A4 Charter

Define Tool

Project: **IM Strategy – IM Assessment**
Ministry: Ministry of Transportation and Infrastructure - Infrastructure & Major Projects Division
Sponsor: Patrick Livolsi (or ED?) **Lead:** Trevor Youdale (and Brittney Speed?)
Prepared by: Jessee Skulmoski, Gislene Guenard, Trevor Youdale **Date:** <date>

Problem Statement
• *Assess the state of information management within the department to support strategic IM decisions*

Scope of Process Involved			
Process Description	Data gathering, series of interviews, summery of findings.		
Start of Process	*Meeting with client*	End of Process	*Presentation of findings, recommendations*
Included		Excluded	
• *All recorded information under control of department* • SME and leadership time		• *Other records management project work* •	

Goal Statement
• *To discover areas for improvement and support information schedule development*

Performance Measures				
Objective	Measure	Units	Current Measure	Control Measure
Identify records holdings *Interview SMEs*	*Assessments* *interviews comepleted* *Summary of findings* *Meetin with executive*	*Number of interviews* *Presentattion to executive*		

Potential Benefits	
Tangible Gains	Intangible Gains
• *Number of issues identified*	• *Enagement, change management, awareness*

Opportunities/Assumptions/Risks/Constraints			
Opportunities	Assumptions	Risks	Constraints
• *To engage programs area staff*	• *Executive support and participation by leaders and program area*	• *Availability of particupants* • *Clarity of purpose and scope*	• *Participant schedules*

	employees	• *Travel logistics*	

Project Team		
Name	Project Role	% Time Available for Project
• *Trevor Youdale* • *Gislene Guenard* • *Brittney Speed* • *Branch ED's*	• *IM Assessment Lead, lead interviewer* • *Corporate IM Manager – connector* • *Manager Divisiosnl Operations – coordinator* • *Executive Directors or delegates*	• *33?*

Project Schedule			
Phase / Deliverable	Scheduled Start Date	Scheduled Complete Date	Actual Complete Date
Define			
Measure			
Workshop			
Analyze			
Improve/Implement			
Control			

Signatures					
Sponsor		Date:	Champion		Date:

ARIS IOC ID	Type	Lvl	Current Name	Current System CRMS,TRIM P,P/E	CRMS Org Unit ID	Name of CRMS Org Unit Used	Number of boxes in offsite storage	Number of Records in CRMS	Number of Active Records in CRMS	Last Create Date CRMS Data YYYY/MM/DD	Name of TRIM Record Type Used	Date of Last Edit of TRIM Data YYYY/MM/DD	Has Trim End Users	Have added TRIM E-records this year
	C	2	**MINISTRY OF**											
	E	3	Executive Committee											
	E	4	**Minister**											
	E	5	Deputy Minister / Chief Executive Officer											
	E	6	ADM,											
	E	6	Exec Dir, Corporate Initiatves											
	C	3	Division											
	C	4	**Branch**											
	C	5	Unit											

Applicable ORCS Record Schedules			Current in-Branch RM Support Provided by?	LAN Organization initiative underway?	Address of Branch shared drives \\sharename\S#####	Contacts	Director/Program Head	Comments/Notes

1 To what extent are business records that are critical for your operations clearly identified and findable?

2 To what extent are your transitory records identified? (eg. Are working documents marked as DRAFT and easily distinguishable from FINAL versions?)

3 To what extent are both electronic and physical copies of the same document kept? (e.g. keeping printed copies of digital records (or scans of paper)

4 Is there a legal requirement for some / all of your information to be maintained in a physical form? (make note of specifics)

5 Do you have a plan to digitize (scan) some or all of the current physical (paper)?

6 To what extent do you have your work unit's records management processes been documented? (eg: written documents detailing naming conventions, records retention schedules, off boarding employee/contractor requirements)

7 To what extent are your work units records management processes being used?

8A To what extent are staff trained in your work units records management process?

8B To what extent do staff know and use the ARCS and ORCS classifications relevant to the records they create?

9 How much effort is required by your work unit to find information to do their daily work?

10 How much effort is required to find information for extraordinary requests? (FOI, minister requests, etc)

11 Approximate extent of staff in your work unit that have received training in Government Records Management practices within the past 5 years? (this can include formal, online, internal, and informal training)

12 What is biggest challenge (pain point) for dealing with email? (e.g. running out of space, duplication and tracking of threads, finding relevant email,

13 Describe for us what would be your biggest driver to change? In your opinion, what would be reasons to change your current Information Management practises? (e.g. Legislation, legal decision, moving location, workforce demographics, technology, new program, etc.)

14 What is the biggest challenge (pain point) in practicing Information Management today?

15 What would be a quick win to improving your current practices?

16 How would you rate your work unit's general level of knowledge about the Information Management Act? Refer to diagram of Information Management

17 How would you rate your work units' enthusiasm to changing your current Information Management practices?

18 Would your work unit be interested to be an early-adopter in IMA related project?

19 In your opinion, what is the maturity level of your Information Management Processes? (Refer to diagram of Information Management Maturity Levels in the accompanying reference document – this is a self-assessment)

20 Where is your work unit's information currently stored? (see options below)

21A Have any LAN re-organization efforts occurred in your Branch?

21B To what degree is the shared drive associated/ aligned with ARCS/ORCS?

22 Does your work unit(s) have [cross-ministry records e.g. licensing/permitting]?

23 Last question! In your opinion, what was the degree of difficulty responding to these interview questions?

Unstructured Data	Y/N	Identify approximate % of total holdings (number not size)
TRIM		
SharePoint		
Shared Network Drive (LAN)		
Personal Network Drive (H:)		
Local Drive (C:)		
Shared Govt Email		
Personal Govt Email		
USB Key		
Portable Hard drive		
DVD/CD		
Mobile Device / Smartphone		
Other		
Paper		
# of physical records (file cabinets, etc)		

Structured Data Systems	Y/N	Name of System
Line of Business Systems		
Corporate systems		
Access database systems		
Data warehouse systems		
Data marts systems		
Catalogs		
Other		
Lan Share Name		
Share Point Root Url		
Shared Email Name		

ARIS IOC ID	Current Name	Contacts	Director/Program Head	Interviewer(s)	Interviews Complete	Comments/Notes
	MINISTRY OF					
	Executive Committee					
	Minister					
	Deputy Minister / Chief Executive Officer					
	ADM,					
	Exec Dir, Corporate Initiatves					
	Division					
	Branch					
	Unit					
	Unit					
	Unit					
	Unit					

MoTI Infrastructure and Major Projects IM Assessment project- data gathering template

PROGRAM AREA:			Infrastructure Development	Planning and Programming	Evergreen Line	GMTRP	Procurement & Public Private Partnerships	Metro Vancouver Major Projects	ADM		
Interviewer:											
Program Contact:											
Interview Participants:											
A - PHYSICAL RECORDS	1)	Do you keep paper copies of current records? YES/NO									
	1. a	Identify main categories of paper records currently created:									
	1. b	Comments:									
	2)	Are your paper records tracked in any records management systems other than CRMS or TRIM (eg. Index cards, Excel, databases)? YES/NO									
	2. a	Identify systems used:									
	2. b	Identify record series tracked in alternative systems:									
	2. c	Comments:									
	3)	Are there any legal or business reasons for them to be in paper format? YES/NO/UNKNOWN									
	3. a	Reasons for paper format:									
	3. b	Comments:									
	4)	Are there any digitization or scanning projects being planned for									
	4. a	Records series captured or in consideration:									
	4. b	Comments:									
		Additional Comments:									
B - EMAIL RECORDS	1)	To what extent are business emails stored in a shared location accessible by appropriate branch staff? MINIMAL / SOMEWHAT / MOSTLY									
	1. a	What is the branch practice for capturing and sharing emails?									
	1. b	Comments:									
	T.C.	Please identify the primary challenges associated with managing email records in your branch (eg. Running out of space, duplication and tracking of threads, finding relevant email, storing on backups, etc.):									
		Additional Comments:									
C - ELECTRONIC DOCUMENTS	1)	To what extent are branch electronic documents stored in a									
	1. a	Identify top three locations [by approximate volume] where branch									
	1. b	Identify addresses of active and legacy LAN drives owned by branch:									
	1. c	Comments:									
	2)	Are branch electronic documents on LANs associated with ARCS/ORCS									
	2. a	Is final disposition applied to those electronic documents that are									
	2. b	Describe the disposition process followed:									
	2. c	Comments:									
	3)	To what extent does your branch keep both electronic and paper									
	3. a	In what circumstances?									
	3. b	Do staff know which is the official document? YES / NO									
	3. c	Comments:									
	T.C.	Please identify the primary challenges associated with									
		Additional Comments:									
D - STRUCTURED DATABASES	1)	Does branch use Line-of-Business systems (eg. Compliance Verification Information System) YES / NO									
	1. a	Identify systems [full names – no acronyms please ☺]:									
	1. b	Is your branch the primary owner of these systems? Please specify:									
	1. c	Comments:									
	2)	Do any of the systems store electronic documents? YES / NO									
	2. a	Which systems store electronic documents?									
	2. b	Which record series?									
	2. c	Comments:									
	3)	Do any business systems house the official copy of electronic									
	3. a	Identify system:									
	3. b	Are duplicates of the information managed elsewhere (eg. LAN,									
	3. c	Is the final disposition of electronic documents managed in the system?									
	3. d	Comments:									
	4)	Who is the current IMB business portfolio contact for the systems?									
	4. a	Identify IMB contacts for systems?									
	4. b	Comments:									
	T.C.	Please identify the primary challenges associated with									
		Additional Comments:									

MoTI Infrastructure and Major Projects IM Assessment project- data gathering template

PROGRAM AREA:			Infrastructure Development	Planning and Programming	Evergreen Line	GMTRP	Procurement & Public Private Partnerships	Metro Vancouver Major Projects	ADM
E - INFORMATION SCHEDULES	1)	Does your branch have an Operational Records Classification Schedule (ORCS) for the records it creates? YES / NO							
	1. a	Identify information schedules used (title or #):							
	1. b	Is it used across branch?							
	1. c	Comments:							
	2)	Does the information schedule being used reflect current business functions? YES / NO / UNKNOWN							
	2. a	Identify any known gaps or problem areas in information scheduling (if							
	2. b	Comments:							
	T.C.	Please identify the primary challenges associated with							
		Additional Comments:							
F - RECORDS MANAGEMENT PROCEDURES AND PRACTICE	1)	Do offices have branch-specific business procedures for information and records management? YES / NO							
	1. a	Are these procedures documented and easy to reference?							
	1. b	Comments:							
	2)	Can your branch easily find its business critical information and							
	2.a/b	1 - Business Critical Record Series:							
		Large Quantity of Paper Onsite? Y/N							
		High Med Low Business Access?							
		Frequent Public Access Y/N? (Routine, FOI, Litigation)							
		Good Candidate for Paper Scanning Y/N?							
	2.a/b	2 - Business Critical Record Series:							
		Large Quantity of Paper Onsite? Y/N							
		High Med Low Business Access?							
		Frequent Public Access Y/N? (Routine, FOI, Litigation)							
		Good Candidate for Paper Scanning Y/N?							
	2.a/b	3 - Business Critical Record Series:							
		Large Quantity of Paper Onsite? Y/N							
		High Med Low Business Access?							
		Frequent Public Access Y/N? (Routine, FOI, Litigation)							
		Good Candidate for Paper Scanning Y/N?							
	2. c	Are there any additional series of paper records that should be							
	3)	no question #3							
	4)	To what extent do branch employees know how to classify their business critical records according to ARCS/ORCS? MINIMAL / SOMEWHAT / MOSTLY							
	4. a	Is classification done individually or centrally?							
	4. b	Do naming conventions exist for business critical records?							
	4. c	Comments:							
	5)	Does the branch have specific employees tasked with Information							
	5. a	Identify position(s) and Current staff:							
	5. b	Describe assigned functions/responsibilities:							
	5. c	Comments:							
	6)	To what extent does your branch send out communication regarding							
	6. a	To what extent are new employees trained in branch practice?							
	6. b	To what extent are the records of departing employees managed							
	6. c	Comments:							
	T.C.	Please identify the primary challenges associated with records							
		Additional Comments:							
G - CORPORATE RECORDS AND INFORMATION TRAINING AND SUPPORT	1)	Is there an expectation in your branch that staff take the corporate							
	1. a	Estimate % of staff who have taken online courses IM117, IM110 and							
	1. b	Estimate % of staff who have taken the classroom courses in government							
	1. c	Comments:							
	2)	Do employees know who to contact at Government Records Services for							
	2. a	Who are primary internal, sector and/or corporate contacts?							
	2. b	Are employees aware of online records and information							
	2. c	Comments:							
	3)	Are branch employees aware that changes to information and records							
	3. a	Which issues should take priority in your branch if it is to meet the							
	3. b	Comments:							
	T.C.	Please identify the primary challenges associated with							
		Additional Comments:							

MoTI Infrastructure and Major Projects IM Assessment project- data gathering template

PROGRAM AREA:			Infrastructure Development	Planning and Programming	Evergreen Line	GMTRP	Procurement & Public Private Partnerships	Metro Vancouver Major Projects	ADM		
H - MINISTRY SPECIFIC QUESTIONS	1)	TBD									
		If yes, ...									
		Comments:									
	T.C.	Please identify any ministry-specific challenges associated with									
		Additional Comments:									
VOLUME OF ONSITE FILES	1)	# of linear feet in CENTRAL office spaces:									
	2)	# of linear feet in PERSONAL office spaces:									
	3)	# of OPEN SHELF file cabinets and their dimensions:									
	4)	Total Linear Feet of Records For Office								Ministry Total Linear Feet	0
	5)	Notes / Comments:									

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, including documenting government decisions, and business areas have clearly assigned accountabilities across the Ministry with additional role specific records management duties, as appropriate. There is a clear understanding of respective roles and responsibilities, the names of such persons or groups and their responsibilities are communicated to internal employees.	The Ministry has not articulated responsibility for records management or documenting government decisions to ministry employees. Records management issues are addressed reactively. Few or no employees are aware of their individual responsibilities for appropriate records management or documenting government decisions.	The Ministry has not articulated responsibility for records management, or employees' responsibilities for documenting government decisions, and current mechanisms are often informal and fragmented. There is some level of awareness by employees of their individual records management responsibilities, including responsibilities for documenting government decisions, and the role of the Government Records Service.	Defined roles and responsibilities have been developed and employees are aware of and understand their records management and documenting government decisions responsibilities. The Ministry is aware of and work collaboratively with the Government Records Service.	Management regularly reviews the ministry's records management program, 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	**Records Management Policies/Procedures** The Ministry implements records management policies and/or procedures provided by GRS, including documenting government decisions. The Guideline and Directive on documenting government decisions have been formally shared and their importance communicated across the Ministry.	The Ministry has not implemented records management policies and/or procedures provided by GRS, including documenting government decisions.The Guideline and Directive on documenting government decisions have not been formally shared and their importance has not been communicated across the Ministry.	The Ministry implements records management policies and/or procedures provided by GRS, including documenting government decisions; however, employees' awareness remain inconsistent. The Guideline and Directive on documenting government decisions have been shared inconsistently.	The Ministry implements records management policies and/or procedures provided by GRS, including documenting government decisions. The Guideline and Directive on documenting government decisions have been formally shared and their importance communicated across the Ministry.	Management regularly reviews the ministry's records management adherence to GRS' policies and/or procedures, including documenting government decisions. The Ministry seeks ways to improve employee awareness regarding documenting government decisions.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include regular communications about the records management policies and/or procedures that has led to high visibility and a higher level of Ministry employees' awareness 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 (i.e. IM117) training related to records management. The training is scheduled, timely, consistent and periodically refreshed.	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. Training is refreshed at least every two years. Training is scheduled, timely, consistent, monitored and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.). The process for monitoring training completion is documented.	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.). Training is refreshed at least every two years and all Ministry employees 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-Based Training** Employees have received additional, role-based records management training (beyond IM117) where appropriate, and relevant Ministry employees have undergone training on the creation and maintenance of adequate records of government decisions, and documenting government decisions.	There is a general understanding of the need for role-based records management training; however, Ministry employees who require such training are not identified. Where employees have been identified, these individuals have not undertaken the role-based training on the creation and maintenance of adequate records of government decisions, and documenting government decisions. Additional training is provided in an inconsistent and reactive manner.	Ministry employees who require additional training relevant to their roles are identified, but training is inconsistent, and completion is not tracked or documented.	There is a documented process in place to identify Ministry employees who require additional training. All additional training is scheduled and delivered in a timely and consistent manner. Employees have undertaken additional training on the creation and maintenance of adequate records of government decisions in accordance to the Directive CRO 01-2019, Guidelines on Documenting Government Decisions and Section 6(1) of *Information Management Act*.	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, which will include their responsibilities relating to documenting government decisions.
3. Records Classification and Information Schedules						

Records Management		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
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 and/or organize records and an inconsistent 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.
3.2	**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 maintenance of information schedules.	Processes to support and enable the development, implementation, and 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.
4. Digitization Requirements						
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 inconsistent 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 inconsistent 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.
4.2	**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.
5. Records Retention, Maintenance and Disposition						

Records Management		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
5.1	**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.
5.2	**Records Transfers to IMA Bodies** The Ministry has 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.
5.3	**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.
5.4	**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 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.
6. Recordkeeping Systems and Inventories						
6.1	**Manage Information in Recordkeeping Systems** The Ministry manages government information through its lifecycle using recordkeeping systems as appropriate. Systems are used to meet records management requirements, including schedules as mandated in the *Information Management Act* and ensuring records capture the Ministry's documenting government decisions requirements, are preserved and accessible as required and appropriate.	Recordkeeping systems and adequate records of government decisions are not implemented and/or procedures are not communicated to employees.	The Ministry maintains some, but not all of the appropriate records and records of government decisions within recordkeeping systems. The overall management of records is not consistent, records management lifecycle supporting the preservation and accessibility of records is not communicated to employees and the Ministry has an informal systems to document government decisions.	The Ministry has established procedures and communicated to employees the processes needed to manage information appropriately in recordkeeping systems. Ministry records, including records documenting government decisions, 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 systems 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 recordkeeping, the *Information Management Act* and the Directive on documenting government decisions. 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 systems to allow uniform lifecycle management to be applied; * the optimization of information schedules to enable easy classification across disparate systems and platforms; and/or * mechanisms and strategies to continuously refine recordkeeping systems adopted for documenting government decisions; ensuring its alignment with Directive CRO 01-2019 and section 6 of the *Information Management Act.*

Records Management		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
6.2	**Inventory of Ministry Systems and Repositories** The Ministry maintains an inventory of ministry systems and repositories that manage and/or store government information.	No inventory of Ministry systems and repositories exists.	An inventory of Ministry systems and repositories exists, but it is not complete or regularly updated.	A documented procedure is in place for the creation and maintenance of an inventory of systems and repositories, and an up-to-date inventory is in place.	The inventory process is regularly monitored and exceptions are identified and updated in the inventory on an ongoing basis, where required.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include the automation of the system/repository inventory.

