Ownership of assets is assigned and accountabilities associated with ownership are defined.				No inventory of information assets or systems exists and no ownership has been assigned or is in place.	A basic inventory exists, but there is no documented process for information asset management. Some ownership exists for assets and systems wherein functions related to the protection and management of these assets are fulfilled.	An asset management process is in place and a formal inventory of information assets and systems is maintained. Accountabilities for ownership are clearly defined and implemented.	An inventory of information assets and systems is maintained and actively monitored, and the inventory is updated periodically. Ownership of assets is regularly reviewed and accountabilities are monitored.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to asset management. This could include incorporating ownership accountabilities and performance into personal performance ratings.
1.6	Employee Accountabilities Information protection roles and accountabilities for employees are documented, and employees acknowledge their responsibilities for the protection of personal and sensitive information prior to employment and periodically.				No accountabilities related to security or information protection are documented.	Accountabilities are not documented; however, there is a demonstrated awareness of fundamental security responsibilities. There is no formal acknowledgement or attestation process in place.	Accountabilities for security and information protection are documented and/or included in job descriptions. Ministry staff are required to sign off periodically (i.e., annually) to acknowledge their accountabilities with respect to security and information protection.	Accountabilities for security are defined and regularly updated to reflect changes in Ministry programs and/or compliance requirements. Performance is monitored and reported regularly and there is a process to verify that all staff complete their periodic sign-off.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to human resources security. This could include incorporating security and information protection accountabilities in annual employee performance ratings.
1.7	Physical and Environmental Protection Equipment containing personal or sensitive information must be protected throughout its lifecycle, including secure disposal, to reduce the risks from unauthorized access or loss.				No physical/environmental protection program is documented.	Physical/environmental controls are not documented, but some practices are informally conducted.	Controls are documented regarding equipment protection, including asset disposal.	Controls related to physical/environmental protection are documented and monitored for effectiveness. They are reviewed and updated on a regular basis.	Level 4 has been attained and the Ministry has demonstrated additional leading practiced related to equipment protection.
1.8	Protection Against Malicious Code There an established process in place to prevent, detect, and resolve malicious code infections on information systems and infrastructure.				No process is in place to prevent, detect and/or resolve malicious code.	No processes related to malicious code are defined, but some informal practices are in place.	Processes related to malicious code are defined and implemented.	Controls related to malicious code are regularly monitored and updated to reflect changes in risk, Ministry operations or compliance requirements. Incidents related to malicious code are reported and followed up on.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to malicious code management. This could include actively monitoring and acting on threat intelligence.
1.9	Security Classification Records are organized so that security classifications can be applied to protect different classes of information based on their sensitivity.				No process is in place for security classification, and classification is not practiced.	No documented process is in place for security classification; however, information is protected based on sensitivity in some cases and/or classification has been accomplished for some data repositories or information systems.	Information security classification processes are formalized and information assets and systems are classified according to the OCIO data security classification standard (or similar). Assets are managed according to their security classification.	Data security classification processes and ratings are regularly reviewed and updated.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to security classification.
1.10	Portable Media A formal inventory of portable media devices is maintained. Where devices are used, they comply with OCIO standards, are encrypted, and are managed with controls appropriate for the sensitivity of the data contained on the media, including logging/tracking and secure storage, transfer and disposal.				No inventory of portable media is maintained. No assessment of compliance of portable media to applicable standards is conducted.	An inventory of portable media is not maintained, but efforts are made informally to minimize and control the use of portable media. In certain cases, the use of portable media is logged/tracked with secure storage, transfer and disposal, but this is not formalized or consistently applied.	An inventory of portable media is in place, an approval process for the use of portable media exists, and the use of portable media is tracked/logged. Appropriate steps are taken to ensure that portable media devices in use comply with applicable OCIO standards and devices are managed with controls appropriate for the sensitivity of the data they contain.	The inventory and tracking/logging of portable media devices is actively maintained and reviewed.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to portable media management. This could include providing more secure mechanisms for data transfer to eliminate the need for portable media.
1.11	User Access and Responsibilities - Users must only access information permitted by their assigned roles and responsibilities -Users must ensure unattended equipment has appropriate protection. -Users must ensure the safety of sensitive information from unauthorized access, loss or damage.				Documented processes for user access, system privileges and review of access privileges are not in place. User awareness of their responsibilities is sporadic and they may be unaware of their responsibilities for maintaining a clean desk and protecting equipment and information while not at their workstations.	There are no documented processes in place, but repeatable practices for access and protection of unattended equipment and information are observed.	Documented processes are in place for user responsibilities and access. Staff is aware of and adheres to the clean desk policy and the need to protect unattended equipment and access to government information.	User responsibilities are up to date and monitored. Access and user controls are kept up to date and are regularly monitored for accuracy and currency.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to access control and user responsibilities.
1.12	Access Control Logical access to personal information is restricted by procedures that address the following matters: - Authorizing and registering internal personnel and individuals - Identifying and authenticating internal personnel and individuals - Access privilege change requests and permissions - Granting system access privileges and permissions - The access rights to information systems must be removed upon termination or change of employment/position of staff. Access rights should be reviewed and monitored at regular intervals, depending on the sensitivity of the information.				Access control processes are not in place and no repeatable processes are observed.	Documented processes are not in place, but repeatable access control practices are observed.	Documented access control processes are in place covering the full range of access management (granting, reviewing, removing, changing, etc.) and they apply to both employees and contractors.	Access controls are regularly monitored, reported on and updated on a regular basis.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to access control. This could include the assessment of instances of inappropriate access attempts to determine root causes and potential exposures and the development of remedial action plans.
1.13	Security requirements for information systems Security controls are identified as part of the business requirements for new information systems or enhancements to existing information systems through the information security risk assessment (the former STRA) process, and controls are implemented and reviewed prior to implementation.				No formal information security risk assessment (ISRA) process exists or is followed. ISRAs are not conducted for all new systems or enhancements to existing systems.	A formal ISRA process does not exist within the Ministry, but ISRAs are conducted on a majority of new systems or system enhancements.	A formal ISRA process is in place in the Ministry. ISRAs are completed for all new systems and system enhancements. Accountabilities for ISRAs are clearly defined.	An inventory of ISRAs (complete and ongoing) is maintained and regularly reviewed. Outstanding items are tracked and monitored to confirm completion.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to security requirements for information systems. This could include taking a "privacy by design" and/or a "security by design" approach that looks to formalize all relevant compliance requirements during the design phase and includes formal testing of security controls prior to, and after, go-live.
1.14	Technical Vulnerability Management - A Vulnerability and Risk Management (VRM) Program has been developed, documented, approved, and implemented by the Office of the Government Chief Information Officer (OCIO). Ministries should identify the criticality of information systems and regularly assess and evaluate information security vulnerabilities, potential risks evaluated, and vulnerabilities mitigated or remediated.				Vulnerability assessments have not been conducted and are not planned.	Vulnerability assessments are conducted in an inconsistent manner. Risks arising from vulnerability assessments are remediated.	Vulnerability assessments are planned and conducted on a regular basis (based on risk). Vulnerabilities are risk ranked and remediated in priority order.	Remediation activities are planned, tracked and verified, and escalation takes place in cases where remediation is not completed.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to vulnerability management. This could include active monitoring of relevant threat intelligence to inform the Ministry's vulnerability management approach and priorities.
1.15	Logging and Monitoring Audit logs recording user and privileged user activities, exceptions, and information security events are kept and protected for an appropriate period of time to assist in monitoring and future investigations. Logs are monitored and the result of the monitoring activities are regularly reviewed and acted upon as necessary.				No audit logs are retained for key systems. No monitoring of access or exceptions is possible.	No logging or monitoring program is in place. Logging is enabled on some key systems. Logs are not monitored, but can be accessed for retrospective review.	Logging is enabled on key systems (based on risk and security classification). Logs are maintained and controls are in place to limit access to these logs. Manual monitoring or basic automated monitoring is in place for critical/high-risk systems.	Log monitoring and correlation capabilities are in place and exceptions are reviewed and acted upon as necessary. Results of monitoring activities are reported and are used to enhance access and security controls on an ongoing basis.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to logging and monitoring. This could include advanced monitoring analytics and/or the use of threat intelligence to regularly update the configuration of monitoring tools.