Records Management		1 - initial 2 - repeatable 3 - defined 4 - managed 5 - optimaized
#	Criteria	
1. Governance and Accountability		
1.1	Records Management Accountabilities	s.13
1.2	Records Management Policies/Procedures	
2. Education and Awareness		
2.1	Mandatory Employee Training	
2.2	Role-Based Training	
3. Records Classification and Information Schedules		
3.1	Record Classification	
3.2	Information Schedule Development and Maintenance	
4. Digitization Requirements		
4.1	4.1 Digital Records	
4.2	Identify and Protect Digital Records Scheduled for Archiving	
5. Records Retention, Maintenance and Disposition		
5.1	Records Retention, Holds and Disposition	
5.2	Records Transfers to IMA Bodies	
5.3	~~Records Transfers to Non-IMA Bodies~~	
5.4	Manage Physical Records	
6. Recordkeeping Systems and Inventories		
6.1	Manage Information in Recordkeeping Systems	
6.2	Inventory of Ministry Systems and Repositories	

Page 016 of 444 to/à Page 021 of 444

Withheld pursuant to/removed as

s.13

Privacy		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Governance and Accountability						
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 inconsistent 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 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 FOIPPA Delegation Instrument is in place, maintained and communicated to CIRMO by the MPO.	The Deputy Minister has delegated duties, powers, or functions but has not used a delegation instrument. There is no recognition of roles with accountability for certain duties, powers or functions. Privacy issues are addressed reactively, on a case-by-case basis.	The Deputy Minister has delegated duties, powers, or functions but has not used a delegation instrument. There is informal recognition of roles with accountability for certain duties, powers or functions.	The Deputy Minister has delegated duties, powers, or functions to certain roles (e.g. MPO) and has used a FOIPPA Delegation Instrument. The FOIPPA Delegation Instrument is maintained and communicated to CIRMO by the MPO.	The MPO maintains and monitors all Ministry FOIPPA Delegation Instruments.	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, the delegation is documented and current. The MPO remains accountable as the single point-of-contact for CIRMO.	The MPO has delegated duties, powers, or functions but has not documented the delegation. There is no recognition of roles with accountability for certain duties, powers or functions. Privacy issues are addressed reactively, on a case-by-case basis.	The MPO has delegated duties, powers, or functions but has not documented the delegation. There is informal recognition of roles with accountability for certain duties, powers or functions.	The MPO has delegated duties, powers, or functions to certain roles (e.g. Privacy Analyst) and has documented the delegation. The delegation documentation is maintained and current.	The MPO monitors all delegated duties, powers and functions.	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 by the MPO, where appropriate, and have been reviewed by CIRMO.	No documented Ministry-specific privacy policies and procedures exist, where appropriate. Privacy-related practices across the Ministry are variable and reactive.	Ministry-specific privacy policies and procedures are in place where appropriate but have not been documented. These practices are inconsistent across the Ministry.	Ministry-specific privacy policies and procedures have been developed and documented where appropriate. The policies have been reviewed by CIRMO.	Ministry-specific privacy policies and procedures 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 or changes in programs or information systems).	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include 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 (i.e. IM117) related to privacy. The training is scheduled, timely, consistent and periodically refreshed.	A large portion of Ministry employees have not completed mandatory privacy training. There is no process for monitoring training completion.	Mandatory privacy training has been completed by a majority of Ministry employees. There is a process for monitoring training completion but it is not documented.	Employees receive training when they are hired. Training is refreshed at least every two years. Training is scheduled, timely, consistent, monitored and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.). The process for monitoring training completion is documented.	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 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 and additional training/awareness activities (e.g. ministry-specific awareness days; engagement and/or awareness activities; increased attendance at PriSm and/or the Privacy and Security Conference). 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 Training** The MPO develops and delivers additional role-based privacy training (beyond IM117). Role-based privacy training is provided to employees using information systems that involve the handling of high-risk or sensitive personal information within the Ministry.	There is a general understanding of the need for role-based privacy training. Employees who require role-based privacy training are not identified. Role-based training is provided in an inconsistent and reactive manner.	Employees who require role-based privacy training are identified by the MPO. Training development and implementation is inconsistent. Completion of training is not tracked or documented.	The MPO has documented a process to identify employees who require role-based privacy training. The training is developed in consultation with CIRMO. The training is tracked and documented.	A Ministry-wide privacy awareness and training program, including any additional or role-based training, exists and the MPO takes a proactive approach to monitor these programs to ensure the training has been taken.	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 and additional training/awareness activities (e.g. ministry-specific awareness days; engagement and/or awareness activities; increased attendance at PriSm and/or the Privacy and Security Conference). 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.
3. Privacy Impact Assessments						

Privacy		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
3.1	**Processes for PIAs** The MPO has developed, maintained and reviewed internal processes (e.g. an PIA inventory) to ensure employee completion of PIAs. The MPO maintains a process to follow up on outstanding PIA items.	The MPO has not developed, maintained and reviewed internal processes to ensure employee completion of PIAs. PIAs are assessed in an inconsistent and reactive manner.	The MPO is aware of which PIAs have been completed and outstanding PIA items. Tracking is done informally, processes are not documented and may be inconsistently applied.	The MPO has developed, maintained and reviewed internal processes (e.g. an PIA inventory) to ensure employee completion of PIAs and follow up on outstanding PIA items.	The MPO monitors the compliance with internal processes to ensure the completion of PIAs.	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 PIA process. Employees inform the MPO of the effectiveness of PIA processes within the Ministry. Such information is analyzed and, where necessary, changes are made to improve effectiveness.
3.2	**Requirement to Complete PIAs** PIAs are conducted prior to the start of any proposed enactment, system, project, program or activity. PIAs are provided to CIRMO and CIRMO feedback is addressed before the PIA is finalized. Once finalized, PIAs are provided to CIRMO for retention and entry into the Personal Information Directory (PID).	PIAs are conducted prior to the start of any proposed enactment, system, project, program or activity, but are completed in an inconsistent and reactive manner. There is little to no communication with CIRMO during the development of PIAs. Some PIAs are provided to CIRMO for entry in to the PID.	PIAs are conducted prior to the start of any proposed enactment, system, project, program or activity. PIAs are provided to CIRMO and CIRMO feedback is addressed before the PIA is finalized. Once finalized, PIAs are provided to CIRMO for retention and entry into the PID.	There is a documented process to ensure that PIAs are conducted prior to the start of any proposed enactment, system, project, program or activity. PIAs are provided to CIRMO and CIRMO feedback is addressed before the PIA is finalized. Once finalized, PIAs are provided to CIRMO for retention and entry into the PID.	The MPO monitors the compliance with policies and procedures to ensure the completion of PIAs in a timely manner.	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	**Process for 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 completed 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 in an inconsistent and reactive manner.	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 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.	Any ISAs reported to CIRMO are done in an inconsistent and reactive 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 after finalization.	The MPO monitors the process to ensure the ISAs are reported to CIRMO.	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 in-progress and completed RAs. The MPO maintains 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 current 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 the RAs tracking process and ensures outstanding items are followed up in a timely manner.	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 requirements in agreements** There is a process in place for the monitoring of compliance with privacy requirements (e.g. section 30 of FOIPPA) outlined in agreements. If needed, there are adequate provisions in place to deal with issues of non-compliance.	There is no process in place for monitoring counterparty compliance with privacy requirements.	Certain privacy requirements have been communicated to counterparties; however, the requirements are not documented, and there is no formal process to monitor compliance.	There is a documented process for the monitoring of counterparty compliance with privacy requirements. If needed, there are adequate provisions in place to deal with issues of non-compliance.	Through review of prior agreements, the MPO assess 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 in all contracts that involve personal information in the custody or under the control of the public body. Amendments to Privacy Protection Schedules are approved by CIRMO.	Service provider contracts that involve personal information do not include the standard Privacy Protection Schedule.	Privacy Protection Schedules are generally included in contracts that involve personal information in the custody or under the control of the public body, but are incomplete or inconsistently applied.	There is a documented process to ensure Privacy Protection Schedules are included in contracts that involve personal information. Amendments to Privacy Protection Schedules are approved by CIRMO.	There is a monitoring process for contracts that involve 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 compliance of Privacy Protection Schedules requirement by the service providers and volunteers that have access to personal information. Such information is analyzed and, where necessary, corrective actions are made to existing and future contracts.
5.2	**Access to Personal Information by Service Providers and Volunteers** The MPO has been informed of all service providers and volunteers who have access to personal information (PI) within the Ministry's custody or control.	Service providers and volunteers who have access to personal information are not identified to the MPO.	Service providers and volunteers who have access to personal information are identified to the MPO in an inconsistent and reactive manner.	There is a documented process for informing the MPO of service providers and volunteers who have access to personal information.	There is a monitoring of the process for informing the MPO of service providers and volunteers who have access to personal information.	Through regular reviews 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.

Privacy		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
5.3	**Mandatory Service Provider Privacy Training** The MPO must ensure that service providers and volunteers who have access to personal information have completed prescribed privacy training related to the collection, use, disclosure, storage and destruction of personal information. This training must be completed prior to providing services.	There is not a general understanding of the need for service providers and volunteers who have access to personal information to complete privacy training.	There is a general understanding of the need for service providers and volunteers who have access to personal information to complete privacy training; however, these groups of employees are not identified. Training is provided in a inconsistent and reactive manner.	The MPO has a documented process to ensure that service providers and volunteers who have access to personal information have completed prescribed privacy training related to the collection, use, disclosure, storage and destruction of personal information. The training has been completed prior to providing services.	Training for service providers and volunteers is documented, scheduled, timely, consistent and is augmented by regular awareness activities (e.g. emails, posters, presentations, etc.).	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 and additional training/awareness activities (e.g. ministry-specific awareness days; engagement and/or awareness activities; increased attendance at PriSm and/or the Privacy and Security Conference). 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.
5.4	**Service Provider Compliance with the Privacy Protection Schedule** A process is in place for ensuring service provider compliance with Privacy Protection Schedules. If needed, there are adequate provisions in place to deal with issues of non-compliance.	There is no process in place for monitoring service provider compliance with the Privacy Protection Schedule.	The Privacy Protection Schedule requirements have been communicated to service providers; however, there is no formal process to monitor compliance.	There is a documented process for ensuring service provider compliance with Privacy Protection Schedules. If needed, there are adequate provisions in place to deal with issues of non-compliance.	There is a monitoring process for ensuring service provider compliance with Privacy Protection Schedules.	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** The MPO creates and maintains a Personal Information Inventory, and creates it within one year of the Personal Information Inventory Policy being published.	There is no process to track personal information in 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 process for creating and maintaining a Personal Information Inventory. The tracking of personal information in the Ministry is informal and not fully documented.	A documented process exists for creating and maintaining a Personal Information Inventory. A Personal Information Inventory is created within one year of the Personal Information Inventory Policy being published.	The MPO monitors the process for creating and maintaining 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** The MPO reports to CIRMO all Personal Information Banks (PIBs), as required.	There is no process for creating and reporting of PIBs to CIRMO.	Some PIBs created within the Ministry are reported to CIRMO. There is no documented process for determining how and when PIBs must be created or reported to CIRMO.	The MPO has a documented process for creating and reporting all PIBs to CIRMO that result from new enactments, systems, projects, programs or activities of the Ministry.	The MPO monitors the process for creating and reporting PIBs to CIRMO.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of the process for creating and reporting all PIBs to CIRMO. Such information is analyzed and, where necessary, changes are made to improve accuracy and effectiveness.
6.3	**Health Information Banks** *For the Ministry of Health:* The MPO for the Ministry of Health has a process in place for creating and reporting all Health Information Banks (HIBs) to CIRMO.	There is no process for creating and reporting of HIBs to CIRMO.	Some HIBs created within the Ministry are reported to CIRMO. There is no documented process for determining how and when HIBs must be created or reported to CIRMO.	The MPO in the Ministry of Health has a documented process for creating and reporting all HIBs to CIRMO.	The MPO monitors the process for creating and reporting HIBs to CIRMO.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of the process for creating and reporting all HIBs to CIRMO. Such information is analyzed and, where necessary, changes are made to improve accuracy and effectiveness.
6.4	**Monitoring of the Personal Information Directory (PID)** The MPO has a process 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 to the PID and accurately recorded.	The MPO has a documented process 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.	Through review of PID, the MPO assesses the effectiveness of the monitoring process.	Through quality reviews and other assessments of the PID, the MPO is informed of its effectiveness 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	**Process for Reporting Foreign Demands for Disclosure** A process is in place for reporting foreign demands for disclosure to CIRMO in the manner and form directed by CIRMO.	There is no process for reporting foreign demands for disclosure to CIRMO. Any reports to CIRMO are inconsistent and ad hoc.	Some foreign demands for disclosure are communicated to CIRMO; there is no documented reporting process.	A documented process, in compliance with FOIPPA, is in place for reporting foreign demands for disclosure to CIRMO.	A Ministry-wide awareness and training program exists for reporting all foreign demands for disclosure to CIRMO.	Through quality reviews and other assessments, the Ministry 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** Employees report actual or suspected incidents as per the Information Incident Management Process (IIMP). The Ministry follows CIRMO instructions and addresses recommendations as required.	Information incidents are reported in an inconsistent and informal manner. IIMP reporting requirements are followed inconsistently. Employees are not aware of the IIMP.	Information incidents are informally communicated and/or reported. IIMP reporting requirements are followed in most cases. Employees are generally aware of the IIMP.	Employees report actual or suspected incidents as per the IIMP. As part of the response to incidents, the Ministry follows CIRMO instructions and addresses recommendations as required.	A Ministry-wide awareness and training program exists for responding to information management incidents. Role-based training is provided for those involved in incident response processes. The Ministry takes a proactive approach to monitor these programs to ensure the training has been taken.	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 and additional training/awareness activities (e.g. ministry-specific awareness days; engagement and/or awareness activities; increased attendance at PriSm and/or the Privacy and Security Conference). 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.

Access to Information		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Governance and 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 employees. Ministry employees 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 employees to follow when responding to FOI requests. Employees are unaware of their obligations under FOIPPA, and do not respond to FOI requests as required.	Employees response to FOI requests are ad hoc and inconsistent. There are no documented processes or procedures for employees to follow, and employees' knowledge regarding their obligations under FOIPPA is inconsistent.	There are established processes and procedures in place for employees to follow in responding adequately and in a timely fashion to FOI requests. Employees 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	**Mandatory Employee Training** Employees have completed mandatory (i.e. IM117) training related to FOI/ Information Access. The training is scheduled, timely, consistent and periodically refreshed.	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. Training is refreshed at least every two years. Training is scheduled, timely, consistent, monitored and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.). The process for monitoring training completion is documented.	A Ministry-wide FOI awareness and training program exists and is monitored by the MPO. Training activities are monitored, regularly scheduled to provide timely and consistent FOI awareness (e.g., emails, posters, presentations, etc.) All employees are aware of, and understand, their responsibilities under FOIPPA.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion.
2.2	**Role-Based Training** Individuals have received additional, role-based Access training (beyond IM117) where appropriate (e.g. ministerial employees, 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 inconsistent and reactive manner.	Employees who require additional training relevant to their job are identified, but implementation is 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 FOI 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 Employees						
3.1	**Designated Employee** A ministry employee is designated as the person in charge of all FOI requests involving a Minister's office. This person is accountable for contacting all employees directly, in writing, with the details of the request and directing that employees search for responsive records and respond within a set time period.	A ministry employee has not been designated as the person in charge of all FOI requests involving a Minister's office.	Accountabilities have not been assigned to a designated employee for these processes, but this role is informally in place and supports FOI requests as they are received.	A designated employee has been assigned this role. Responsibilities are formally defined and documented.	Accountabilities are reviewed at least annually (or when there are significant changes to policy or regulatory requirements) and updated as required. Responsibilities are included in the designated employee's job description.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include analyzing and assessing the effectiveness of the designated employee accountabilities and where necessary, changes are made to existing and future accountabilities in order to improve compliance.
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 ministry and service provider 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 ministry or service provider non-compliance with timeliness and/or "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 inconsistency.	There is a documented process for the monitoring of ministry and service provider 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 ministry and service provider 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. This could include analyzing and assessing the effectiveness of the FOI monitoring process and where necessary, changes are made to existing and future processes in order to improve with timeliness and/or "duty to assist" requirements.

Access to Information		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Governance and 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 employees. Ministry employees 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 employees to follow when responding to FOI requests. Employees are unaware of their obligations under FOIPPA, and do not respond to FOI requests as required.	Employees response to FOI requests are ad hoc and inconsistent. There are no documented processes or procedures for employees to follow, and employees' knowledge regarding their obligations under FOIPPA is inconsistent.	There are established processes and procedures in place for employees to follow in responding adequately and in a timely fashion to FOI requests. Employees 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	**Mandatory Employee Training** Employees have completed mandatory (i.e. IM117) training related to FOI/ Information Access. The training is scheduled, timely, consistent and periodically refreshed.	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. Training is refreshed at least every two years. Training is scheduled, timely, consistent, monitored and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.). The process for monitoring training completion is documented.	A Ministry-wide FOI awareness and training program exists and is monitored by the MPO. Training activities are monitored, regularly scheduled to provide timely and consistent FOI awareness (e.g., emails, posters, presentations, etc.) All employees are aware of, and understand, their responsibilities under FOIPPA.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion.
2.2	**Role-Based Training** Individuals have received additional, role-based Access training (beyond IM117) where appropriate (e.g. ministerial employees, 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 inconsistent and reactive manner.	Employees who require additional training relevant to their job are identified, but implementation is 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 FOI 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 Employees						
3.1	**Designated Employee** A ministry employee is designated as the person in charge of all FOI requests involving a Minister's office. This person is accountable for contacting all employees directly, in writing, with the details of the request and directing that employees search for responsive records and respond within a set time period.	A ministry employee has not been designated as the person in charge of all FOI requests involving a Minister's office.	Accountabilities have not been assigned to a designated employee for these processes, but this role is informally in place and supports FOI requests as they are received.	A designated employee has been assigned this role. Responsibilities are formally defined and documented.	Accountabilities are reviewed at least annually (or when there are significant changes to policy or regulatory requirements) and updated as required. Responsibilities are included in the designated employee's job description.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include analyzing and assessing the effectiveness of the designated employee accountabilities and where necessary, changes are made to existing and future accountabilities in order to improve compliance.
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 ministry and service provider 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 ministry or service provider non-compliance with timeliness and/or "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 inconsistency.	There is a documented process for the monitoring of ministry and service provider 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 ministry and service provider 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. This could include analyzing and assessing the effectiveness of the FOI monitoring process and where necessary, changes are made to existing and future processes in order to improve with timeliness and/or "duty to assist" requirements.

Information Protection		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Governance and Accountability						
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). Responsibilities for the Information Security Program are documented and assigned. There is a clear understanding of respective roles and responsibilities, the names of such persons or groups and their responsibilities are communicated to internal employees.	No documented security policy or procedures exist and formal accountabilities for security have not been assigned. Security is managed in an ad-hoc and reactive manner. Respective roles and responsibilities have not been defined or communicated.	An Information Security Program based on ISP has been developed, but has not been documented, approved or implemented. Responsibilities for the Information Security Program have been assigned but have not been documented. There is a general understanding of respective roles and responsibilities, the names of such persons or groups and their responsibilities are informally communicated to internal employees.	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). Responsibilities for the Information Security Program are documented and assigned. There is a clear understanding of respective roles and responsibilities, the names of such persons or groups and their responsibilities are communicated to internal employees.	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 Accountabilities** The Ministry has articulated employees' responsibilities for information security. Ministry employees are required to sign off periodically (i.e. annually) to acknowledge their accountabilities with respect to information security.	The Ministry has articulated employees' responsibilities for information security. Ministry employees are not required to sign off periodically (i.e. annually) to acknowledge their accountabilities with respect to information security.	Employees' are generally aware of their responsibilities for information security. Ministry employees sign off inconsistently to acknowledge their accountabilities with respect to information security.	The Ministry has articulated employees' responsibilities for information security. All employees sign off periodically (i.e. annually) to acknowledge their accountabilities with respect to information security.	Accountabilities for information security are defined and regularly updated to reflect changes in Ministry programs and/or compliance requirements. Performance is monitored, reported regularly and there is a process to verify that all employees complete their periodic sign-off.	Level 4 has been attained and the Ministry has demonstrated additional leading practices. This could include incorporating information security accountabilities in annual employee performance reviews.
2. Education and Awareness						
2.1	**Mandatory Employee Training** Employees have completed mandatory (i.e. IM117) training related to the protection of government information. The training is scheduled, timely, consistent and periodically refreshed.	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. Training is refreshed at least every two years. Training is scheduled, timely, consistent, monitored and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.). The process for monitoring training completion is documented.	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.). Training is refreshed at least every two years and all Employees 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.
2.2	**Role-Based Training** A process is in place to develop and deliver additional training (beyond IM117) on information security to employees.	There is a general understanding of the need for role-based information security training; however, employees who require such training are not identified. Additional training is provided in an inconsistent and reactive manner.	Employees who require additional training relevant to their job are identified, but implementation is 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 security 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. Service Provider Management						
3.1	**External Parties** Assessment of risks from external party access to government information, information systems or information processing facilities are performed and appropriate security controls are 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 employees. 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.
3.2	**Monitoring Service Provider Compliance with information security Requirements** The ministry has a process to monitor service provider compliance with information security requirements. If needed, there are adequate provisions in place to deal with issues of non-compliance. This wording is also included in privacy 4.4 and 5.4	There is a lack of awareness of the need for contractors to comply with government information security requirements. There are inadequate mechanisms in place in contracts to ensure contractor compliance with information security requirements	There are adequate provisions in contracts to reinforce compliance with information security 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 security requirements. If needed, there are adequate provisions in place to deal with issues of non-compliance.	The ministry monitors service provider compliance with information security 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 security requirements. Such information is analyzed and, where necessary, changes are made to existing and future agreements in order to improve compliance.
4. Security Requirement and Classification						
4.1	**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.
4.2	**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.

Information Protection		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
4.3	**Protection Against Malicious Code** There is 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.
4.4	**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.
5. User Access Management						
5.1	**Access Control** Access control processes are in place covering the full range of access management for employees and service providers (granting, reviewing, removing, changing, etc.).	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 for employees and service providers (granting, reviewing, removing, changing, etc.).	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.
5.2	**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.
5.3	**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 inconsistent 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. Employees 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.
6. Asset Management, Protection and BCP						
6.1	**Business Continuity Management** Business continuity management processes and plans have been developed tested, maintained, updated and they include provisions to maintain security and information security 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 security.	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.
6.2	**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.
6.3	**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.
6.4	**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. Portable/media devices comply with OCIO standards with controls appropriate for the sensitivity of the data they contain.	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.

2019 Practice Review Framework

Criteria

Domain	# of Assessment Criteria
Privacy	23
Records Management	14
Information Access	6
Information Protection	17
	60

NOTE: certain criteria relate to requirements that are not yet in force. Employees 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
CPPM 12	Core Policy and Procedures Manual 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

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
1	Governance and Accountability				
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.	The responsibilities of the MPO have been documented and included in the MPO's job description.	What This Means: Responsibilities of the MPO are documented. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**
1.2	**Deputy Delegation of Duties** If the Deputy Minister has delegated any duties, powers or functions, a FOIPPA Delegation Instrument is in place, maintained and communicated to CIRMO by the MPO.	The Deputy Minister has delegated duties, powers, or functions to certain roles (e.g. MPO) and has used a FOIPPA Delegation Instrument. The FOIPPA Delegation Instrument is maintained and communicated to CIRMO by the MPO.	What This Means: The ministry maintains a copy of its FOIPPA delegation instrument and communicates changes to CIRMO. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**
1.3	**MPO Delegation of Duties** If the MPO has delegated any duties, powers, or functions, the delegation is documented and current. The MPO remains accountable as the single point-of-contact for CIRMO.	The MPO has delegated duties, powers, or functions to certain roles (e.g. Privacy Analyst) and has documented the delegation. The delegation documentation is maintained and current.	What This Means: If the MPO has delegated any accountabilities or responsibilities under PMAP, the delegation been documented. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
1.4	**Privacy Policies/Procedures** Ministry-specific privacy policies and procedures, incorporating Ministry-specific privacy requirements, have been developed and deployed by the MPO, where appropriate, and have been reviewed by CIRMO.	Ministry-specific privacy policies and procedures have been developed and documented where appropriate. The policies have been reviewed by CIRMO.	What This Means: If the ministry has any ministry-specific privacy policies (beyond PMAP), the policies have been reviewed by CIRMO and communicated to employees. Who To Ask: The MPO, managers and employees.	**MPO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
2	**Education and Awareness**				
2.1	**Mandatory Employee Training** Employees have completed mandatory training (i.e. IM117) related to privacy. The training is scheduled, timely, consistent and periodically refreshed.	Employees receive training when they are hired. Training is refreshed at least every two years. Training is scheduled, timely, consistent, monitored and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.). The process for monitoring training completion is documented.	What This Means: The ministry ensures that IM 117 training is provided and tracked for new and existing employees. Who To Ask: The MPO, managers, staff.	**MPO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
2.2	**Role-Based Training** The MPO develops and delivers additional role-based privacy training (beyond IM117). Role-based privacy training is provided to employees using information systems that involve the handling of high-risk or sensitive personal information within the Ministry.	The MPO has documented a process to identify employees who require role-based privacy training. The training is developed in consultation with CIRMO. The training is tracked and documented.	What This Means: If employees require additional privacy training, the training is developed in consultation with CIRMO, provided to appropriate employees and tracked. Who To Ask: The MPO, managers, staff	**MPO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
3	**Privacy Impact Assessments**				
3.1	**Processes for PIAs** The MPO has developed, maintained and reviewed internal processes (e.g. an PIA inventory) to ensure employee completion of PIAs. The MPO maintains a process to follow up on outstanding PIA items.	The MPO has developed, maintained and reviewed internal processes (e.g. an PIA inventory) to ensure employee completion of PIAs and follow up on outstanding PIA items.	What This Means: The MPO has developed a process that ensures completion and tracking of ministry PIAs. Who To Ask: The MPO, managers,staff	**MPO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
3.2	**Requirement to Complete PIAs** PIAs are conducted prior to the start of any proposed enactment, system, project, program or activity. PIAs are provided to CIRMO and CIRMO feedback is addressed before the PIA is finalized. Once finalized, PIAs are provided to CIRMO for retention and entry into the Personal Information Directory (PID).	There is a documented process to ensure that PIAs are conducted prior to the start of any proposed enactment, system, project, program or activity. PIAs are provided to CIRMO and CIRMO feedback is addressed before the PIA is finalized. Once finalized, PIAs are provided to CIRMO for retention and entry into the PID.	What This Means: There is a documented process to ensure that PIAs are conducted where appropriate, provided to CIRMO for review and retention, and are entered into the PID. Who To Ask: The MPO, managers and employees.	**MPO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
4	Agreements				
4.1	**Process for 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 completed 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 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.	What This Means: The MPO collaborates with branches to ensure that agreements are completed as required. Who To Ask: The MPO, managers and employees.	**MPO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
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 a documented process to ensure that ISAs are reported to CIRMO for entry into the PID after finalization.	What This Means: The MPO has a documented process that ensures that ISAs are reported to CIRMO for entry into the PID. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**
4.3	**Inventory of all Research Agreements** The MPO has a current inventory of all in-progress and completed RAs. The MPO maintains a process to follow up on outstanding items.	The MPO has a current inventory to track which RAs are completed and in progress. The MPO has established a documented process to follow up on outstanding items.	What This Means: The MPO maintains an inventory to track completed and in-progress research agreements. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**
4.4	**Monitoring compliance with privacy requirements in agreements** There is a process in place for the monitoring of compliance with privacy requirements (e.g. section 30 of FOIPPA) outlined in agreements. If needed, there are adequate provisions in place to deal with issues of non-compliance.	There is a documented process for the monitoring of counterparty compliance with privacy requirements. If needed, there are adequate provisions in place to deal with issues of non-compliance.	What This Means: The ministry monitors compliance of privacy requirements outlined in agreements. Who To Ask: The MPO and managers.	**MPO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
5	**Service Provider Management**				

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
5.1	**Privacy Protection Schedules** Privacy Protection Schedules are included in all contracts that involve personal information in the custody or under the control of the public body. Amendments to Privacy Protection Schedules are approved by CIRMO.	There is a documented process to ensure Privacy Protection Schedules are included in contracts that involve personal information. Amendments to Privacy Protection Schedules are approved by CIRMO.	What This Means: The ministry ensures that PPSs are included in all contracts that involve personal information and the MPO is advised of all such contracts. Who To Ask: Managers/contract managers.	**MPO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
5.2	**Access to Personal Information by Service Providers and Volunteers** The MPO has been informed of all service providers and volunteers who have access to personal information (PI) within the Ministry's custody or control.	There is a documented process for informing the MPO of service providers and volunteers who have access to personal information.	What This Means: The ministry informs the MPO of service providers and volunteers who have access to personal information. Who To Ask: The MPO and managers/contract managers.	**MPO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
5.3	**Mandatory Service Provider Privacy Training** The MPO must ensure that service providers and volunteers who have access to personal information have completed prescribed privacy training related to the collection, use, disclosure, storage and destruction of personal information. This training must be completed prior to providing services.	The MPO has a documented process to ensure that service providers and volunteers who have access to personal information have completed prescribed privacy training related to the collection, use, disclosure, storage and destruction of personal information. The training has been completed prior to providing services.	What This Means: The MPO maintains a documented process that confirms service providers and volunteers have had the mandatory privacy training prior to providing services. Who To Ask: MPO,managers/contract managers.	**MPO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
5.4	**Service Provider Compliance with the Privacy Protection Schedule** A process is in place for ensuring service provider compliance with Privacy Protection Schedules. If needed, there are adequate provisions in place to deal with issues of non-compliance.	There is a documented process for ensuring service provider compliance with Privacy Protection Schedules. If needed, there are adequate provisions in place to deal with issues of non-compliance.	What This Means: The ministry maintains a process to monitor service provider compliance with privacy requirements outlined in contracts. Who To Ask: Managers/contract managers.	**MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
6	**Personal Information Inventory**				

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
6.1	**Create and Maintain Personal Information Inventory** The MPO creates and maintains a Personal Information Inventory, and creates it within one year of the Personal Information Inventory Policy being published.	A documented process exists for creating and maintaining a Personal Information Inventory. A Personal Information Inventory is created within one year of the Personal Information Inventory Policy being published.	NA The PII does not yet exist.	NA	NA
6.2	**Reporting to CIRMO** The MPO reports to CIRMO all Personal Information Banks (PIBs), as required.	The MPO has a documented process for creating and reporting all PIBs to CIRMO that result from new enactments, systems, projects, programs or activities of the Ministry.	What This Means: The MPO maintains a process to report new ministry PIBs to CIRMO. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**
6.3	**Health Information Banks** *For the Ministry of Health:* The MPO for the Ministry of Health has a process in place for creating and reporting all Health Information Banks (HIBs) to CIRMO.	The MPO in the Ministry of Health has a documented process for creating and reporting all HIBs to CIRMO.	What This Means: The Ministry of Health MPO maintains a process to report new ministry HIBs to CIRMO. Who To Ask: The MPO for Ministry of Health.	**MPO** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
6.4	**Monitoring of the Personal Information Directory (PID)** The MPO has a process 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.	The MPO has a documented process 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.	What This Means: The MPO periodically reviews the PID to ensure ministry information is accurate and updated as needed. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**
7	**Foreign Demands for Disclosure**				
7.1	**Process for Reporting Foreign Demands for Disclosure** A process is in place for reporting foreign demands for disclosure to CIRMO in the manner and form directed by CIRMO.	A documented process, in compliance with FOIPPA, is in place for reporting foreign demands for disclosure to CIRMO.	What This Means: When ministries receive foreign demands (i.e. an order, demand or request from an authority outside of Canada for the unauthorized disclosure of personal information), the demands are reported to CIRMO. Who To Ask: The MPO, managers and employees.	**MPO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
8	**Information Incident Management**				