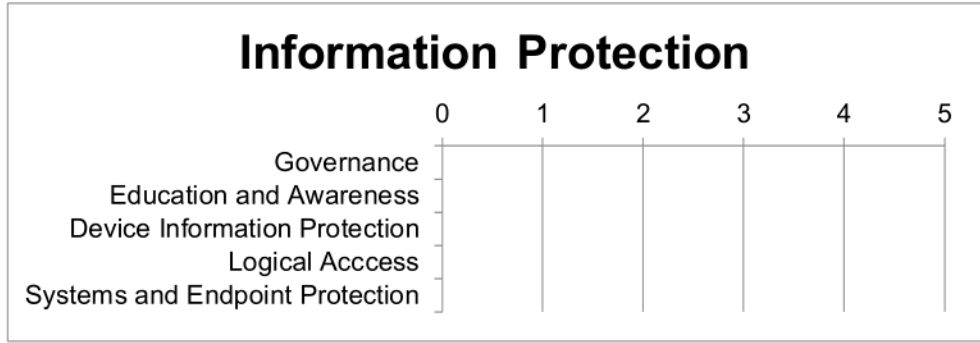
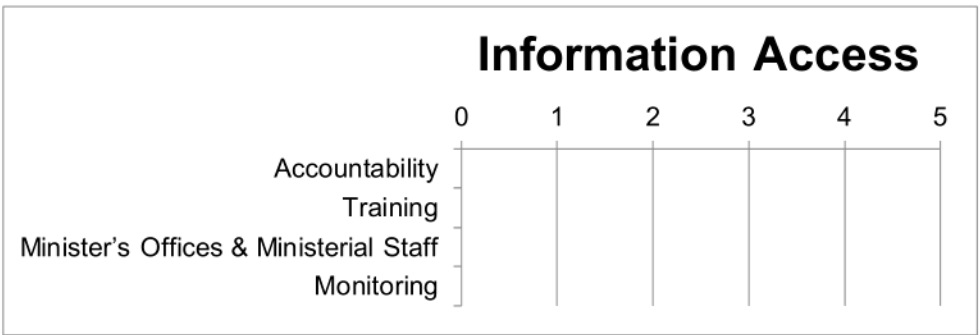
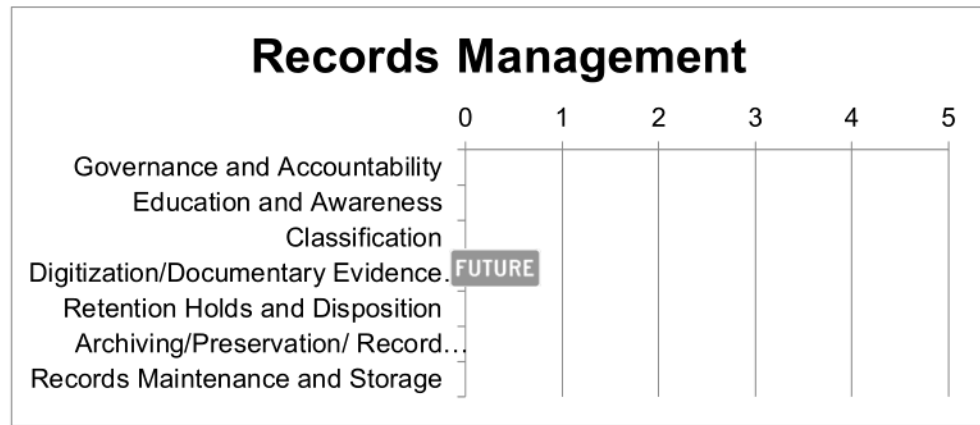
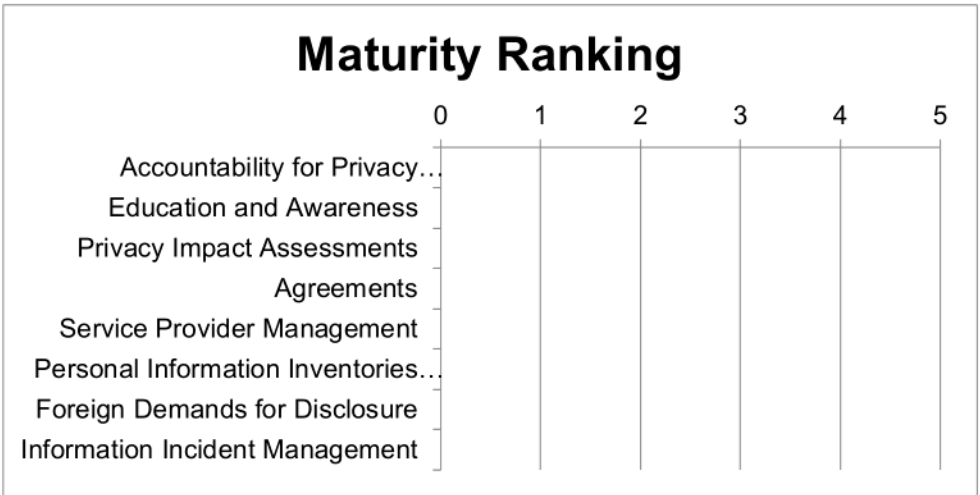
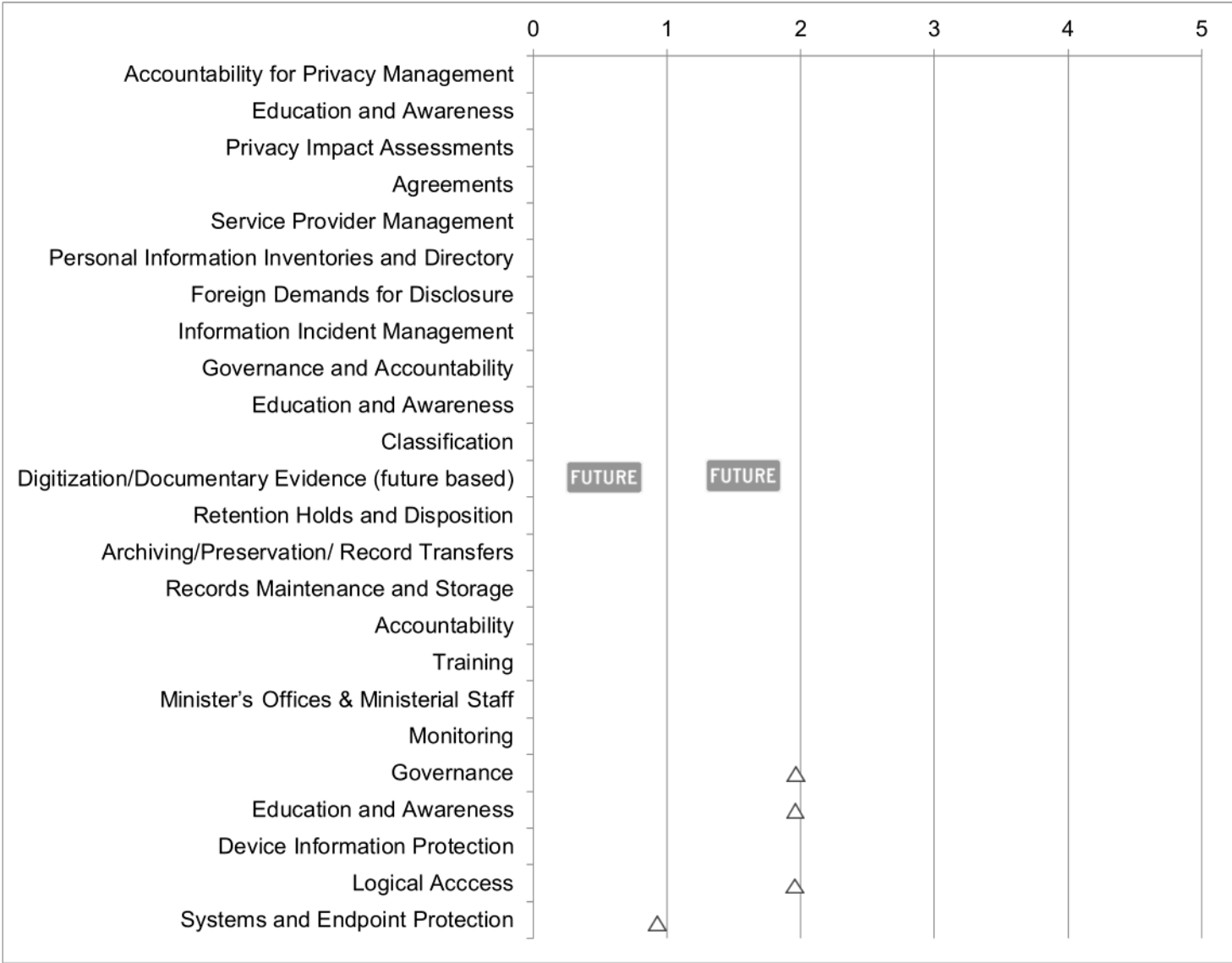
1.16	Business Continuity Management Business continuity management processes and plans have been developed tested, maintained, updated and they include provisions to maintain security and information protection in the case of an incident.				No business continuity plan has been defined.	No business continuity plan has been defined, but recovery procedures have been defined for some key systems. Security is not addressed formally in these procedures.	A documented business continuity plan exists. The plan includes an assessment of risk and information sensitivity and incorporates appropriate controls to address information protection.	The business continuity plan is regularly reviewed and exercises are conducted on a periodic basis to test and improve the plan.	Level 4 has been attained and the Ministry has demonstrated additional leading practices related to business continuity management. This could include regular independent or external reviews of the business continuity plan and involvement of related third parties in exercises and tests.
1.17	Monitoring Service Provider Compliance with Information Protection requirements The Ministry has a process to monitor service provider compliance for information protection requirements				There is a lack of awareness of the need for contractors to comply with government information protection requirements. There are inadequate mechanisms in place in contracts to ensure contractor compliance with information protection requirements	There are adequate provisions in contracts to reinforce compliance with information protection requirements. Contractors are aware of their obligations, but there are insufficient mechanisms in place to deal with issues of non-compliance.	There is a documented process for the monitoring of service provider compliance with information protection requirements. There are adequate provisions in place to deal with issues of non-compliance.	The ministry monitors service provider compliance with information protection requirements. Corrective actions are addressed with service providers and remediated.	Through assessments and the analysis of lessons learned from prior service provider agreements, the ministry is informed of the effectiveness of monitoring service provider compliance with information protection requirements. Such information is analyzed and, where necessary, changes are made to existing and future agreements in order to improve compliance.

This TABLE is a duplicate of the TABLE in **Appendix 1. Summary of Framework Ratings** of the Self Assessment IMPR Report. After completing the Review and entering the results into the other tabs of the Spreadsheet please **COPY** this **TABLE** and **PASTE** it over the TABLE in **Appendix 1. Summary of Framework Ratings of the Self Assessment IMPR Report**

The Maturity Rankings (Score) are linked to the Domains and will update automatically.

Information Management Domains	Criteria	Score
Privacy	(# not scored)	(Average for each heading)
Accountability for Privacy Management	1.1 1.2 1.4 1.3#	#DIV/0!
Education and Awareness	2.1 2.2	#DIV/0!
Privacy Impact Assessments	3.1 3.2 3.3	#DIV/0!
Agreements	4.1 4.2 4.3 4.4	#DIV/0!
Service Provider Management	5.1 5.2 5.3 5.4	#DIV/0!
Personal Information Inventories and Directory	6.2 6.3 6.4 6.1#	#DIV/0!
Foreign Demands for Disclosure	7.1	#DIV/0!
Information Incident Management	8.1	#DIV/0!
Records Management		
Governance and Accountability	1.1 1.2	#DIV/0!
Education and Awareness	2.1 2.2	#DIV/0!
Classification	3.1	#DIV/0!
Digitization/Documentary Evidence	4.1 #	#DIV/0!
Retention Holds and Disposition	5.1 5.2	#DIV/0!
Archiving/Preservation/Record Transfers	6.2 6.3 6.1#	#DIV/0!
Records Maintenance and Storage	7.1 7.2 7.3	#DIV/0!
Information Access		
Accountability	1.1 1.2	#DIV/0!
Training	2.1 2.2	#DIV/0!
Minister’s Offices & Ministerial Staff	3.1	#DIV/0!
Monitoring	4.1 4.2	#DIV/0!
Information Protection		
Security Program	1.1	0
Employee Training	1.2	0
Role Based Training	1.3	0
External Parties	1.4	0
Asset Management	1.5	0
Employee Accountabilities	1.6	0
Physical and Environment Protection	1.7	0
Protection Against Malicious Code	1.8	0
Security Classification	1.9	0
Portable Media	1.1	0
User Access and Responsibilities	1.11	0
Access Control	1.12	0
Security Requirements for Information Systems	1.13	0
Technical Vulnerability Management	1.14	0
Logging and Monitoring	1.15	0
Business Continuity Management	1.16	0
Monitoring Service Provider Compliance with Information Protection Requirements	1.17	0