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
8.1	**Information Incident Management** Employees report actual or suspected incidents as per the Information Incident Management Process (IIMP). The Ministry follows CIRMO instructions and addresses recommendations as required.	Employees report actual or suspected incidents as per the IIMP. As part of the response to incidents, the Ministry follows CIRMO instructions and addresses recommendations as required.	What This Means: Ministry employees know how to identify and report information incidents. The ministry addresses CIRMO recommendations arising from information incidents. Who To Ask: Managers and employees.	**MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
8.2	**Information Incident Tracking** The ministry regularly and consistently tracks key information about information incidents within their responsibility.	The ministry regularly and consistently tracks key information about information incidents within their responsibility.	What This Means: The ministry retains summary information regarding its information incidents. Potential information to track: breach category, party responsible, identification of PI, notification date, and OCIO file number. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Records Management			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
1	Governance and Accountability				
1.1	**Records Management Accountabilities** The Ministry has articulated employees' responsibilities for records management, including documenting government decisions, and business areas have clearly assigned accountabilities across the Ministry with additional role specific records management duties, as appropriate. There is a clear understanding of respective roles and responsibilities, the names of such persons or groups and their responsibilities are communicated to internal employees	Defined roles and responsibilities have been developed and employees are aware of and understand their records management and documenting government decisions responsibilities. The Ministry is aware of and work collaboratively with the Government Records Service.	What This Means: Ministry employees are aware of and understand their records management responsibilities. Employees utilize services provided by GRS (e.g. offsiting, records management enquiries, training, etc.). Who To Ask: RO, managers and employees.	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
1.2	**Records Management Policies/Procedures** The Ministry implements records management policies and/or procedures provided by GRS, including documenting government decisions.The Guideline and Directive on documenting government decisions have been formally shared and their importance	The Ministry implements records management policies and/or procedures provided by GRS, including documenting government decisions. The Guideline and Directive on documenting government decisions have been formally shared and their importance	What This Means: Your ministry manages records in accordance with GRS' direction, including the requirement to document goverment decisions. Who To Ask:	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or	**Document Name:** **Location:**
2	Education and Awareness				

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Records Management			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
2.2	**Role-Based Training** Employees have received additional, role-based records management training (beyond IM117) where appropriate, and relevant Ministry employees have undergone training on the creation and maintenance of adequate records of government decisions, and documenting government decisions.	There is a documented process in place to identify Ministry employees who require additional training. All additional training is scheduled and delivered in a timely and consistent manner. Employees have undertaken additional training on the creation and maintenance of adequate records of government decisions in accordance to the Directive CRO 01-2019, Guidelines on	What This Means: If employees require additional records management training, the training is provided to appropriate employees. Who To Ask: RO, managers and employees.	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
3	**Records Classification and Information Schedules**				
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.	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.	What This Means: Your records must be organized or 'classified' by business function and in such a way that you can find them. These processes are documented, understood and followed by employees. Who To Ask: RO, managers and employees.	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Records Management			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
3.2	**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**.**	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.	What This Means: Ministry-specific records schedules (i.e. ORCS) are developed and updated when necessary. The Ministry is responsible for initiating this process with GRS. Who To Ask: RO, managers and employees.	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
4	**Digitization Requirements**				
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 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.	NA The “digitization” requirements in section 9 of the IMA are not yet in force.	NA	NA

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Records Management			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
4.2	**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.	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.	What This Means: Ministry records must be exportable (transferrable) to the digital archives. Who To Ask: RO and managers.	**RO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
5	**Records Retention, Maintenance and Disposition**				
5.1	**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.	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.	What This Means: The ministry offsites and/or destroys eligible records as appropriate. The ministry has processes to place holds on records responsive to FOI or legal requests. Who To Ask: RO, managers and employees	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Records Management			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
5.2	**Records Transfers to IMA Bodies** The Ministry has 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 and for monitoring of such transfers have been documented and implemented.	What This Means: Legal custody of records is transferred and documented when ministries reorganize (i.e. transfer or end functions or programs). The ministry is responsible for notifying GRS when ministry reorganizations occur, as GRS maintains the system in which legal custody of records is tracked. Who To Ask: RO and managers.	**RO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
5.3	**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 have been documented. Legal instruments and associated processes have also been defined and implemented where appropriate.	What This Means: The ministry must use an appropriate legal instrument (contract, legislation, etc) when transferring records to a non-IMA body, and must advise GRS of all transfers. Who To Ask: RO and managers	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Records Management			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
5.4	**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.	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.	What This Means: The ministry ensures that onsite physical records are appropriately secured based on level of information sensitivity. When records are offsited, access lists for records in offsite are updated when appropriate (e.g. when authorized employees retire, if legal custody of records is transferred, etc.). Who To Ask: RO, managers and employees.	**RO** - Yes or No **MGR** - Yes or No **EMP**- Yes or No	**Document Name:** **Location:**
6	**Recordkeeping Systems and Inventories**				
6.1	**Manage Information in Recordkeeping Systems** The Ministry manages government information through its lifecycle using recordkeeping systems as appropriate. Systems are used to meet records management requirements, including schedules as mandated in the *Information Management Act* and ensuring records capture the Ministry's documenting government decisions requirements, are preserved and accessible as required and appropriate.	The Ministry has established procedures and communicated to employees the processes needed to manage information appropriately in recordkeeping systems. Ministry records, including records documenting government decisions, are managed throughout their lifecycle and information schedules are applied, but disposition may not be consistently performed.	What This Means: Employees manage ministry records in appropriate record keeping systems (e.g. systems that have logical naming conventions, preserve records and their accessibility, protect against unauthorized access, and permit the retention requirements to be applied accurately). Who To Ask: RO, managers and employees.	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Records Management			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
6.2	**Inventory of Ministry Systems and Repositories** The Ministry maintains an inventory of ministry systems and repositories that manage and/or store government information.	A documented procedure is in place for the creation and maintenance of an inventory of systems and repositories, and an up-to-date inventory is in place.	What This Means: The ministry is aware of all the locations where its information is stored. Who To Ask: Managers and MISO.	**MGR** - Yes or No **MISO** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
	Access to Information		What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
1	Governance and 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 employees. Ministry employees 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 established processes and procedures in place for employees to follow in responding adequately and in a timely fashion to FOI requests. Employees are aware of their obligations under FOIPPA to conduct adequate searches for responsive records and consistently do so in a timely fashion.	What This Means: Employees know their responsibilities with respect to FOI (e.g. conducting thorough records searches). Processes are in place to ensure adequate and timely responses to FOI requests. Who To Ask: FOI Coordinator, managers and employees..	**FOI** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
2	Education and Awareness				
2.2	**Role-Based Training** Individuals have received additional, role-based Access training (beyond IM117) where appropriate (e.g. ministerial employees, FOI co-ordinators).	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.	What This Means: If employees require additional FOI training, the training is provided to appropriate employees. Who To Ask: FOI Coordinator,managers and employees.	**FOI** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
3	Minister's Offices & Ministerial Employees				
3.1	**Designated Employee** A ministry employee is designated as the person in charge of all FOI requests involving a Minister's office. This person is accountable for contacting all employees directly, in writing, with the details of the request and directing that employees search for responsive records and respond within a set time period.	A designated employee has been assigned this role. Responsibilities are formally defined and documented.	What This Means: The ministry has designated an employee as the person in charge of all FOI requests involving a Minister's office. Who To Ask: FOI Coordinator.	**FOI** - Yes or No	**Document Name:** **Location:**
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 ministry and service provider compliance with timeliness and/or "duty to assist" requirements	There is a documented process for the monitoring of ministry and service provider 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".	What This Means: The ministry is aware monitors the timeliness and completion of all FOI requests. An escalation process exists for tineliness or "duty to assist" issues. Who To Ask: FOI Coordinator and manager.	**FOI** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Information Protection			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
1	**Governance and Accountability**				
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). Responsibilities for the Information Security Program are documented and assigned. There is a clear understanding of respective roles and	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). Responsibilities for the Information Security Program are documented and assigned. There is a clear understanding	What This Means: The ministry has implemented an Information Security Program. Information security responsibilties within the ministry have been defined, documented and communicated to appropriate employees. Who To Ask: MISO.	**MISO** - Yes or No	**Document Name:** **Location:**
1.2	**Employee Accountabilities** The Ministry has articulated employees' responsibilities for information security. Ministry employees are required to sign off periodically (i.e. annually) to acknowledge their accountabilities with respect to information security.	The Ministry has articulated employees' responsibilities for information security. All employees sign off periodically (i.e. annually) to acknowledge their accountabilities with respect to information security.	What This Means: Employees have been informed of information security policies and procedures. Who To Ask: Managers and employees.	**MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
2	**Education and Awareness**				
2.2	**Role-Based Training** A process is in place to develop and deliver additional training (beyond IM117) on information security to employees.	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.	What This Means: If employees require additional information protection training, the training is provided to appropriate employees. Who To Ask: MISO, managers and employees.	**MISO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
3	**Service Provider Management**				
3.1	**External Parties** Assessment of risks from external party access to government information, information systems or information processing facilities are performed and appropriate security controls are implemented prior to granting access.	A documented risk assessment process exists and is communicated to Ministry employees. Reviews are conducted for all external party access.	What This Means: The ministry has a documented risk assessment process for providing access to external parties. Risk assessments are completed where appropriate. Who To Ask: MISO and managers.	**MISO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
3.2	**Monitoring Service Provider Compliance with information security Requirements** The ministry has a process to monitor service provider compliance with information security requirements. If needed, there are adequate provisions in place to deal with issues of non-compliance. This wording is also included in privacy 4.4 and 5.4	There is a documented process for the monitoring of service provider compliance with information security requirements. If needed, there are adequate provisions in place to deal with issues of non-compliance.	What This Means: The ministry maintains a process to monitor service provider compliance with security requirements outlined in contracts. Who To Ask: The MISO and managers/contract managers.	**MISO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
4	**Security Requirement and Classification**				
4.1	**Security Classification** Records are organized so that security classifications can be applied to protect different classes of information based on their sensitivity.	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.	What This Means: The ministry has applied security classfications to its information. Who To Ask: MISO.	**MISO** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Information Protection			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
4.2	**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.	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.	What This Means: There is a documented process to ensure that ISRAs are conducted where appropriate (i.e. for new and updated systems). Who To Ask: MISO.	**MISO** - Yes or No	**Document Name:** **Location:**
4.3	**Protection Against Malicious Code** There an established process in place to prevent, detect, and resolve malicious code infections on information systems and infrastructure.	Processes related to malicious code are defined and implemented.	What This Means: Employees are aware of procedures to prevent malicious code infections (e.g. supervisor approval is required to download new software or applications, do not click suspicious links, etc.). There is a documented procedure for detecting and resolving infections. Who To Ask: The MISO, managers and employees.	**MISO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
4.4	**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	Vulnerability assessments are planned and conducted on a regular basis (based on risk). Vulnerabilities are risk ranked and remediated in priority order.	What This Means: The ministry has identified its critical systems and has a documented process to identify, assess, and respond to vulnerabilities within these systems. Who To Ask: MISO.	**MISO** - Yes or No	**Document Name:** **Location:**
5	**User Access Management**				
5.1	**Access Control** Access control processes are in place covering the full range of access management for employees and service providers (granting, reviewing, removing, changing, etc.).	Documented access control processes are in place covering the full range of access management for employees and service providers (granting, reviewing, removing, changing, etc.).	What This Means: The ministry has a documented process for providing, updating and removing employee and service provider access to systems. Who To Ask: MISO and managers.	**MISO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
5.2	**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.	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.	What This Means: The ministry has identified its critical systems and implemented logging capabilities for these systems. The logs are monitored. Logs are secured and accessed by authorized employees only. Who To Ask: MISO and managers.	**MISO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
5.3	**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 are in place for user responsibilities and access. Employees are aware of and adheres to the clean desk policy and the need to protect unattended equipment and access to government information.	What This Means: Employees have been informed of their responsibilities to prevent unathorized access to government information. (i.e. clean desk, do not leave equipment unattended, do not share passwords, lock screens, do not share confidential information, etc.). Who To Ask: The MISO, managers and employees.	**MISO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Information Protection			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
6	**Asset Management, Protection and BCP**				
6.1	**Business Continuity Management** Business continuity management processes and plans have been developed tested, maintained, updated and they include provisions to maintain security and information security in the case of an incident.	A documented business continuity plan exists. The plan includes an assessment of risk and information sensitivity and incorporates appropriate controls to address information security.	What This Means: The ministry has developed a BCP that includes controls addressing information security during incidents. Disaster Recovery Plans have been created for critical systems. Who To Ask: MISO.	**MISO** - Yes or No	**Document Name:** **Location:**
6.2	**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.	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.	What This Means: The ministry maintains an inventory of government information systems and mobile devices. Who To Ask: MISO and manager.	**MISO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
6.3	**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.	Controls are documented regarding equipment protection, including asset disposal.	What This Means: The ministry has a documented process to ensure the removal of government information from devices that are no longer in use. Who To Ask: MISO and manager.	**MISO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
6.4	**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.	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.	What This Means: The ministry maintains an portable media inventory and approval process. A documented process in place to ensure portable media devices are used according to OCIO standards. Who To Ask: The MISO, managers and employees.	**MISO** - Yes or No **MGR** - Yes **EMP** - Yes	**Document Name:** **Location:**

Term	Defintion
CIRMO	Corporate Information Records Management Office
Delegation Instrument	A delegation matrix used by leaders to aid in the decision as to which tasks to delegate and which to retain
DGD	Documenting Government Decisions
Duty to Assist	The head of a public body must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely
FOI	Freedom of Information
FOIPPA	Freedom of Information and Privacy Protection Act
GRS	Government Records Service
HIB	Health Information Bank
IIMP	Information Incident Management Process
IM117	Mandatory IM training for all government employees
IMA	Information Management Act
IMPR	Information Management Practice Review
ISA	Information Sharing Agreement
ISP	Information Security Policy (government-wide) Information Security Program (Ministry-specific)
Legal Instrument	Is any formally executed written document that can be formally attributed to its author, records and formally expresses a legally enforceable act, process, or contractual duty, obligation, or right, and therefore evidences that act, process, or agreement.
MISO	Ministry Information Security Officer
MPO	Ministry Privacy Officer
OCIO	Office of the Chief Information Officer
PI	Personal Information
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
PID	Personal Information Directory
PII	Personal Information Inventory Policy
PMAP	Privacy, Management and Accountability Policy
PPS	Privacy Protection Schedules
RM	Records Management
RO	Records Officer
Service Providers	A person retained under a contract to perform services for a public body

Records Management

1 - initial
2 - repeatable
3 - defined
4 - managed
5 - optimaized

#	Criteria	
1. Governance and Accountability		
1.1	Records Management Accountabilities	s.13
1.2	Records Management Policies/Procedures	
2. Education and Awareness		
2.1	Mandatory Employee Training	
2.2	Role-Based Training	
3. Records Classification and Information Schedules		
3.1	Record Classification	
3.2	Information Schedule Development and Maintenance	
4. Digitization Requirements		
4.1	4.1 Digital Records	
4.2	Identify and Protect Digital Records Scheduled for Archiving	
5. Records Retention, Maintenance and Disposition		
5.1	Records Retention, Holds and Disposition	
5.2	Records Transfers to IMA Bodies	
5.3	~~Records Transfers to Non-IMA Bodies~~	
5.4	Manage Physical Records	
6. Recordkeeping Systems and Inventories		
6.1	Manage Information in Recordkeeping Systems	
6.2	Inventory of Ministry Systems and Repositories	

Page 053 of 444 to/à Page 058 of 444

Withheld pursuant to/removed as

s.13

Privacy		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Governance and Accountability						
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 inconsistent 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 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 FOIPPA Delegation Instrument is in place, maintained and communicated to CIRMO by the MPO.	The Deputy Minister has delegated duties, powers, or functions but has not used a delegation instrument. There is no recognition of roles with accountability for certain duties, powers or functions. Privacy issues are addressed reactively, on a case-by-case basis.	The Deputy Minister has delegated duties, powers, or functions but has not used a delegation instrument. There is informal recognition of roles with accountability for certain duties, powers or functions.	The Deputy Minister has delegated duties, powers, or functions to certain roles (e.g. MPO) and has used a FOIPPA Delegation Instrument. The FOIPPA Delegation Instrument is maintained and communicated to CIRMO by the MPO.	The MPO maintains and monitors all Ministry FOIPPA Delegation Instruments.	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, the delegation is documented and current. The MPO remains accountable as the single point-of-contact for CIRMO.	The MPO has delegated duties, powers, or functions but has not documented the delegation. There is no recognition of roles with accountability for certain duties, powers or functions. Privacy issues are addressed reactively, on a case-by-case basis.	The MPO has delegated duties, powers, or functions but has not documented the delegation. There is informal recognition of roles with accountability for certain duties, powers or functions.	The MPO has delegated duties, powers, or functions to certain roles (e.g. Privacy Analyst) and has documented the delegation. The delegation documentation is maintained and current.	The MPO monitors all delegated duties, powers and functions.	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 by the MPO, where appropriate, and have been reviewed by CIRMO.	No documented Ministry-specific privacy policies and procedures exist, where appropriate. Privacy-related practices across the Ministry are variable and reactive.	Ministry-specific privacy policies and procedures are in place where appropriate but have not been documented. These practices are inconsistent across the Ministry.	Ministry-specific privacy policies and procedures have been developed and documented where appropriate. The policies have been reviewed by CIRMO.	Ministry-specific privacy policies and procedures 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 or changes in programs or information systems).	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include 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 (i.e. IM117) related to privacy. The training is scheduled, timely, consistent and periodically refreshed.	A large portion of Ministry employees have not completed mandatory privacy training. There is no process for monitoring training completion.	Mandatory privacy training has been completed by a majority of Ministry employees. There is a process for monitoring training completion but it is not documented.	Employees receive training when they are hired. Training is refreshed at least every two years. Training is scheduled, timely, consistent, monitored and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.). The process for monitoring training completion is documented.	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 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 and additional training/awareness activities (e.g. ministry-specific awareness days; engagement and/or awareness activities; increased attendance at PriSm and/or the Privacy and Security Conference). 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 Training** The MPO develops and delivers additional role-based privacy training (beyond IM117). Role-based privacy training is provided to employees using information systems that involve the handling of high-risk or sensitive personal information within the Ministry.	There is a general understanding of the need for role-based privacy training. Employees who require role-based privacy training are not identified. Role-based training is provided in an inconsistent and reactive manner.	Employees who require role-based privacy training are identified by the MPO. Training development and implementation is inconsistent. Completion of training is not tracked or documented.	The MPO has documented a process to identify employees who require role-based privacy training. The training is developed in consultation with CIRMO. The training is tracked and documented.	A Ministry-wide privacy awareness and training program, including any additional or role-based training, exists and the MPO takes a proactive approach to monitor these programs to ensure the training has been taken.	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 and additional training/awareness activities (e.g. ministry-specific awareness days; engagement and/or awareness activities; increased attendance at PriSm and/or the Privacy and Security Conference). 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.
3. Privacy Impact Assessments						