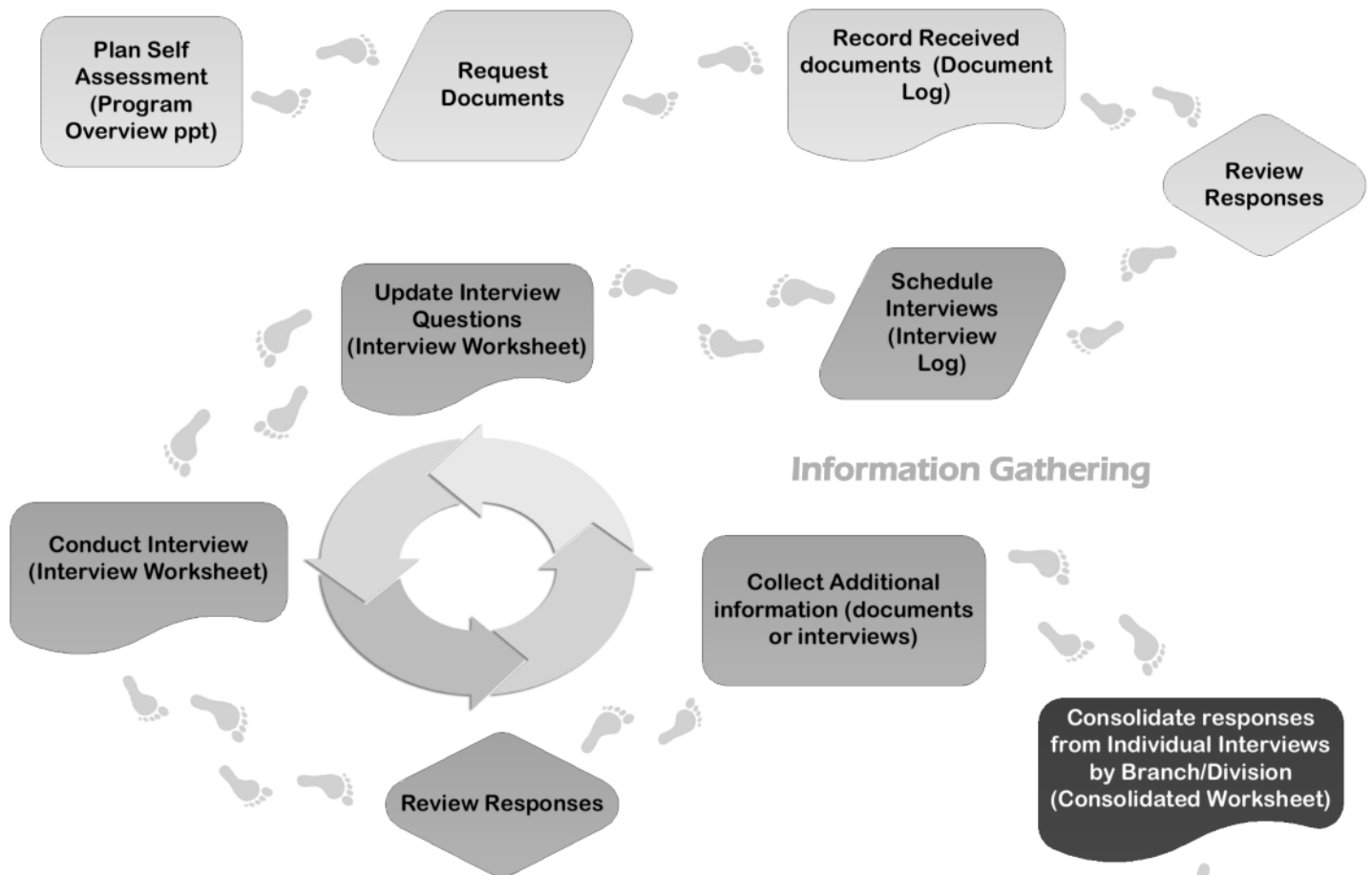
Headings	Maturity Ranking	
Accountability for Privacy Management	#DIV/0!	
Education and Awareness	#DIV/0!	
Privacy Impact Assessments	#DIV/0!	
Agreements	#DIV/0!	
Service Provider Management	#DIV/0!	
Personal Information Inventories and Directory	#DIV/0!	
Foreign Demands for Disclosure	#DIV/0!	
Information Incident Management	#DIV/0!	
Governance and Accountability	#DIV/0!	
Education and Awareness	#DIV/0!	
Classification	#DIV/0!	
Digitization/Documentary Evidence (future based)	#DIV/0!	
Retention Holds and Disposition	#DIV/0!	
Archiving/Preservation/ Record Transfers	#DIV/0!	
Records Maintenance and Storage	#DIV/0!	
Accountability	#DIV/0!	
Training	#DIV/0!	
Minister's Offices & Ministerial Staff	#DIV/0!	
Monitoring	#DIV/0!	
Governance	0	
Education and Awareness	0	
Device Information Protection	0	
Logical Access	0	
Systems and Endpoint Protection	0	
Governance	0	Warning
Security Program	0	
Employee Accountabilities	0	
Security Classification	0	
Monitoring Service Provider Compliance with Information Protection Requirements	0	
Logging and Monitoring	0	
Business Continuity Management	0	
Education and Awareness	0	Warning
Employee Training	0	
Role Based Training	0	
Device Information Protection	0	Warning
Asset Management	0	
Physical and Environment Protection	0	
Portable Media	0	
Logical Access	0	Warning
User Access and Responsibilities	0	
Access Control	0	
External Parties	0	
Systems and Endpoint Protection	0	Warning
Protection Against Malicious Code	0	
Security Requirements for Information Systems	0	
Technical Vulnerability Management	0	



Self-Assessment Walkthrough

IM Practice Review

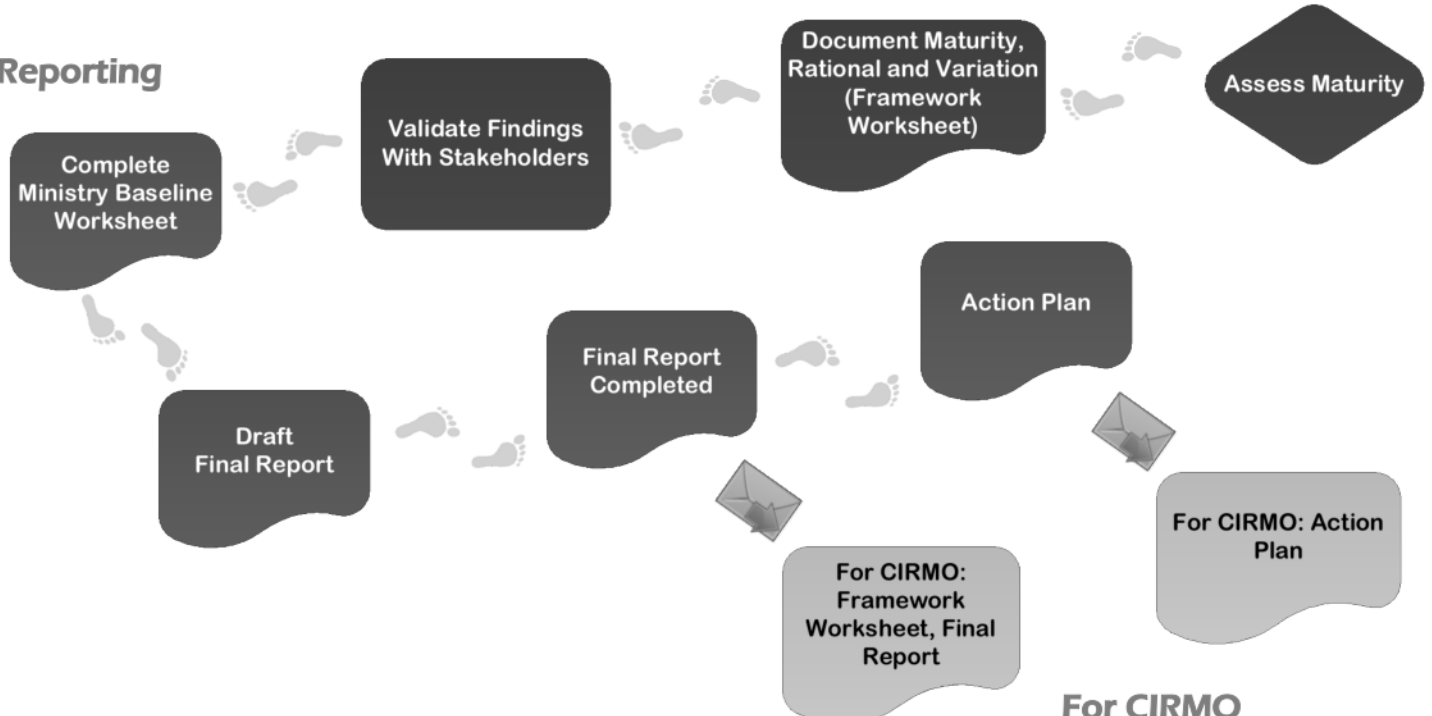
Scoping and Planning



Information Gathering

Analysis and Validation

Reporting

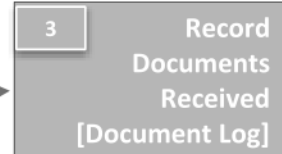
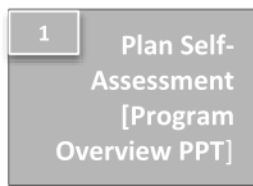