Privacy		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
3.1	**Processes for PIAs** The MPO has developed, maintained and reviewed internal processes (e.g. an PIA inventory) to ensure employee completion of PIAs. The MPO maintains a process to follow up on outstanding PIA items.	The MPO has not developed, maintained and reviewed internal processes to ensure employee completion of PIAs. PIAs are assessed in an inconsistent and reactive manner.	The MPO is aware of which PIAs have been completed and outstanding PIA items. Tracking is done informally, processes are not documented and may be inconsistently applied.	The MPO has developed, maintained and reviewed internal processes (e.g. an PIA inventory) to ensure employee completion of PIAs and follow up on outstanding PIA items.	The MPO monitors the compliance with internal processes to ensure the completion of PIAs.	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 PIA process. Employees inform the MPO of the effectiveness of PIA processes within the Ministry. Such information is analyzed and, where necessary, changes are made to improve effectiveness.
3.2	**Requirement to Complete PIAs** PIAs are conducted prior to the start of any proposed enactment, system, project, program or activity. PIAs are provided to CIRMO and CIRMO feedback is addressed before the PIA is finalized. Once finalized, PIAs are provided to CIRMO for retention and entry into the Personal Information Directory (PID).	PIAs are conducted prior to the start of any proposed enactment, system, project, program or activity, but are completed in an inconsistent and reactive manner. There is little to no communication with CIRMO during the development of PIAs. Some PIAs are provided to CIRMO for entry in to the PID.	PIAs are conducted prior to the start of any proposed enactment, system, project, program or activity. PIAs are provided to CIRMO and CIRMO feedback is addressed before the PIA is finalized. Once finalized, PIAs are provided to CIRMO for retention and entry into the PID.	There is a documented process to ensure that PIAs are conducted prior to the start of any proposed enactment, system, project, program or activity. PIAs are provided to CIRMO and CIRMO feedback is addressed before the PIA is finalized. Once finalized, PIAs are provided to CIRMO for retention and entry into the PID.	The MPO monitors the compliance with policies and procedures to ensure the completion of PIAs in a timely manner.	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	**Process for 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 completed 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 in an inconsistent and reactive manner.	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 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.	Any ISAs reported to CIRMO are done in an inconsistent and reactive 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 after finalization.	The MPO monitors the process to ensure the ISAs are reported to CIRMO.	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 in-progress and completed RAs. The MPO maintains 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 current 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 the RAs tracking process and ensures outstanding items are followed up in a timely manner.	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 requirements in agreements** There is a process in place for the monitoring of compliance with privacy requirements (e.g. section 30 of FOIPPA) outlined in agreements. If needed, there are adequate provisions in place to deal with issues of non-compliance.	There is no process in place for monitoring counterparty compliance with privacy requirements.	Certain privacy requirements have been communicated to counterparties; however, the requirements are not documented, and there is no formal process to monitor compliance.	There is a documented process for the monitoring of counterparty compliance with privacy requirements. If needed, there are adequate provisions in place to deal with issues of non-compliance.	Through review of prior agreements, the MPO assess 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 in all contracts that involve personal information in the custody or under the control of the public body. Amendments to Privacy Protection Schedules are approved by CIRMO.	Service provider contracts that involve personal information do not include the standard Privacy Protection Schedule.	Privacy Protection Schedules are generally included in contracts that involve personal information in the custody or under the control of the public body, but are incomplete or inconsistently applied.	There is a documented process to ensure Privacy Protection Schedules are included in contracts that involve personal information. Amendments to Privacy Protection Schedules are approved by CIRMO.	There is a monitoring process for contracts that involve 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 compliance of Privacy Protection Schedules requirement by the service providers and volunteers that have access to personal information. Such information is analyzed and, where necessary, corrective actions are made to existing and future contracts.
5.2	**Access to Personal Information by Service Providers and Volunteers** The MPO has been informed of all service providers and volunteers who have access to personal information (PI) within the Ministry's custody or control.	Service providers and volunteers who have access to personal information are not identified to the MPO.	Service providers and volunteers who have access to personal information are identified to the MPO in an inconsistent and reactive manner.	There is a documented process for informing the MPO of service providers and volunteers who have access to personal information.	There is a monitoring of the process for informing the MPO of service providers and volunteers who have access to personal information.	Through regular reviews 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.

Privacy		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
5.3	**Mandatory Service Provider Privacy Training** The MPO must ensure that service providers and volunteers who have access to personal information have completed prescribed privacy training related to the collection, use, disclosure, storage and destruction of personal information. This training must be completed prior to providing services.	There is not a general understanding of the need for service providers and volunteers who have access to personal information to complete privacy training.	There is a general understanding of the need for service providers and volunteers who have access to personal information to complete privacy training; however, these groups of employees are not identified. Training is provided in a inconsistent and reactive manner.	The MPO has a documented process to ensure that service providers and volunteers who have access to personal information have completed prescribed privacy training related to the collection, use, disclosure, storage and destruction of personal information. The training has been completed prior to providing services.	Training for service providers and volunteers is documented, scheduled, timely, consistent and is augmented by regular awareness activities (e.g. emails, posters, presentations, etc.).	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 and additional training/awareness activities (e.g. ministry-specific awareness days; engagement and/or awareness activities; increased attendance at PriSm and/or the Privacy and Security Conference). 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.
5.4	**Service Provider Compliance with the Privacy Protection Schedule** A process is in place for ensuring service provider compliance with Privacy Protection Schedules. If needed, there are adequate provisions in place to deal with issues of non-compliance.	There is no process in place for monitoring service provider compliance with the Privacy Protection Schedule.	The Privacy Protection Schedule requirements have been communicated to service providers; however, there is no formal process to monitor compliance.	There is a documented process for ensuring service provider compliance with Privacy Protection Schedules. If needed, there are adequate provisions in place to deal with issues of non-compliance.	There is a monitoring process for ensuring service provider compliance with Privacy Protection Schedules.	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** The MPO creates and maintains a Personal Information Inventory, and creates it within one year of the Personal Information Inventory Policy being published.	There is no process to track personal information in 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 process for creating and maintaining a Personal Information Inventory. The tracking of personal information in the Ministry is informal and not fully documented.	A documented process exists for creating and maintaining a Personal Information Inventory. A Personal Information Inventory is created within one year of the Personal Information Inventory Policy being published.	The MPO monitors the process for creating and maintaining 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** The MPO reports to CIRMO all Personal Information Banks (PIBs), as required.	There is no process for creating and reporting of PIBs to CIRMO.	Some PIBs created within the Ministry are reported to CIRMO. There is no documented process for determining how and when PIBs must be created or reported to CIRMO.	The MPO has a documented process for creating and reporting all PIBs to CIRMO that result from new enactments, systems, projects, programs or activities of the Ministry.	The MPO monitors the process for creating and reporting PIBs to CIRMO.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of the process for creating and reporting all PIBs to CIRMO. Such information is analyzed and, where necessary, changes are made to improve accuracy and effectiveness.
6.3	**Health Information Banks** *For the Ministry of Health:* The MPO for the Ministry of Health has a process in place for creating and reporting all Health Information Banks (HIBs) to CIRMO.	There is no process for creating and reporting of HIBs to CIRMO.	Some HIBs created within the Ministry are reported to CIRMO. There is no documented process for determining how and when HIBs must be created or reported to CIRMO.	The MPO in the Ministry of Health has a documented process for creating and reporting all HIBs to CIRMO.	The MPO monitors the process for creating and reporting HIBs to CIRMO.	Through quality reviews and other assessments, the MPO is informed of the effectiveness of the process for creating and reporting all HIBs to CIRMO. Such information is analyzed and, where necessary, changes are made to improve accuracy and effectiveness.
6.4	**Monitoring of the Personal Information Directory (PID)** The MPO has a process 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 to the PID and accurately recorded.	The MPO has a documented process 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.	Through review of PID, the MPO assesses the effectiveness of the monitoring process.	Through quality reviews and other assessments of the PID, the MPO is informed of its effectiveness 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	**Process for Reporting Foreign Demands for Disclosure** A process is in place for reporting foreign demands for disclosure to CIRMO in the manner and form directed by CIRMO.	There is no process for reporting foreign demands for disclosure to CIRMO. Any reports to CIRMO are inconsistent and ad hoc.	Some foreign demands for disclosure are communicated to CIRMO; there is no documented reporting process.	A documented process, in compliance with FOIPPA, is in place for reporting foreign demands for disclosure to CIRMO.	A Ministry-wide awareness and training program exists for reporting all foreign demands for disclosure to CIRMO.	Through quality reviews and other assessments, the Ministry 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** Employees report actual or suspected incidents as per the Information Incident Management Process (IIMP). The Ministry follows CIRMO instructions and addresses recommendations as required.	Information incidents are reported in an inconsistent and informal manner. IIMP reporting requirements are followed inconsistently. Employees are not aware of the IIMP.	Information incidents are informally communicated and/or reported. IIMP reporting requirements are followed in most cases. Employees are generally aware of the IIMP.	Employees report actual or suspected incidents as per the IIMP. As part of the response to incidents, the Ministry follows CIRMO instructions and addresses recommendations as required.	A Ministry-wide awareness and training program exists for responding to information management incidents. Role-based training is provided for those involved in incident response processes. The Ministry takes a proactive approach to monitor these programs to ensure the training has been taken.	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 and additional training/awareness activities (e.g. ministry-specific awareness days; engagement and/or awareness activities; increased attendance at PriSm and/or the Privacy and Security Conference). 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.

Access to Information		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Governance and 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 employees. Ministry employees 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 employees to follow when responding to FOI requests. Employees are unaware of their obligations under FOIPPA, and do not respond to FOI requests as required.	Employees response to FOI requests are ad hoc and inconsistent. There are no documented processes or procedures for employees to follow, and employees' knowledge regarding their obligations under FOIPPA is inconsistent.	There are established processes and procedures in place for employees to follow in responding adequately and in a timely fashion to FOI requests. Employees 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	**Mandatory Employee Training** Employees have completed mandatory (i.e. IM117) training related to FOI/ Information Access. The training is scheduled, timely, consistent and periodically refreshed.	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. Training is refreshed at least every two years. Training is scheduled, timely, consistent, monitored and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.). The process for monitoring training completion is documented.	A Ministry-wide FOI awareness and training program exists and is monitored by the MPO. Training activities are monitored, regularly scheduled to provide timely and consistent FOI awareness (e.g., emails, posters, presentations, etc.) All employees are aware of, and understand, their responsibilities under FOIPPA.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion.
2.2	**Role-Based Training** Individuals have received additional, role-based Access training (beyond IM117) where appropriate (e.g. ministerial employees, 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 inconsistent and reactive manner.	Employees who require additional training relevant to their job are identified, but implementation is 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 FOI 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 Employees						
3.1	**Designated Employee** A ministry employee is designated as the person in charge of all FOI requests involving a Minister's office. This person is accountable for contacting all employees directly, in writing, with the details of the request and directing that employees search for responsive records and respond within a set time period.	A ministry employee has not been designated as the person in charge of all FOI requests involving a Minister's office.	Accountabilities have not been assigned to a designated employee for these processes, but this role is informally in place and supports FOI requests as they are received.	A designated employee has been assigned this role. Responsibilities are formally defined and documented.	Accountabilities are reviewed at least annually (or when there are significant changes to policy or regulatory requirements) and updated as required. Responsibilities are included in the designated employee's job description.	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion. This could include analyzing and assessing the effectiveness of the designated employee accountabilities and where necessary, changes are made to existing and future accountabilities in order to improve compliance.
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 ministry and service provider 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 ministry or service provider non-compliance with timeliness and/or "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 inconsistency.	There is a documented process for the monitoring of ministry and service provider 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 ministry and service provider 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. This could include analyzing and assessing the effectiveness of the FOI monitoring process and where necessary, changes are made to existing and future processes in order to improve with timeliness and/or "duty to assist" requirements.

Information Protection		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Governance and Accountability						
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). Responsibilities for the Information Security Program are documented and assigned. There is a clear understanding of respective roles and responsibilities, the names of such persons or groups and their responsibilities are communicated to internal employees.	No documented security policy or procedures exist and formal accountabilities for security have not been assigned. Security is managed in an ad-hoc and reactive manner. Respective roles and responsibilities have not been defined or communicated.	An Information Security Program based on ISP has been developed, but has not been documented, approved or implemented. Responsibilities for the Information Security Program have been assigned but have not been documented. There is a general understanding of respective roles and responsibilities, the names of such persons or groups and their responsibilities are informally communicated to internal employees.	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). Responsibilities for the Information Security Program are documented and assigned. There is a clear understanding of respective roles and responsibilities, the names of such persons or groups and their responsibilities are communicated to internal employees.	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 Accountabilities** The Ministry has articulated employees' responsibilities for information security. Ministry employees are required to sign off periodically (i.e. annually) to acknowledge their accountabilities with respect to information security.	The Ministry has articulated employees' responsibilities for information security. Ministry employees are not required to sign off periodically (i.e. annually) to acknowledge their accountabilities with respect to information security.	Employees' are generally aware of their responsibilities for information security. Ministry employees sign off inconsistently to acknowledge their accountabilities with respect to information security.	The Ministry has articulated employees' responsibilities for information security. All employees sign off periodically (i.e. annually) to acknowledge their accountabilities with respect to information security.	Accountabilities for information security are defined and regularly updated to reflect changes in Ministry programs and/or compliance requirements. Performance is monitored, reported regularly and there is a process to verify that all employees complete their periodic sign-off.	Level 4 has been attained and the Ministry has demonstrated additional leading practices. This could include incorporating information security accountabilities in annual employee performance reviews.
2. Education and Awareness						
2.1	**Mandatory Employee Training** Employees have completed mandatory (i.e. IM117) training related to the protection of government information. The training is scheduled, timely, consistent and periodically refreshed.	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. Training is refreshed at least every two years. Training is scheduled, timely, consistent, monitored and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.). The process for monitoring training completion is documented.	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.). Training is refreshed at least every two years and all Employees 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.
2.2	**Role-Based Training** A process is in place to develop and deliver additional training (beyond IM117) on information security to employees.	There is a general understanding of the need for role-based information security training; however, employees who require such training are not identified. Additional training is provided in an inconsistent and reactive manner.	Employees who require additional training relevant to their job are identified, but implementation is 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 security 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. Service Provider Management						
3.1	**External Parties** Assessment of risks from external party access to government information, information systems or information processing facilities are performed and appropriate security controls are 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 employees. 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.
3.2	**Monitoring Service Provider Compliance with information security Requirements** The ministry has a process to monitor service provider compliance with information security requirements. If needed, there are adequate provisions in place to deal with issues of non-compliance. This wording is also included in privacy 4.4 and 5.4	There is a lack of awareness of the need for contractors to comply with government information security requirements. There are inadequate mechanisms in place in contracts to ensure contractor compliance with information security requirements	There are adequate provisions in contracts to reinforce compliance with information security 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 security requirements. If needed, there are adequate provisions in place to deal with issues of non-compliance.	The ministry monitors service provider compliance with information security 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 security requirements. Such information is analyzed and, where necessary, changes are made to existing and future agreements in order to improve compliance.
4. Security Requirement and Classification						
4.1	**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.
4.2	**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.

Information Protection		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
4.3	**Protection Against Malicious Code** There is 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.
4.4	**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.
5. User Access Management						
5.1	**Access Control** Access control processes are in place covering the full range of access management for employees and service providers (granting, reviewing, removing, changing, etc.).	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 for employees and service providers (granting, reviewing, removing, changing, etc.).	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.
5.2	**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.
5.3	**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 inconsistent 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. Employees 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.
6. Asset Management, Protection and BCP						
6.1	**Business Continuity Management** Business continuity management processes and plans have been developed tested, maintained, updated and they include provisions to maintain security and information security 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 security.	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.
6.2	**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.
6.3	**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.
6.4	**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. Portable/media devices comply with OCIO standards with controls appropriate for the sensitivity of the data they contain.	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.