For CIRMO

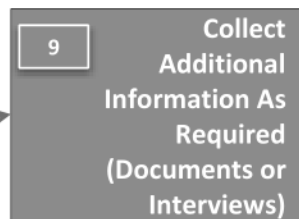
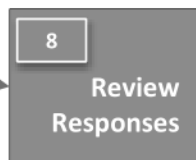
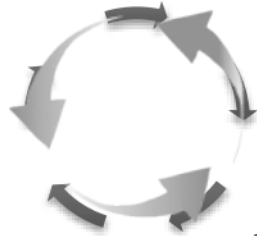
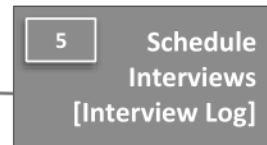
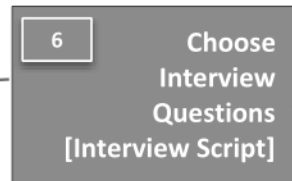
Information Management Practice Review Program

Self-Assessment Walkthrough

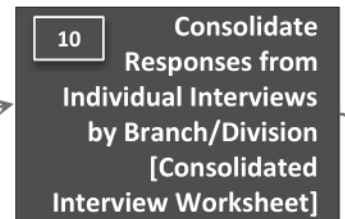
Scoping and Planning



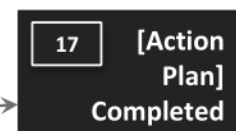
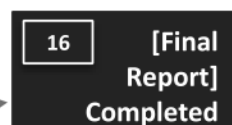
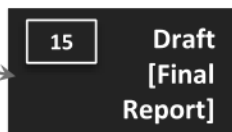
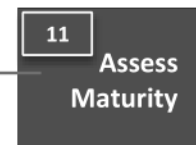
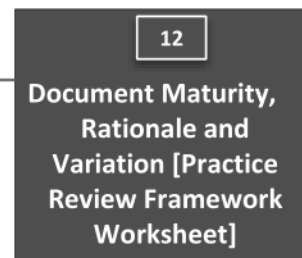
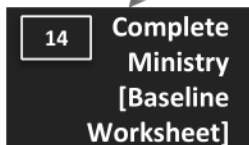
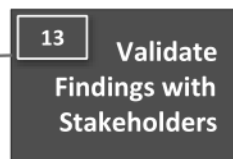
Information Gathering



Analysis and Validation



Reporting



Submit to CIRMO:
[Framework Worksheet] and
[Final Report]

Submit to CIRMO:
[Action Plan]

Page 114 of 142 to/à Page 120 of 142

Withheld pursuant to/removed as

s.13

CIRMO

Staff Name:	
Auditors:	
Date:	
Notes reviewed by:	

Criteria	Questions	Response
Privacy		
1.1 Designated Ministry Privacy Officer The Deputy Minister has named a Ministry Privacy Officer and roles and responsibilities related to privacy in the ministry have been clearly defined.	Do you know who your MPO is?	
1.2 Deputy Delegation of Duties If the Deputy Minister has delegated any duties, powers or functions, a formal delegation instrument is in place and all such current delegation instruments are maintained and communicated to the CIRMO.	Has your area been formally delegated any duties, powers or functions of the DM in relation to FOI/privacy? How do you deal with privacy issues as they arise?	
1.4 Privacy Policies Ministry-specific privacy policies, building upon PMAP but incorporating Ministry-specific privacy requirements, have been developed and deployed, where appropriate.	Do you feel that your branch deals with programs, processes, environments or systems that have significant amounts of personal information? Can you describe the sensitivity and types of PI that are regularly handled? Do you have any branch specific privacy policies or procedures in place for how staff should handle the	

	<p>info they deal with?</p> <p>How are those policies/procedures updated and communicated to staff?</p>	
<p>2.1 Employee Training Employees have completed mandatory training related to privacy (IM117 or equivalent). Individuals have received additional, role-specific privacy training where appropriate (e.g. MPOs, employees who handle sensitive personal information, and employees with access to information systems containing personal information such as ICM or Pharmanet).</p>	<p>What training do staff in your area receive related to privacy? Have you also completed this training and/or do you have additional training?</p> <p>Do employees certify that they are aware of, and understand, their responsibilities under FOIPPA regarding the sharing and protection of personal information in their care? How do they do this? How often do they attest to the understanding of their responsibilities (e.g., annually)</p> <p>Are you aware of any other privacy programs/awareness activities promoted in CIRMO that we haven't covered yet?</p>	
<p>2.2 Role Based Privacy Training A process is in place to develop and deliver additional privacy training (beyond IM117 or equivalent) to employees whose duties require: - Access to information systems containing personal information - Working with sensitive personal information - Supporting PIAs or ISAs</p> <p>As appropriate, role-specific privacy training may address topics such as: PIAs, ISAs, Foreign Demands for Disclosure and appropriate collection, use and disclosure.</p>	<p>Do staff in your area receive role specific privacy training? Who provides the training?</p> <p>How do you identify people that need additional training?</p> <p>Do you coordinate the training with the MPO?</p> <p>Do staff receive periodic updates on their training?</p>	

<p>3.1 Process for PIAs</p> <p>The MPO has developed and maintains internal processes regarding the completion of PIAs within their Ministry, and these are easily accessible by all employees.</p>	<p>If you had to do a PIA how would you go about it?</p> <p>What is the role of the MPO in the PIA process?</p> <p>s. 13</p>	
<p>3.2 Inventory of PIAs</p> <p>The MPO has a current inventory of all PIAs completed and in progress, and a process to follow up on outstanding items.</p>	<p>N/A</p>	
<p>3.3 Requirement to Complete PIAs</p> <p>There is a process in place to ensure that PIAs are completed prior to the start of any proposed enactment, system, project, program or activity. This process includes the sharing of PIAs with the CIRMO and follow up to ensure all CIRMO feedback is addressed prior to the PIA being finalized. Further, once complete, all PIAs are sent to the CIRMO for</p>	<p>Do you know when and in what circumstances PIAs are to be completed?</p> <p>What is your process for ensuring feedback is incorporated into the PIA?</p> <p>Is there a documented process for what to do with the PIA once completed?</p>	

retention and to be entered into the Personal Information Directory (PID).		
4.1 Completion and updating of ISAs, RAs, CPAs and IPAs The ministry has a process to identify when ISAs, RAs, CPAs, and IPAs need to be developed and/or updated. This process includes engagement by the MPO as part of the development or updating of the agreement.	Do you ever need to complete a ISA, RA, IPA and/or CPA in your area? Is there a documented process for the ISA, RA, IPA processes? What role does the MPO have in these processes?	
4.2 ISAs are reported to the CIRMO The MPO has a process in place to ensure all ISAs are reported to the CIRMO for entry into the Personal Information Directory (PID) once completed.	N/A	
4.3 Inventory of all Research Agreements The MPO has a current inventory of all RAs completed and in progress, and a process to follow up on outstanding items.	N/A	
4.4 How do you communicate privacy requirements (what types) to counterparties? Monitoring compliance with privacy and security requirements in agreements There is a process in place for the ongoing monitoring of compliance with privacy/security requirements (e.g. section 30 of FOIPPA) outlined in agreements.	See 4.1 also How do you confirm that privacy requirements in those agreements are met?	