2019 Practice Review Framework

Criteria

Domain	# of Assessment Criteria
Privacy	23
Records Management	14
Information Access	6
Information Protection	17
	60

NOTE: certain criteria relate to requirements that are not yet in force. Employees 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
CPPM 12	Core Policy and Procedures Manual 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

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
1	Governance and Accountability				
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.	The responsibilities of the MPO have been documented and included in the MPO's job description.	What This Means: Responsibilities of the MPO are documented. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**
1.2	**Deputy Delegation of Duties** If the Deputy Minister has delegated any duties, powers or functions, a FOIPPA Delegation Instrument is in place, maintained and communicated to CIRMO by the MPO.	The Deputy Minister has delegated duties, powers, or functions to certain roles (e.g. MPO) and has used a FOIPPA Delegation Instrument. The FOIPPA Delegation Instrument is maintained and communicated to CIRMO by the MPO.	What This Means: The ministry maintains a copy of its FOIPPA delegation instrument and communicates changes to CIRMO. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**
1.3	**MPO Delegation of Duties** If the MPO has delegated any duties, powers, or functions, the delegation is documented and current. The MPO remains accountable as the single point-of-contact for CIRMO.	The MPO has delegated duties, powers, or functions to certain roles (e.g. Privacy Analyst) and has documented the delegation. The delegation documentation is maintained and current.	What This Means: If the MPO has delegated any accountabilities or responsibilities under PMAP, the delegation been documented. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**
1.4	**Privacy Policies/Procedures** Ministry-specific privacy policies and procedures, incorporating Ministry-specific privacy requirements, have been developed and deployed by the MPO, where appropriate, and have been reviewed by CIRMO.	Ministry-specific privacy policies and procedures have been developed and documented where appropriate. The policies have been reviewed by CIRMO.	What This Means: If the ministry has any ministry-specific privacy policies (beyond PMAP), the policies have been reviewed by CIRMO and communicated to employees. Who To Ask: The MPO, managers and employees.	**MPO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
2	Education and Awareness				
2.1	**Mandatory Employee Training** Employees have completed mandatory training (i.e. IM117) related to privacy. The training is scheduled, timely, consistent and periodically refreshed.	Employees receive training when they are hired. Training is refreshed at least every two years. Training is scheduled, timely, consistent, monitored and is augmented by regular awareness activities (e.g., emails, posters, presentations, etc.). The process for monitoring training completion is documented.	What This Means: The ministry ensures that IM 117 training is provided and tracked for new and existing employees. Who To Ask: The MPO, managers, staff.	**MPO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
2.2	**Role-Based Training** The MPO develops and delivers additional role-based privacy training (beyond IM117). Role-based privacy training is provided to employees using information systems that involve the handling of high-risk or sensitive personal information within the Ministry.	The MPO has documented a process to identify employees who require role-based privacy training. The training is developed in consultation with CIRMO. The training is tracked and documented.	What This Means: If employees require additional privacy training, the training is developed in consultation with CIRMO, provided to appropriate employees and tracked. Who To Ask: The MPO, managers, staff	**MPO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
3	Privacy Impact Assessments				

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
3.1	**Processes for PIAs** The MPO has developed, maintained and reviewed internal processes (e.g. an PIA inventory) to ensure employee completion of PIAs. The MPO maintains a process to follow up on outstanding PIA items.	The MPO has developed, maintained and reviewed internal processes (e.g. an PIA inventory) to ensure employee completion of PIAs and follow up on outstanding PIA items.	What This Means: The MPO has developed a process that ensures completion and tracking of ministry PIAs. Who To Ask: The MPO, managers,staff	MPO - Yes or No MGR - Yes or No EMP - Yes or No	Document Name: Location:
3.2	**Requirement to Complete PIAs** PIAs are conducted prior to the start of any proposed enactment, system, project, program or activity. PIAs are provided to CIRMO and CIRMO feedback is addressed before the PIA is finalized. Once finalized, PIAs are provided to CIRMO for retention and entry into the Personal Information Directory (PID).	There is a documented process to ensure that PIAs are conducted prior to the start of any proposed enactment, system, project, program or activity. PIAs are provided to CIRMO and CIRMO feedback is addressed before the PIA is finalized. Once finalized, PIAs are provided to CIRMO for retention and entry into the PID.	What This Means: There is a documented process to ensure that PIAs are conducted where appropriate, provided to CIRMO for review and retention, and are entered into the PID. Who To Ask: The MPO, managers and employees.	MPO - Yes or No MGR - Yes or No EMP - Yes or No	Document Name: Location:
4	**Agreements**				
4.1	**Process for 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 completed 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 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.	What This Means: The MPO collaborates with branches to ensure that agreements are completed as required. Who To Ask: The MPO, managers and employees.	MPO - Yes or No MGR - Yes or No EMP - Yes or No	Document Name: Location:
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 a documented process to ensure that ISAs are reported to CIRMO for entry into the PID after finalization.	What This Means: The MPO has a documented process that ensures that ISAs are reported to CIRMO for entry into the PID. Who To Ask: The MPO.	MPO - Yes or No	Document Name: Location:
4.3	**Inventory of all Research Agreements** The MPO has a current inventory of all in-progress and completed RAs. The MPO maintains a process to follow up on outstanding items.	The MPO has a current inventory to track which RAs are completed and in progress. The MPO has established a documented process to follow up on outstanding items.	What This Means: The MPO maintains an inventory to track completed and in-progress research agreements. Who To Ask: The MPO.	MPO - Yes or No	Document Name: Location:
4.4	**Monitoring compliance with privacy requirements in agreements** There is a process in place for the monitoring of compliance with privacy requirements (e.g. section 30 of FOIPPA) outlined in agreements. If needed, there are adequate provisions in place to deal with issues of non-compliance.	There is a documented process for the monitoring of counterparty compliance with privacy requirements. If needed, there are adequate provisions in place to deal with issues of non-compliance.	What This Means: The ministry monitors compliance of privacy requirements outlined in agreements. Who To Ask: The MPO and managers.	MPO - Yes or No MGR - Yes or No	Document Name: Location:
5	**Service Provider Management**				

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
5.1	**Privacy Protection Schedules** Privacy Protection Schedules are included in all contracts that involve personal information in the custody or under the control of the public body. Amendments to Privacy Protection Schedules are approved by CIRMO.	There is a documented process to ensure Privacy Protection Schedules are included in contracts that involve personal information. Amendments to Privacy Protection Schedules are approved by CIRMO.	What This Means: The ministry ensures that PPSs are included in all contracts that involve personal information and the MPO is advised of all such contracts. Who To Ask: Managers/contract managers.	**MPO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
5.2	**Access to Personal Information by Service Providers and Volunteers** The MPO has been informed of all service providers and volunteers who have access to personal information (PI) within the Ministry's custody or control.	There is a documented process for informing the MPO of service providers and volunteers who have access to personal information.	What This Means: The ministry informs the MPO of service providers and volunteers who have access to personal information. Who To Ask: The MPO and managers/contract managers.	**MPO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
5.3	**Mandatory Service Provider Privacy Training** The MPO must ensure that service providers and volunteers who have access to personal information have completed prescribed privacy training related to the collection, use, disclosure, storage and destruction of personal information. This training must be completed prior to providing services.	The MPO has a documented process to ensure that service providers and volunteers who have access to personal information have completed prescribed privacy training related to the collection, use, disclosure, storage and destruction of personal information. The training has been completed prior to providing services.	What This Means: The MPO maintains a documented process that confirms service providers and volunteers have had the mandatory privacy training prior to providing services. Who To Ask: MPO,managers/contract managers.	**MPO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
5.4	**Service Provider Compliance with the Privacy Protection Schedule** A process is in place for ensuring service provider compliance with Privacy Protection Schedules. If needed, there are adequate provisions in place to deal with issues of non-compliance.	There is a documented process for ensuring service provider compliance with Privacy Protection Schedules. If needed, there are adequate provisions in place to deal with issues of non-compliance.	What This Means: The ministry maintains a process to monitor service provider compliance with privacy requirements outlined in contracts. Who To Ask: Managers/contract managers.	**MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
6	**Personal Information Inventory**				
6.1	**Create and Maintain Personal Information Inventory** The MPO creates and maintains a Personal Information Inventory, and creates it within one year of the Personal Information Inventory Policy being published.	A documented process exists for creating and maintaining a Personal Information Inventory. A Personal Information Inventory is created within one year of the Personal Information Inventory Policy being published.	NA The PII does not yet exist.	NA	NA
6.2	**Reporting to CIRMO** The MPO reports to CIRMO all Personal Information Banks (PIBs), as required.	The MPO has a documented process for creating and reporting all PIBs to CIRMO that result from new enactments, systems, projects, programs or activities of the Ministry.	What This Means: The MPO maintains a process to report new ministry PIBs to CIRMO. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documents
Privacy			What This Means and Who To Ask	If Y, Supporting Documents Required	Document Name and Location (Do Not Submit to IMPR)
6.3	**Health Information Banks** *For the Ministry of Health:* The MPO for the Ministry of Health has a process in place for creating and reporting all Health Information Banks (HIBs) to CIRMO.	The MPO in the Ministry of Health has a documented process for creating and reporting all HIBs to CIRMO.	What This Means: The Ministry of Health MPO maintains a process to report new ministry HIBs to CIRMO. Who To Ask: The MPO for Ministry of Health.	**MPO** - Yes or No	**Document Name:** **Location:**
6.4	**Monitoring of the Personal Information Directory (PID)** The MPO has a process 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.	The MPO has a documented process 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.	What This Means: The MPO periodically reviews the PID to ensure ministry information is accurate and updated as needed. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**
7	**Foreign Demands for Disclosure**				
7.1	**Process for Reporting Foreign Demands for Disclosure** A process is in place for reporting foreign demands for disclosure to CIRMO in the manner and form directed by CIRMO.	A documented process, in compliance with FOIPPA, is in place for reporting foreign demands for disclosure to CIRMO.	What This Means: When ministries receive foreign demands (i.e. an order, demand or request from an authority outside of Canada for the unauthorized disclosure of personal information), the demands are reported to CIRMO. Who To Ask: The MPO, managers and employees.	**MPO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
8	**Information Incident Management**				
8.1	**Information Incident Management** Employees report actual or suspected incidents as per the Information Incident Management Process (IIMP). The Ministry follows CIRMO instructions and addresses recommendations as required.	Employees report actual or suspected incidents as per the IIMP. As part of the response to incidents, the Ministry follows CIRMO instructions and addresses recommendations as required.	What This Means: Ministry employees know how to identify and report information incidents. The ministry addresses CIRMO recommendations arising from information incidents. Who To Ask: Managers and employees.	**MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
8.2	**Information Incident Tracking** The ministry regularly and consistently tracks key information about information incidents within their responsibility.	The ministry regularly and consistently tracks key information about information incidents within their responsibility.	What This Means: The ministry retains summary information regarding its information incidents. Potential information to track: breach category, party responsible, identification of PI, notification date, and OCIO file number. Who To Ask: The MPO.	**MPO** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Records Management			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
1	Governance and Accountability				
1.1	**Records Management Accountabilities** The Ministry has articulated employees' responsibilities for records management, including documenting government decisions, and business areas have clearly assigned accountabilities across the Ministry with additional role specific records management duties, as appropriate. There is a clear understanding of respective roles and responsibilities, the names of such persons or groups and their responsibilities are communicated to internal employees.	Defined roles and responsibilities have been developed and employees are aware of and understand their records management and documenting government decisions responsibilities. The Ministry is aware of and work collaboratively with the Government Records Service.	What This Means: Ministry employees are aware of and understand their records management responsibilities. Employees utilize services provided by GRS (e.g. offsiting, records management enquiries, training, etc.). Who To Ask: RO, managers and employees.	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
1.2	**Records Management Policies/Procedures** The Ministry implements records management policies and/or procedures provided by GRS, including documenting government decisions.The Guideline and Directive on documenting government decisions have been formally shared and their importance	The Ministry implements records management policies and/or procedures provided by GRS, including documenting government decisions. The Guideline and Directive on documenting government decisions have been formally shared and their importance	What This Means: Your ministry manages records in accordance with GRS' direction, including the requirement to document goverment decisions. Who To Ask:	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or	**Document Name:** **Location:**
2	Education and Awareness				
2.2	**Role-Based Training** Employees have received additional, role-based records management training (beyond IM117) where appropriate, and relevant Ministry employees have undergone training on the creation and maintenance of adequate records of government decisions, and documenting government decisions.	There is a documented process in place to identify Ministry employees who require additional training. All additional training is scheduled and delivered in a timely and consistent manner. Employees have undertaken additional training on the creation and maintenance of adequate records of government decisions in accordance to the Directive CRO 01-2019, Guidelines on	What This Means: If employees require additional records management training, the training is provided to appropriate employees. Who To Ask: RO, managers and employees.	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Records Management			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
3	**Records Classification and Information Schedules**				
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.	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.	What This Means: Your records must be organized or 'classified' by business function and in such a way that you can find them. These processes are documented, understood and followed by employees. Who To Ask: RO, managers and employees.	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
3.2	**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.	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.	What This Means: Ministry-specific records schedules (i.e. ORCS) are developed and updated when necessary. The Ministry is responsible for initiating this process with GRS. Who To Ask: RO, managers and employees.	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
4	**Digitization Requirements**				

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Records Management			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
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 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.	NA The "digitization" requirements in section 9 of the IMA are not yet in force.	NA	NA
4.2	**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.	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.	What This Means: Ministry records must be exportable (transferrable) to the digital archives. Who To Ask: RO and managers.	**RO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
5	**Records Retention, Maintenance and Disposition**				

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Records Management			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
5.1	**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.	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.	What This Means: The ministry offsites and/or destroys eligible records as appropriate. The ministry has processes to place holds on records responsive to FOI or legal requests. Who To Ask: RO, managers and employees	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
5.2	**Records Transfers to IMA Bodies** The Ministry has 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 and for monitoring of such transfers have been documented and implemented.	What This Means: Legal custody of records is transferred and documented when ministries reorganize (i.e. transfer or end functions or programs). The ministry is responsible for notifying GRS when ministry reorganizations occur, as GRS maintains the system in which legal custody of records is tracked. Who To Ask: RO and managers.	**RO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Records Management			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
5.3	**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 have been documented. Legal instruments and associated processes have also been defined and implemented where appropriate.	What This Means: The ministry must use an appropriate legal instrument (contract, legislation, etc) when transferring records to a non-IMA body, and must advise GRS of all transfers. Who To Ask: RO and managers	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
5.4	**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.	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.	What This Means: The ministry ensures that onsite physical records are appropriately secured based on level of information sensitivity. When records are offsited, access lists for records in offsite are updated when appropriate (e.g. when authorized employees retire, if legal custody of records is transferred, etc.). Who To Ask: RO, managers and employees.	**RO** - Yes or No **MGR** - Yes or No **EMP**- Yes or No	**Document Name:** **Location:**
6	**Recordkeeping Systems and Inventories**				

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Records Management			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
6.1	**Manage Information in Recordkeeping Systems** The Ministry manages government information through its lifecycle using recordkeeping systems as appropriate. Systems are used to meet records management requirements, including schedules as mandated in the *Information Management Act* and ensuring records capture the Ministry's documenting government decisions requirements, are preserved and accessible as required and appropriate.	The Ministry has established procedures and communicated to employees the processes needed to manage information appropriately in recordkeeping systems. Ministry records, including records documenting government decisions, are managed throughout their lifecycle and information schedules are applied, but disposition may not be consistently performed.	What This Means: Employees manage ministry records in appropriate record keeping systems (e.g. systems that have logical naming conventions, preserve records and their accessibility, protect against unauthorized access, and permit the retention requirements to be applied accurately). Who To Ask: RO, managers and employees.	**RO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
6.2	**Inventory of Ministry Systems and Repositories** The Ministry maintains an inventory of ministry systems and repositories that manage and/or store government information.	A documented procedure is in place for the creation and maintenance of an inventory of systems and repositories, and an up-to-date inventory is in place.	What This Means: The ministry is aware of all the locations where its information is stored. Who To Ask: Managers and MISO.	**MGR** - Yes or No **MISO** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Access to Information			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
1	Governance and 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 employees. Ministry employees 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 established processes and procedures in place for employees to follow in responding adequately and in a timely fashion to FOI requests. Employees are aware of their obligations under FOIPPA to conduct adequate searches for responsive records and consistently do so in a timely fashion.	What This Means: Employees know their responsibilities with respect to FOI (e.g. conducting thorough records searches). Processes are in place to ensure adequate and timely responses to FOI requests. Who To Ask: FOI Coordinator, managers and employees..	**FOI** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
2	Education and Awareness				
2.2	**Role-Based Training** Individuals have received additional, role-based Access training (beyond IM117) where appropriate (e.g. ministerial employees, FOI co-ordinators).	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.	What This Means: If employees require additional FOI training, the training is provided to appropriate employees. Who To Ask: FOI Coordinator,managers and employees.	**FOI** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
3	Minister's Offices & Ministerial Employees				
3.1	**Designated Employee** A ministry employee is designated as the person in charge of all FOI requests involving a Minister's office. This person is accountable for contacting all employees directly, in writing, with the details of the request and directing that employees search for responsive records and respond within a set time period.	A designated employee has been assigned this role. Responsibilities are formally defined and documented.	What This Means: The ministry has designated an employee as the person in charge of all FOI requests involving a Minister's office. Who To Ask: FOI Coordinator.	**FOI** - Yes or No	**Document Name:** **Location:**
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 ministry and service provider compliance with timeliness and/or "duty to assist" requirements	There is a documented process for the monitoring of ministry and service provider 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".	What This Means: The ministry is aware monitors the timeliness and completion of all FOI requests. An escalation process exists for tineliness or "duty to assist" issues. Who To Ask: FOI Coordinator and manager.	**FOI** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Information Protection			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
1	**Governance and Accountability**				
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). Responsibilities for the Information Security Program are documented and assigned. There is a clear understanding of respective roles and	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). Responsibilities for the Information Security Program are documented and assigned. There is a clear understanding of respective	What This Means: The ministry has implemented an Information Security Program. Information security responsibilties within the ministry have been defined, documented and communicated to appropriate employees. Who To Ask: MISO.	**MISO** - Yes or No	**Document Name:** **Location:**
1.2	**Employee Accountabilities** The Ministry has articulated employees' responsibilities for information security. Ministry employees are required to sign off periodically (i.e. annually) to acknowledge their accountabilities with respect to information security.	The Ministry has articulated employees' responsibilities for information security. All employees sign off periodically (i.e. annually) to acknowledge their accountabilities with respect to information security.	What This Means: Employees have been informed of information security policies and procedures. Who To Ask: Managers and employees.	**MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
2	**Education and Awareness**				
2.2	**Role-Based Training** A process is in place to develop and deliver additional training (beyond IM117) on information security to employees.	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.	What This Means: If employees require additional information protection training, the training is provided to appropriate employees. Who To Ask: MISO, managers and employees.	**MISO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
3	**Service Provider Management**				