<p>5.1 Privacy Protection Schedules (see 5.4 also) Privacy Protection Schedules are included for contracts containing personal information, and the MPO is made aware of all such contracts.</p>	<p>Do you ever need to develop contracts with other parties e.g., other levels of government, or agencies?</p> <p>Is there a policy, procedure or checklist documenting what the privacy requirements are for agreements</p> <p>What is the role of the MPO in regards to contracts developed for work in your area? E.g., are they informed about the contract, do they review it.</p> <p>Is there a process in place to monitor and ensure that privacy requirements in those agreements are met?</p>	
<p>5.2 Inventory of Access to PI The MPO maintains an up-to-date inventory of all service providers or volunteers with access to personal information within the Ministry's custody and control.</p>	<p>When you onboard staff/volunteers/service providers, does the MPO have a list of staff with access to PI in your area?</p> <p>Do you have a list of staff/volunteers/service providers and their accesses?</p>	
<p>5.3 Mandatory Service Provider Privacy Training MPOs must ensure that all employees who are service providers or volunteers and who collect, create or access personal information, have completed mandatory privacy training related to the collection, use, disclosure, storage and destruction of personal information). This training must be completed prior to providing services.</p>	<p>How do you ensure that contractors/service providers complete Mandatory Service Provider Privacy Training?</p> <p>What role does the MPO have?</p>	
<p>5.4 Service provider compliance with privacy requirements There is a process in place for the ongoing monitoring of service provider compliance</p>	<p>Do you ever need to develop contracts with other parties e.g., other levels of government, or agencies?</p> <p>Is there a policy, procedure or checklist documenting</p>	

with privacy requirements (e.g. Section 30 of FOIPPA).	<p>what the privacy requirements are for agreements?</p> <p>What is the role of the MPO in regards to contracts developed for work in your area?</p> <p>How do you monitor and ensure that privacy requirements in those agreements are met?</p>	
6.2 Reporting to the CIRMO A procedure exists for the creation and reporting (to the CIRMO) of Personal Information Banks that result from new enactments, systems, projects, programs or activities of the ministry.	<p>Do you have PIBs in your area?</p> <p>Is there a documented process to guide you through creation and completion of a PIB?</p> <p>Where would you find that process (if it exists)</p>	
6.3 Health Information Banks For the Ministry of Health: A procedure exists for the creation and reporting (to the CIRMO) of Health Information Banks.	N/A	
6.4 Monitoring of Personal Information Directory A process is in place to review the PID at least annually to ensure all PIAs, ISAs, PIBs and, where applicable, HIBs have been submitted and recorded accurately.	Do you monitor the PID to confirm that any PIAs, ISAs etc are posted and are accurate?	
7.1 Reporting Foreign Demands A procedure is in place for reporting foreign demands for disclosure to the CIRMO.	<p>Have you ever received a request for PI from a foreign jurisdiction?</p> <p>If you received a request for PI from a foreign jurisdiction, what is the process for responding? Is that process documented somewhere?</p>	
8.1 Information Incident Management If an information incident occurred in the past 12 months, the incident was reported	<p>What is the process for reporting an Info Incident?</p> <p>How are staff made aware of the requirements to</p>	

immediately, all CIRMO instructions were followed and all recommendations were implemented.	report information incidents? What is the role of the MPO in the Info Incident process?	
Records		
1.1 Records management accountabilities The Ministry has articulated employees' responsibilities for records management and business areas have clearly assigned accountabilities to employees with additional role specific records management duties, as appropriate. Business areas work collaboratively with the Government Records Service. There is a clear understanding of respective roles and responsibilities and the names of such person(s) or group(s) and their responsibilities are communicated to internal personnel.	Are there defined records mgmt. processes for your area? What are they? How are RM responsibilities communicated to staff? Are specific staff identified for RM duties or are there defined roles and responsibilities for all staff? What is the GRS role for RM in your area?	
1.2 Records Management Policies/Procedures Records management policies and/or procedures have been defined for the ministry and the consequences of non-compliance are communicated at the commencement of employment and at least annually to all of the ministry's internal personnel. Changes to ministry records management policies/procedures are communicated to such personnel shortly after the changes are approved.	Are specific RM policies and practices documented for your area? How are the RM policies/procedures communicated to staff? How are RM policies and procedures developed in your area?	
2.1 Employee Training Employees have completed mandatory training related to records management (e.g. "Managing our information assets" and/or	Other than IM117, have you or any of your staff taken any records management training? If so, what training?	

"Managing government records").	How do you confirm that staff understand their RM responsibilities?	
3.1 Record Classification The ministry has procedures in place to classify and/or organize records so that the records can be managed according to the function of the information and the official and approved retention schedules.	How do you determine how long records should be retained – and when they can be destroyed? Do you categorize or classify records in your area in a specific way? Do you use ARCS/ORCS or some other system? Are the procedures for categorizing records documented?	
5.1 Information Schedule Development and Maintenance The ministry has formalized processes to support and enable the development and implementation of information schedules that include all the information that the ministry creates, captures, transfers or archives. The ministry has a formal procedure to identify records not covered by approved schedules.	Are records in your area covered by an ARCS/ORCS schedule? Do you know when the schedule was last reviewed or updated? Are you aware of a process or procedure to identify records that have not been scheduled?	
5.2 Information Retention Information is retained as long as required by the appropriate, approved information schedule and no longer. Where no schedule applies, the information is not disposed of. Personal information that is used to make a decision that directly affects the individual is retained for at least one full year.	Do you know where the ARCS/ORCS schedules for your records are? What is the process to destroy records with personal information?	
5.3 Records Disposition The ministry has formal procedures to dispose of, transfer, or archive government information based on official policies, specifications, schedules, guidelines, and procedures published by the Government	Who is responsible for disposing of records in your area? And in CIRMO? Do you know if the Ministry has any documented policies/procedures for records mgmt.? Where are the procedures located.	

Record Service.		
6.1 Hold Procedures The ministry has holds and discovery procedures and mechanisms in place to ensure that records are not destroyed in the case of a litigation hold or FOIPPA request.	Do you have a documented process/procedure to ensure that staff understand how to handle records subject to a litigation hold or FOI request are not destroyed?	
7.1 Identify and Protect Digital Records Scheduled for Archiving The ministry has formal procedures for identifying, protecting, and maintaining the usability and integrity of digital records scheduled for transfer to archives.	N/A	
7.2 Record Transfers to IMA Bodies The ministry has agreements and procedures in place to maintain chain of custody and continuity of control for records during transfers to other bodies covered by the Information Management Act. This includes procedures to monitor such transfers.	N/A Do you ever transfer records to other bodies?	
7.3 Record Transfers to Non-IMA Bodies The ministry has formal procedures in place to ensure that records transfers to bodies not covered by the Information Management Act are completed in accordance with an appropriate legal instrument.	N/A	
8.1 Manage Information in Recordkeeping Systems The ministry manages government information in recordkeeping system(s) that manage records throughout their lifecycle. Systems are used to meet records management requirements, including	If staff maintain government records outside of record keeping systems is there a documented process or procedure directing them to manage those records? For example, someone works out of the office and saves work material to their H: drive because the internet is down, do staff move that material so	

schedules as mandated in the IMA.	others can access it?	
8.2 Manage Physical Records Formal procedures exist regarding the management and storage of physical records in appropriate onsite storage (commensurate with degree of information sensitivity) or approved offsite storage facilities.	Do you have any physical records? If so, how do you manage them?	
8.3 Inventory of Ministry Systems and Repositories The ministry maintains an inventory of ministry systems and repositories that manage and/or store government information.	N/A	
Access		
1.1 Duty to Assist Duty to assist procedures has been clearly defined and has been communicated to all staff. Ministry staff is informed and aware of the appropriate response to FOI requests (e.g., how to conduct a comprehensive and timely search for responsive records, seeking clarification, and execute these steps in accordance to defined procedures).	How are FOI requests handled in your area? Who is responsible for initial intake, scope, receiving replies, etc.? Are those roles formally defined in your area? Are procedures for handling FOI requests documented? Within your area? Within the Ministry? How are staff informed of their FOI responsibilities? How are FOI response requirements communicated to staff? When were the procedures last reviewed?	
1.2 Information Access Accountability Accountabilities for FOI requests are assigned, and roles and responsibilities are clearly	See above	