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Information Protection			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
3.1	**External Parties** Assessment of risks from external party access to government information, information systems or information processing facilities are performed and appropriate security controls are implemented prior to granting access.	A documented risk assessment process exists and is communicated to Ministry employees. Reviews are conducted for all external party access.	What This Means: The ministry has a documented risk assessment process for providing access to external parties. Risk assessments are completed where appropriate. Who To Ask: MISO and managers.	**MISO -** Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
3.2	**Monitoring Service Provider Compliance with information security Requirements** The ministry has a process to monitor service provider compliance with information security requirements. If needed, there are adequate provisions in place to deal with issues of non-compliance. This wording is also included in privacy 4.4 and 5.4	There is a documented process for the monitoring of service provider compliance with information security requirements. If needed, there are adequate provisions in place to deal with issues of non-compliance.	What This Means: The ministry maintains a process to monitor service provider compliance with security requirements outlined in contracts. Who To Ask: The MISO and managers/contract managers.	**MISO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
4	**Security Requirement and Classification**				
4.1	**Security Classification** Records are organized so that security classifications can be applied to protect different classes of information based on their sensitivity.	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.	What This Means: The ministry has applied security classfications to its information. Who To Ask: MISO.	**MISO** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Information Protection			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
4.2	**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.	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.	What This Means: There is a documented process to ensure that ISRAs are conducted where appropriate (i.e. for new and updated systems). Who To Ask: MISO.	**MISO** - Yes or No	**Document Name:** **Location:**
4.3	**Protection Against Malicious Code** There an established process in place to prevent, detect, and resolve malicious code infections on information systems and infrastructure.	Processes related to malicious code are defined and implemented.	What This Means: Employees are aware of procedures to prevent malicious code infections (e.g. supervisor approval is required to download new software or applications, do not click suspicious links, etc.). There is a documented procedure for detecting and resolving infections. Who To Ask: The MISO, managers and employees.	**MISO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
4.4	**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.	Vulnerability assessments are planned and conducted on a regular basis (based on risk). Vulnerabilities are risk ranked and remediated in priority order.	What This Means: The ministry has identified its critical systems and has a documented process to identify, assess, and respond to vulnerabilities within these systems. Who To Ask: MISO.	**MISO** - Yes or No	**Document Name:** **Location:**
5	**User Access Management**				

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Information Protection			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
5.1	**Access Control** Access control processes are in place covering the full range of access management for employees and service providers (granting, reviewing, removing, changing, etc.).	Documented access control processes are in place covering the full range of access management for employees and service providers (granting, reviewing, removing, changing, etc.).	What This Means: The ministry has a documented process for providing, updating and removing employee and service provider access to systems. Who To Ask: MISO and managers.	**MISO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
5.2	**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.	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.	What This Means: The ministry has identified its critical systems and implemented logging capabilities for these systems. The logs are monitored. Logs are secured and accessed by authorized employees only. Who To Ask: MISO and managers.	**MISO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
5.3	**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 are in place for user responsibilities and access. Employees are aware of and adheres to the clean desk policy and the need to protect unattended equipment and access to government information.	What This Means: Employees have been informed of their responsibilities to prevent unathorized access to government information. (i.e. clean desk, do not leave equipment unattended, do not share passwords, lock screens, do not share confidential information, etc.). Who To Ask: The MISO, managers and employees.	**MISO** - Yes or No **MGR** - Yes or No **EMP** - Yes or No	**Document Name:** **Location:**
6	**Asset Management, Protection and BCP**				

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Information Protection			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
6.1	**Business Continuity Management** Business continuity management processes and plans have been developed tested, maintained, updated and they include provisions to maintain security and information security in the case of an incident.	A documented business continuity plan exists. The plan includes an assessment of risk and information sensitivity and incorporates appropriate controls to address information security.	What This Means: The ministry has developed a BCP that includes controls addressing information security during incidents. Disaster Recovery Plans have been created for critical systems. Who To Ask: MISO.	**MISO** - Yes or No	**Document Name:** **Location:**
6.2	**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.	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.	What This Means: The ministry maintains an inventory of government information systems and mobile devices. Who To Ask: MISO and manager.	**MISO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**
6.3	**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.	Controls are documented regarding equipment protection, including asset disposal.	What This Means: The ministry has a documented process to ensure the removal of government information from devices that are no longer in use. Who To Ask: MISO and manager.	**MISO** - Yes or No **MGR** - Yes or No	**Document Name:** **Location:**

#	Criteria Statement	Defined Statement	Interpretation	Criteria Met (Y/N)	Supporting Documentation
Information Protection			What This Means and Who To Ask	If Y, Supporting Documentation Required	Name and Location of Supporting Documents (Do Not Submit to IMPR)
6.4	**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.	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.	What This Means: The ministry maintains an portable media inventory and approval process. A documented process in place to ensure portable media devices are used according to OCIO standards. Who To Ask: The MISO, managers and employees.	**MISO** - Yes or No **MGR** - Yes **EMP** - Yes	**Document Name:** **Location:**

Term	Defintion
CIRMO	Corporate Information Records Management Office
Delegation Instrument	A delegation matrix used by leaders to aid in the decision as to which tasks to delegate and which to retain
DGD	Documenting Government Decisions
Duty to Assist	The head of a public body must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely
FOI	Freedom of Information
FOIPPA	Freedom of Information and Privacy Protection Act
GRS	Government Records Service
HIB	Health Information Bank
IIMP	Information Incident Management Process
IM117	Mandatory IM training for all government employees
IMA	Information Management Act
IMPR	Information Management Practice Review
ISA	Information Sharing Agreement
ISP	Information Security Policy (government-wide) Information Security Program (Ministry-specific)
Legal Instrument	Is any formally executed written document that can be formally attributed to its author, records and formally expresses a legally enforceable act, process, or contractual duty, obligation, or right, and therefore evidences that act, process, or agreement.
MISO	Ministry Information Security Officer
MPO	Ministry Privacy Officer
OCIO	Office of the Chief Information Officer
PI	Personal Information
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
PID	Personal Information Directory
PII	Personal Information Inventory Policy
PMAP	Privacy, Management and Accountability Policy
PPS	Privacy Protection Schedules
RM	Records Management
RO	Records Officer
Service Providers	A person retained under a contract to perform services for a public body

Infrastructure and Major Projects Department

BRANCH	Infrastructure Development	Planning and Programming	Evergreen Line	George Massey Tunnel Replacement Project	Procurement and Public Private Partnerships	Metro Vancouver Major Projects				
CRITICAL RECORD SERIES IDENTIFIED	**record type** **records type**	**record type** **records type**	**record type** **records type**	**record type** **records type**	**record type** **records type**	**record type** **records type**				
BUSINESS ACCESS FREQUENCY	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH				
FOI REQUEST FREQUENCY	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH				
PHYSICAL VOLUME (LOW / MED / HIGH)	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH				
FORMAT OF RECORD	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH				
DOCUMENT TYPES IN SERIES	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH				
ARRANGEMENT STANDARDS	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH				
TRACKING SYSTEM USED (eg. TRIM)	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH	LOW/MED/HIGH				
SECONDARY NUMBER										
SECONDARY TITLE										
RETENTION DETAILS (A / SA / FD)										
SO CRITERIA										
FINAL DISPOSITION										
SCHEDULE NUMBER										
DRAFT OR APPROVED										
PHYSICAL VOLUME ONSITE - CRITICAL RECORD SERIES (FT.)										
PHYSICAL VOLUME ONSITE - NOTES										
BOXES OFFSITE - CRITICAL RECORD SERIES (# OF BOXES)										
BOXES OFFSITE - NOTES										
SCAN CANDIDATE FOR LEGACY FILES										
DIGITAL RECORDS - LOCATIONS										
DIGITAL RECORDS - VOLUME (GB)										
DIGITAL RECORDS - DATE RANGES										
DIGITAL RECORDS - ASSOCIATED EMAIL LOCATIONS										
DIGITAL RECORDS - ASSOCIATED EMAIL VOLUME										
DIGITAL DATABASES USED										
DIGITAL DATABASE - NOTES										
DIGITIZATION PLAN FOR SERIES										
DIGITIZATION READINESS										
BRANCH RM NOTES										
RO RECOMMENDATIONS										
BRANCH RM CONTACT										
BRANCH IMB CONTACT										

EXEC CRITIAL RECORDS TABLE

Division	Branch	Critical Record series	Business Access rate	FOI request rate	Physical record volume	RM system used:	TRIM: use / want / no	Format: Digital / Physical	Schedule Number	Secondary Classification	Draft or Approved	Active Retention	Semi - Active Retention	Final Retention	SO criteria	Scan candidate for legacy records (Y/N)	If Yes, make note of date range / volume / content	Physical Records: Location of ON-SITE records in series	Physical Records: Linear feet ON-site - central file	Physical Records: Linear feet ON-site - offices / not	Physical Records: # Boxes in OFF-	Physical Records: CLC Crystal Report	Physical Records: Notes	Digital Records: Storage	Digital Records: Date	Digital Records: Volume (GB)	Digital Records: Associated emails?	If Yes, location of stored	Email volume (GB)	Document Types included in	Document Arrangement Qualifiers	Secondary Arrangement Qualifiers (eg.	Branch Plan to meet IMA Digitization	Planned location status: (give details)	RM System notes	Branch RM Contact	Staff Consulted	RO Recommendations
BC Parks and Conservation Officer Service	Visitor Experience / Business Development / Central File room	Park Operator / Facility Contracts	s.13																																			
BC Parks and Conservation Officer Service	Visitor Experience / Business Development / Central File room	Records of Decisions																																				
BC Parks and Conservation Officer Service	Visitor Experience / Business Development / Central File room	Facility As-Built files																																				
BC Parks and Conservation Officer Service	Conservation, Planning and Aboriginal Relations	Green Legal files																																				
BC Parks and Conservation Officer Service	Conservation, Planning and Aboriginal Relations	Management files																																				
BC Parks and Conservation Officer Service	Conservation, Planning and Aboriginal Relations	Policy																																				
BC Parks and Conservation Officer Service	Conservation Officer Service HQ	Policy																																				
BC Parks and Conservation Officer Service	Conservation Officer Service HQ	MOU																																				
BC Parks and Conservation Officer Service	Conservation Officer Service HQ	COS Appointments																																				
BC Parks and Conservation Officer Service	BC Park - Regional Operations (inventory only)	not documented																																				
Environmental Protection Division	Environmental Standards Branch	Policy																																				
Environmental Protection Division	Environmental Standards Branch	Compliance and Enforcement																																				
Environmental Protection Division	Environmental Standards Branch	Authorizations / License to transport																																				
Environmental Protection Division	Business Services Branch	Manifests for Hazardous waste																																				
Environmental Protection Division	Business Services Branch	Authorizations																																				
Environmental Protection Division	Business Services Branch	Securities																																				
Environmental Protection Division	Land Remediation Branch	Contaminated Sites																																				
Environmental Protection Division	Land Remediation Branch	Policy																																				
Environmental Protection Division	Land Remediation Branch	Legislation and Regulation																																				
Environmental Protection Division	Environmental Emergency Program & Spill Response Project	Dangerous Good Incident Reports																																				
Environmental Protection Division	Environmental Emergency Program & Spill Response Project	Policy																																				
Environmental Protection Division	Environmental Emergency Program & Spill Response Project	Incident room																																				
Environmental Protection Division	EPD - Regional Operations (inventory only)	not documented																																				
Environmental Sustainability and Strategic Policy Division	Ecosystems Branch	Program/Project Areas																																				
Environmental Sustainability and Strategic Policy Division	Ecosystems Branch	Finance/Admin																																				
Environmental Sustainability and Strategic Policy Division	Ecosystems Branch	HR / Staffing																																				
Environmental Sustainability and Strategic Policy Division	Ecosystem Information Branch	Contracts																																				
Environmental Sustainability and Strategic Policy Division	Ecosystem Information Branch	ECOCAT info																																				
Environmental Sustainability and Strategic Policy Division	Ecosystem Information Branch	Standards																																				
Environmental Sustainability and Strategic Policy Division	Environmental Monitoring, Reporting and Economics	Methodology																																				
Environmental Sustainability and Strategic Policy Division	Environmental Monitoring, Reporting and Economics	Standards																																				
Environmental Sustainability and Strategic Policy Division	Environmental Monitoring, Reporting and Economics	Contracts																																				
Environmental Sustainability and Strategic Policy Division	Technical Services Branch	Reports and Planning																																				
Environmental Sustainability and Strategic Policy Division	Technical Services Branch	Contracts/Finance																																				
Environmental Sustainability and Strategic Policy Division	Technical Services Branch	Spatial Information																																				
Environmental Sustainability and Strategic Policy Division	Strategic Policy Branch	not documented																																				
Environmental Sustainability and Strategic Policy Division	Water Protection and Sustainability Branch	Well Records																																				
Environmental Sustainability and Strategic Policy Division	Water Protection and Sustainability Branch	Registration of Drillers																																				
Climate Leadership	Climate Action Secretariat	Agreements																																				
Climate Leadership	Climate Action Secretariat	Project files																																				
Climate Leadership	Climate Action Secretariat	Issues/Information																																				
Climate Leadership	ADM, Climate Action Secretariat	Briefing Notes																																				
Climate Leadership	ADM, Climate Action Secretariat	Cabinet & Treasury																																				
Climate Leadership	ADM, Climate Action Secretariat	Issues/Information																																				
Executive Committee	Correspondence Unit	Executive Correspondence																																				
Executive Committee	ADM	Issues Files																																				
Executive Committee	ADM	Committees																																				
Executive Committee	ADM	Decision notes																																				
Executive Committee	ADM	Calendars																																				
Executive Committee	ADM	Cabinet Documents																																				
ED - Infrastructure	ED																																					

Page 086 of 444 to/à Page 087 of 444

Withheld pursuant to/removed as

s.13

[branch name] – Branch Summary

Physical Records: # total boxes for division

Statements about ORCS, resources, space, major issues and risks

❖ [NAME] Branch

Total box count	**# boxes**
Central Areas	# boxes
Individual Offices	# boxes
Largest file volume	**Records type / record type / record type**
Access need	High/medium/low
Candidate for scanning	yes / no / done / planned
Information Schedule	**ORCS name, section, primary block – approved / draft**
Use of classification	used
RM Systems	**System name**
Use of RM system	Physical and / or electronic
Applications/systems	System name
Use of system	Describe / documentation
Comments	

General Notes from [branch]

Examples of entries here:

- Digital records: primary volume on [location]
- Systems (applciations/databases) used:
  - acronym –full name
  - acronym – full name
- Business emails are...
- Duplication of physical and e-records, but usually [type] considered the official copy.
- Some push to go digital with [plans on systems decommission, succession, development…]
- New schedule has started development with GRS, as current classifications [do / not] adequately reflect function.
- Divisional critical files relate to [function/activity/process]
- Inconsistent/consistent/mature/stale records procedures and practices
- # divisional staff for information and records management and FOI.