defined. Resource allocation should be commensurate with the volume of requests received, and at a classification appropriate to the requirement.		
1.3 Information Access Procedures Information Access procedures have been clearly defined and are made available to all Ministry employees and Ministerial staff. These procedures are reviewed at least annually and updated as required.	See above	
2.1 Employee Training Employees have completed training related to FOI/ Information Access. Individuals have received additional, role-specific FOI/Information Access training where appropriate (E.g. ministerial staff, FOI co-ordinators).	Other than IM 117 have staff received any additional training for FOI info request processes? How are staff made aware of their FOI responsibilities, e.g., duty to assist, other FOI policies/procedures	
3.1 Dedicated Public Servant A dedicated Public Servant is designated as the person in charge of all requests involving a Minister's office. This person is accountable for contacting all staff directly, in writing, with the details of the request and directing that staff search for responsive records and respond within a set time period. This individual must also retain a current list of all Ministerial staff that is shared on an ongoing basis with IAO.	NA	
4.1 Monitoring of FOI Requests A formal process is in place to track and monitor all active FOI requests. This includes regular reporting to Ministry leadership and escalation processes and triggers to be used if	Is there a process to track and monitor FOI requests in your area? In CIRMO? Is that process documented? If there is an issue with an FOI request (e.g.,	

there is a risk of non-compliance with timeliness or "duty to assist" requirements.	problems/delays) how do you escalate it? Is the escalation process documented?	
4.2 Monitoring Service Provider Compliance with FOI requirements There is a process in place for the ongoing monitoring of service provider compliance with processes related to FOI requirements	Do you manage service providers/contractors? Is there a process to track and monitor FOI requests for service providers managed in your area? In CIRMO? Is that process documented? If there is an issue with an FOI request (e.g., problems/delays) how do you escalate it? Is the escalation process documented?	
Information Protection		
1.2 Training	Other than IM 117 do staff receive any additional information protection/information security training	
1.4 Asset Management	Does your area maintain an inventory of assets and systems? Do you have equipment that is signed out by staff? How does the process work?	
1.5 Employee accountabilities	Are information protection requirements documented for staff? Are the information protection requirements included in the job description or in any other documents? E.g., confidentiality agreement, acceptable use policy, etc. How are those responsibilities communicated to	

	<p>staff?</p> <p>How do you confirm/ensure that staff understand their responsibilities?</p>	
1.6 Physical and Environmental Protection (reasonable security)	<p>Are there any documented policies or procedures to guide staff in the handling of equipment with sensitive info?</p> <p>How are those requirements communicated to staff?</p>	
1.8 Security Classification	<p>Do you classify or categorize your records by sensitivity?</p>	
1.9 Portable Media	<p>Do you use portable media devices in your area? E.g., USB sticks, portable hard drives, digital recorders</p> <p>How are those devices managed? Is there use tracked? Is there a process documented to require information to be uploaded to record keeping systems after use? How do you confirm that the devices are protected and managed in accordance with policy requirements?</p>	

1.10 Access control	<p>What information systems are in use in your area?</p> <p>How do you arrange for staff/contractors to have access to each system? Revoke access? How timely is it to revoke access?</p>	
1.14 Business Continuity Management <p>Business continuity management processes and plans have been developed tested, maintained, updated and they include provisions to maintain security and information protection in the case of an incident.</p>	<p>Is a BCP in place you your area?</p> <p>When was the BCP last updated?</p> <p>When was the BCP last tested?</p>	

Assessment Questions for Health

From: Jager, Brenda HLTH:EX <Brenda.Jager@gov.bc.ca>
To: Jackson, Brittany CITZ:EX <Brittany.Jackson@gov.bc.ca>, Grover, Brent CITZ:EX <Brent.Grover@gov.bc.ca>
Sent: August 29, 2018 1:40:29 PM PDT
Attachments: IMCAP Questions-Draft 2018-09-28.docx

Hello Brent and Brittany,
Here are my draft questions for the assessments.

Brenda Jager | Records Officer

Ministry of Health | Health Sector Information Management & Technology Division | Health IT Strategy Branch

Phone: TBD

Self-Assessment Guidance Material (DRAFT)

From: Jackson, Brittany CITZ:EX
s.15; s.22
To: Thibault, Sarah FIN:EX <Sarah.Thibault@gov.bc.ca>
Cc: Grover, Brent CITZ:EX <Brent.Grover@gov.bc.ca>
Sent: July 30, 2018 10:22:47 AM PDT
Attachments: Sample Interview Questions.docx, SA Self Assessment Guide - CURRENT.docx,
SA IMPR Walkthrough - CURRENT.pptx

Hi Sarah,

Attached below is our current, draft guidance material for ministry self-assessments:

We are in the midst of approving final versions of these documents – please note that the versions above may become out-of-date within the next few months.

In addition, there are several resources/templates noted within the guide – these resources will be available once the guidance material is finalized.

Please review the attached documents and let me know if you have any questions or feedback.

Brittany

Brittany Jackson | Senior Auditor | Privacy, Compliance and Training Branch
Ministry of Citizens' Services | T: (250) 356-9639

From: Thibault, Sarah FIN:EX
Sent: Friday, July 27, 2018 11:32 AM
To: Jackson, Brittany CITZ:EX
Cc: Thibault, Sarah FIN:EX
Subject: RE: Meeting Follow-up

I'm on the edge of my seat!

Respectfully,

Sarah Thibault
Divisional Information Management Analyst
Tel: 778.698.4808

RD Information Management Inquiries: FIN.REV.RIM@gov.bc.ca

From: Jackson, Brittany CITZ:EX
Sent: Friday, July 27, 2018 10:53 AM
To: Thibault, Sarah FIN:EX
Subject: RE: Meeting Follow-up

Hi Sarah,

Just to follow up – Brent is amending a few of the guidance documents before I pass them on to you.

I should be able to email you the draft material either today or early next week.

Thanks for your patience,
Britt

Brittany Jackson | Senior Auditor | Privacy, Compliance and Training Branch
Ministry of Citizens' Services | T: (250) 356-9639

From: Thibault, Sarah FIN:EX
Sent: Wednesday, July 25, 2018 2:04 PM
To: Jackson, Brittany CITZ:EX
Cc: Thibault, Sarah FIN:EX
Subject: RE: Meeting Follow-up

That is great news! Thanks for the follow-up Brittany.

Respectfully,

Sarah Thibault
Divisional Information Management Analyst
Tel: 778.698.4808

RD Information Management Inquiries: FIN.REV.RIM@gov.bc.ca

From: Jackson, Brittany CITZ:EX
Sent: Wednesday, July 25, 2018 1:52 PM
To: Thibault, Sarah FIN:EX
Subject: RE: Meeting Followup

Hi Sarah,

Sorry for the late response - our team is meeting tomorrow to discuss our draft versions of the self-assessment guidance documentation.

We will also be discussing the possibility of providing sample interview questions within the guidance documentation.

I will connect with you after the meeting and send you any material we are able to (somewhat) finalize during our meeting.

Britt

Brittany Jackson | Senior Auditor | Privacy, Compliance and Training Branch
Ministry of Citizens' Services | T: (250) 356-9639

From: Thibault, Sarah FIN:EX
Sent: Wednesday, July 18, 2018 1:01 PM
To: Jackson, Brittany CITZ:EX
Cc: Thibault, Sarah FIN:EX
Subject: RE: Meeting Followup

Hi Brittany,

Thank you for your response and for reviewing the Executive Summary – I want to make sure I speak about the assessment accurately, especially at an executive level.

A few more questions if you don't mind:

- I believe either Brent or you were able to provide some questions (not the results) for questions that are typically asked during an assessment –referencing the CIRMO pilot assessment. The questions would be helpful in formatting my questions for the inventory.
- Are you able to share the tools used when conducting a self-assessment?

Much appreciated, thank you

Respectfully,

Sarah Thibault
Divisional Information Management Analyst
Tel: 778.698.4808

RD Information Management Inquiries: FIN.REV.RIM@gov.bc.ca

From: Jackson, Brittany CITZ:EX
Sent: Wednesday, July 11, 2018 3:51 PM
To: Thibault, Sarah FIN:EX
Cc: Grover, Brent CITZ:EX
Subject: RE: Meeting Followup

Hi Sarah,

In order to obtain training stats for your division, please connect with your Ministry Privacy Officer (Richard Barlow).

Your executive summary looks great to me – please let us know if you need any assistance while completing your self-assessment.

Thanks,
Brittany

Brittany Jackson | Senior Auditor | Privacy, Compliance and Training Branch
Ministry of Citizens' Services | T: (250) 356-9639

From: Thibault, Sarah FIN:EX
Sent: Monday, July 9, 2018 8:24 AM
To: Jackson, Brittany CITZ:EX
Cc: Grover, Brent CITZ:EX; Thibault, Sarah FIN:EX
Subject: RE: Meeting Followup

Thank you Brittany, much appreciated – looking forward to your reply.

On another note:

Attached is a draft of an Executive Summary for the Information Management Inventory (one pager). Would you/Brent be able to read through and provide some feedback from the lenses of a records professional? Wondering if the

document makes sense and if I've interpreted and described the assessment correctly. If you both have some time to do so:-), any comments or suggestions is most welcome.

Thank you

Respectfully,

Sarah Thibault
Divisional Information Management Analyst
Tel: 778.698.4808

RD Information Management Inquiries: FIN.REV.RIM@gov.bc.ca

From: Jackson, Brittany CITZ:EX
Sent: Friday, July 6, 2018 3:13 PM
To: Thibault, Sarah FIN:EX; Grover, Brent CITZ:EX
Subject: RE: Meeting Followup

Hi Sarah,

It was nice to meet you today – thanks for asking such great questions, I learned a lot alongside you :-)

Our branch's contact for training stats is currently away until July 11 – I will be able to get you the stats shortly after this date.

Thanks,

Britt

Brittany Jackson | Senior Auditor | Privacy, Compliance and Training Branch
Ministry of Citizens' Services | T: (250) 356-9639

From: Thibault, Sarah FIN:EX
Sent: Friday, July 6, 2018 1:29 PM
To: Grover, Brent CITZ:EX
Cc: Jackson, Brittany CITZ:EX
Subject: RE: Meeting Followup

Brent and Brittany,

Thank you both for meeting with me today, and for your openness to share information. I learned a lot and gained some confidence in our inventory direction.

As discussed, please find attached a draft of our information collection for our inventory. As per your feedback, I've added a bullet point regarding "Authorized accessibility/Monitoring list" for digital records. Should you have any other feedback, I welcome it with open arms. I truly value feedback – it's the best way for me to improve on my skills.

Have a great weekend!

Respectfully,

Sarah Thibault
Divisional Information Management Analyst
Tel: 778.698.4808

RD Information Management Inquiries: FIN.REV.RIM@gov.bc.ca

From: Grover, Brent CITZ:EX
Sent: Friday, July 6, 2018 12:42 PM
To: Thibault, Sarah FIN:EX
Cc: Jackson, Brittany CITZ:EX
Subject: Meeting Followup

Hi Sarah, it was nice meeting you today^{s.22}

The document on Office Recordkeeping Systems is on the GRS Intranet (this is the link).
<<https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/records-management/guides/officerecordkeepingsystem.pdf>>

Brittany will forward the link to the training stats shortly.

Thanks

Brent Grover, MPA|Senior Auditor (Practice Reviews)
Investigations and Reviews|Privacy, Compliance and Training Branch|Ministry of Citizens' Services
Ph: 778-698-4992|M: PO Box 9406, Stn Prov Gov, Victoria BC V8W 9V1

The dogmas of the quiet past are inadequate to the stormy present - Lincoln

Government confidentiality and privilege requirements apply to this message and any attachments. If you are not the intended recipient, you are hereby notified that any review, retransmission, conversion to hard copy, copying, circulation or other use is strictly prohibited. If you are not the intended recipient, please notify the sender immediately, and delete this message and any attachments from both your inbox and deleted items folder. Thank You.

RE: Assessment Questions for Health

From: Grover, Brent CITZ:EX <Brent.Grover@gov.bc.ca>
To: Jager, Brenda HLTH:EX <Brenda.Jager@gov.bc.ca>
Cc: Jackson, Brittany CITZ:EX <Brittany.Jackson@gov.bc.ca>
Sent: August 30, 2018 12:18:44 PM PDT
Attachments: SA IMPR Walkthrough V03 CURRENT.pptx, SA 2018 Practice Review Framework Worksheet CURRENT.xlsx, SA - Self Assessment Guide V03.docx

Hi Brenda, thank you for sharing your questions. As we discussed we are in the midst of preparing materials for Ministries. I have attached some of the DRAFT materials that may be useful including:

- [2018 Practice Review Framework Worksheet](#) this Worksheet has the criteria and maturity rankings used by Ministries to conduct self assessments and by our team to do baseline assessments. We are trying to avoid the duplication of work by used the same Framework and ranking for both types of assessments. There are columns in the Worksheet to provide a maturity ranking, rationale for the ranking and any variances noted in the practices (e.g., exceptional practices);
- [IMPR Walkthrough \(Draft\)](#) a one page graphic of the assessment phases and tasks;
- [Self Assessment Guide \(Draft\)](#) a guide with descriptions for each of the tasks in the assessment phases. Page 11 has a list of the various tools that can be adapted for your use.

If you have any questions or concerns please let us know. At some point we may try to bring the early implementers of the Framework together to share tips and tricks.

Thanks

Brent Grover, MPA | Senior Auditor (Practice Reviews)

Investigations and Reviews | Privacy, Compliance and Training Branch | Ministry of Citizens' Services

Ph: 778-698-4992 | M: PO Box 9406, Stn Prov Gov, Victoria BC V8W 9V1

The dogmas of the quiet past are inadequate to the stormy present - Lincoln

Government confidentiality and privilege requirements apply to this message and any attachments. If you are not the intended recipient, you are hereby notified that any review, retransmission, conversion to hard copy, copying, circulation or other use is strictly prohibited. If you are not the intended recipient, please notify the sender immediately, and delete this message and any attachments from both your inbox and deleted items folder. Thank You.

From: Jager, Brenda HLTH:EX

Sent: Wednesday, August 29, 2018 1:40 PM

To: Jackson, Brittany CITZ:EX; Grover, Brent CITZ:EX

Subject: Assessment Questions for Health

Hello Brent and Brittany,

Here are my draft questions for the assessments.

Brenda Jager | Records Officer

Ministry of Health | Health Sector Information Management & Technology Division | Health IT Strategy Branch

Phone: TBD

IMCAP assessment work at Health - templates etc.

From: Jager, Brenda HLTH:EX <Brenda.Jager@gov.bc.ca>
To: Grover, Brent CITZ:EX <Brent.Grover@gov.bc.ca>, Jackson, Brittany CITZ:EX <Brittany.Jackson@gov.bc.ca>
Cc: Hall, Simon HLTH:EX <Simon.Hall@gov.bc.ca>, Wright, Richelle CITZ:EX <Richelle.Wright@gov.bc.ca>
Sent: November 2, 2018 8:56:45 AM PDT
Attachments: IMCAP Report Template 2018-11-02.docx, IM Best Practices 2018-11-01.docx, IMCAP Sample Report filled 2018-11-02.docx

Hello Brent and Brittany,

To keep you in the loop with my IM maturity level assessments for the Ministry of Health, I thought I would send you my template report document and list of improvement tasks (Best Practises) that I developed to report out to the Branches in the HSIMT Division. To show how they work, I have provided a sample filled out report too.

I have completed the assessments and have circulated the reports. Just waiting for the branches to respond with any inaccuracies.

Please let me know your thoughts on these documents. I consider them continuous improvement projects.

Brenda Jager | Records Officer

Ministry of Health | Health Sector Information Management & Technology Division | Health IT Strategy Branch

Phone: 778 974-4969