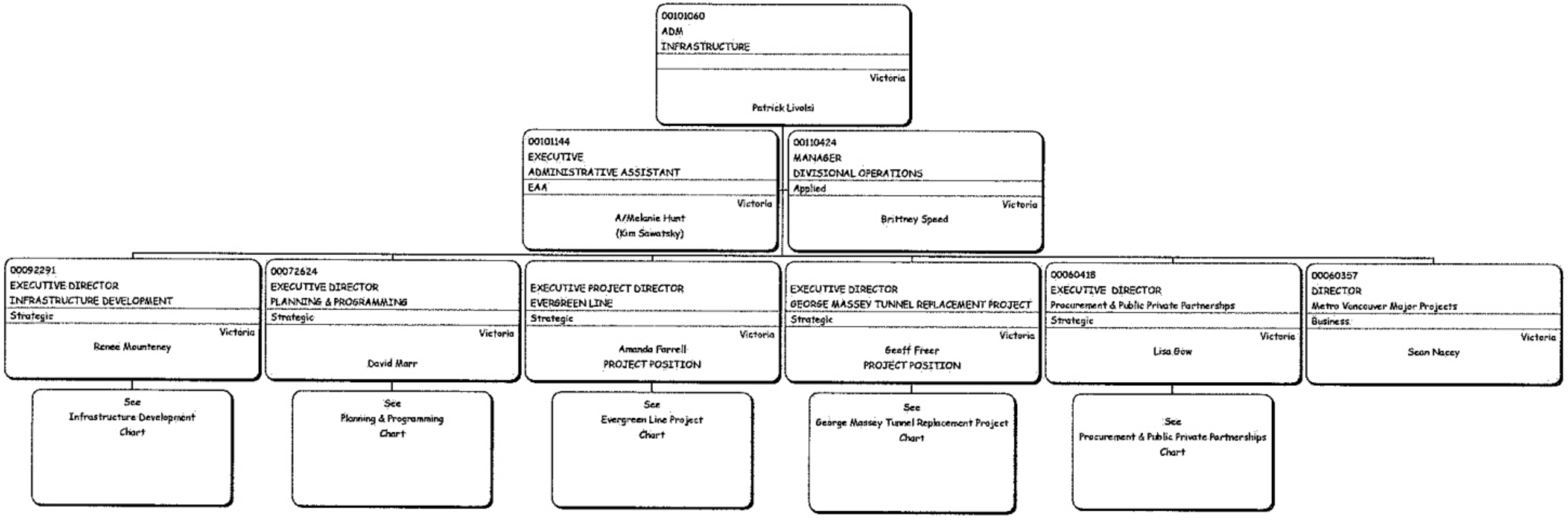
- Expressed need for [resource type] in branches
- Expressed need for [e.g. strong direction and allocated time/resources for RM from DMO]

Page 090 of 444 to/à Page 093 of 444

Withheld pursuant to/removed as

s.13

MINISTRY OF TRANSPORTATION & INFRASTRUCTURE
ORGANIZATION CHART
INFRASTRUCTURE DEPARTMENT - OVERVIEW
Last Modified 2016-12-14



00101060
ADM
INFRASTRUCTURE
Victoria
Patrick Livolsi

00101144
EXECUTIVE
ADMINISTRATIVE ASSISTANT
EAA
Victoria
A/Melanie Hunt
(Kim Sawatsky)

00110424
MANAGER
DIVISIONAL OPERATIONS
Applied
Victoria
Brittney Speed

00092291
EXECUTIVE DIRECTOR
INFRASTRUCTURE DEVELOPMENT
Strategic
Victoria
Renee Mounteney

See
Infrastructure Development
Chart

00072624
EXECUTIVE DIRECTOR
PLANNING & PROGRAMMING
Strategic
Victoria
David Marr

See
Planning & Programming
Chart

EXECUTIVE PROJECT DIRECTOR
EVERGREEN LINE
Strategic
Victoria
Amanda Farrell
PROJECT POSITION

See
Evergreen Line Project
Chart

EXECUTIVE DIRECTOR
GEORGE MASSEY TUNNEL REPLACEMENT PROJECT
Strategic
Victoria
Geoff Freer
PROJECT POSITION

See
George Massey Tunnel Replacement Project
Chart

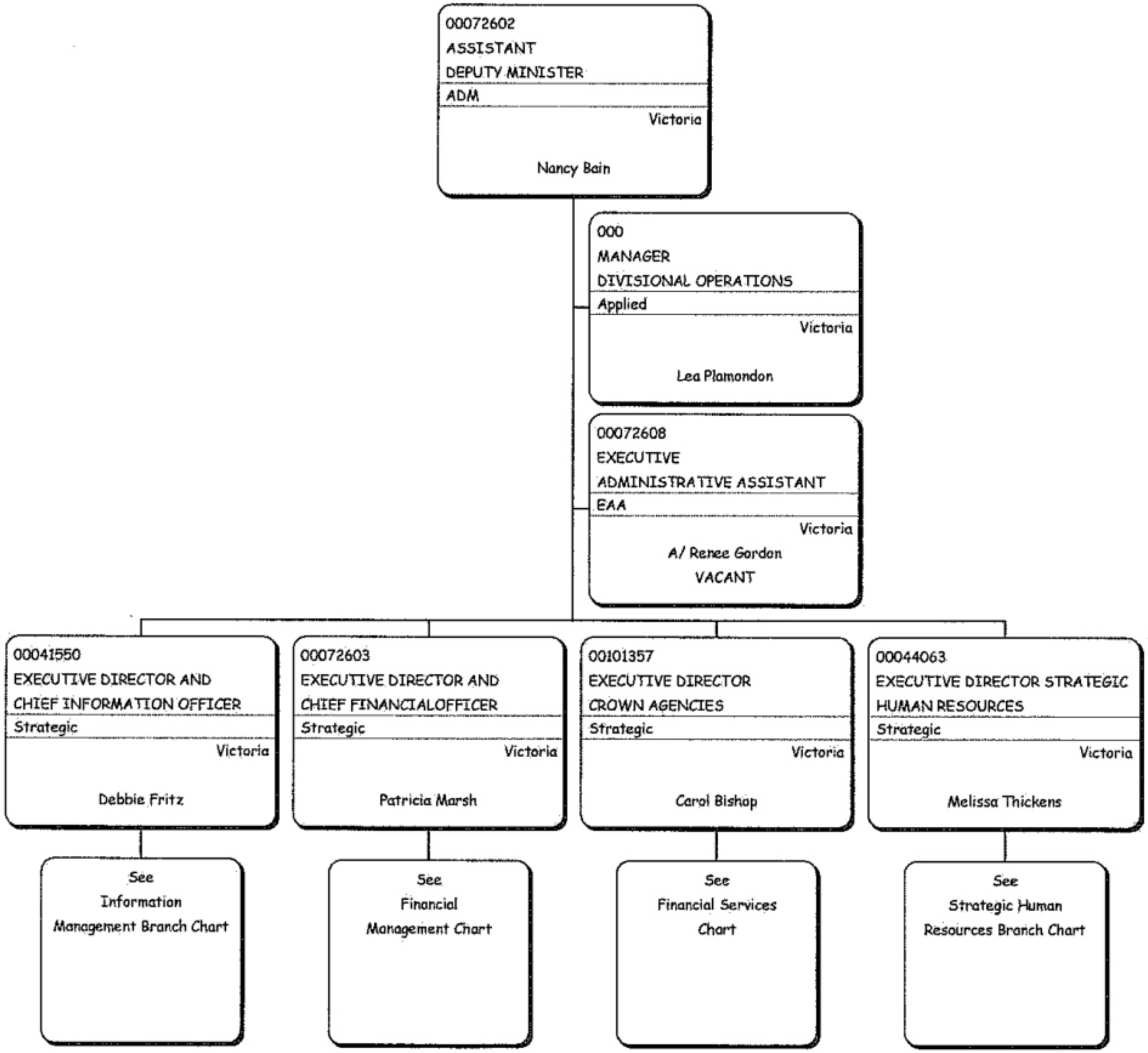
00060418
EXECUTIVE DIRECTOR
Procurement & Public Private Partnershps
Strategic
Victoria
Lisa Gow

See
Procurement & Public Private Partnerships
Chart

00060357
DIRECTOR
Metro Vancouver Major Projects
Business
Victoria
Sean Nacey

Infrastructure Department Overview.opx

MINISTRY OF TRANSPORTATION AND INFRASTRUCTURE
ORGANIZATION CHART
FINANCE AND MANAGEMENT SERVICES DEPARTMENT
Last Modified 2017-06-06



00072602
ASSISTANT
DEPUTY MINISTER
ADM
Victoria
Nancy Bain

000
MANAGER
DIVISIONAL OPERATIONS
Applied
Victoria
Lea Plamondon

00072608
EXECUTIVE
ADMINISTRATIVE ASSISTANT
EAA
Victoria
A/ Renee Gordon
VACANT

00041550
EXECUTIVE DIRECTOR AND
CHIEF INFORMATION OFFICER
Strategic
Victoria
Debbie Fritz

See
Information
Management Branch Chart

00072603
EXECUTIVE DIRECTOR AND
CHIEF FINANCIALOFFICER
Strategic
Victoria
Patricia Marsh

See
Financial
Management Chart

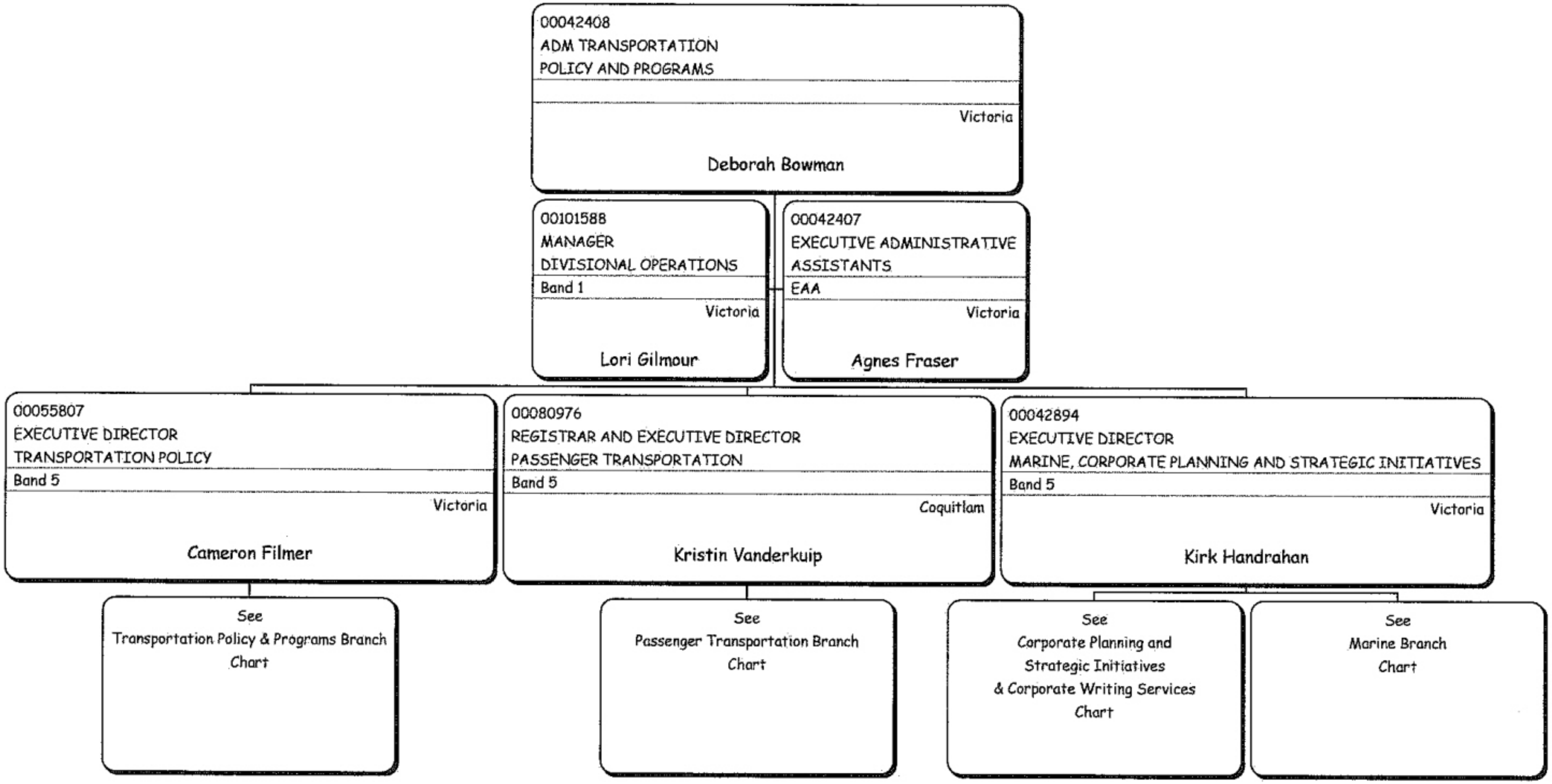
00101357
EXECUTIVE DIRECTOR
CROWN AGENCIES
Strategic
Victoria
Carol Bishop

See
Financial Services
Chart

00044063
EXECUTIVE DIRECTOR STRATEGIC
HUMAN RESOURCES
Strategic
Victoria
Melissa Thickens

See
Strategic Human
Resources Branch Chart

MINISTRY OF TRANSPORTATION & INFRASTRUCTURE
TRANSPORTATION POLICY AND PROGRAMS DEPARTMENT - OVERVIEW
Last modified 2017-Feb-16



00042408
ADM TRANSPORTATION
POLICY AND PROGRAMS
Victoria
Deborah Bowman

00101588
MANAGER
DIVISIONAL OPERATIONS
Band 1
Victoria
Lori Gilmour

00042407
EXECUTIVE ADMINISTRATIVE
ASSISTANTS
EAA
Victoria
Agnes Fraser

00055807
EXECUTIVE DIRECTOR
TRANSPORTATION POLICY
Band 5
Victoria
Cameron Filmer

00080976
REGISTRAR AND EXECUTIVE DIRECTOR
PASSENGER TRANSPORTATION
Band 5
Coquitlam
Kristin Vanderkuip

00042894
EXECUTIVE DIRECTOR
MARINE, CORPORATE PLANNING AND STRATEGIC INITIATIVES
Band 5
Victoria
Kirk Handrahan

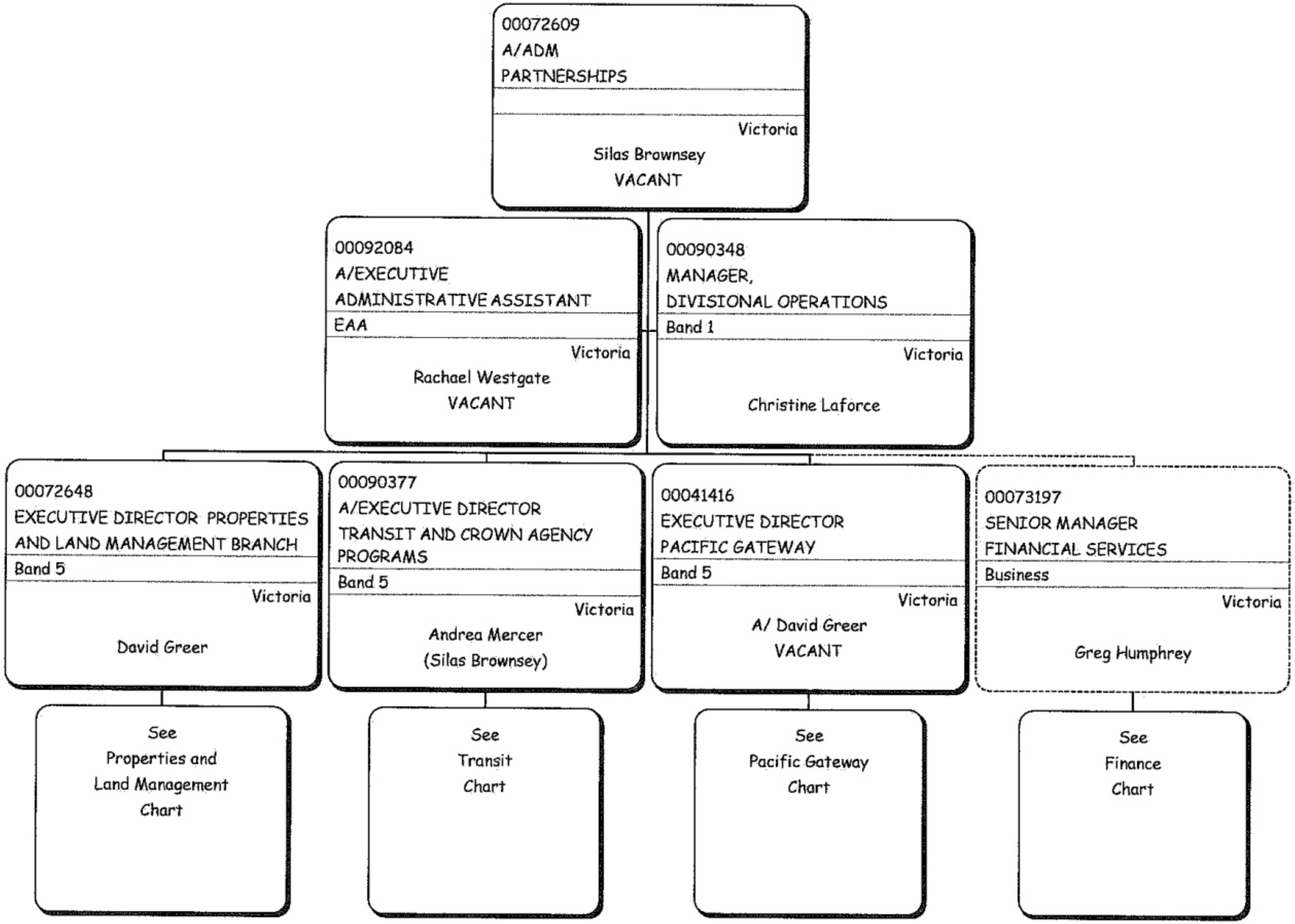
See
Transportation Policy & Programs Branch
Chart

See
Passenger Transportation Branch
Chart

See
Corporate Planning and
Strategic Initiatives
& Corporate Writing Services
Chart

See
Marine Branch
Chart

MINISTRY OF TRANSPORTATION AND INFRASTRUCTURE
ORGANIZATION CHART
PARTNERSHIPS DEPARTMENT - OVERVIEW
2016-06-20



00072609
A/ADM
PARTNERSHIPS
Victoria
Silas Brownsey
VACANT

00092084
A/EXECUTIVE
ADMINISTRATIVE ASSISTANT
EAA
Victoria
Rachael Westgate
VACANT

00090348
MANAGER,
DIVISIONAL OPERATIONS
Band 1
Victoria
Christine Laforce

00072648
EXECUTIVE DIRECTOR PROPERTIES
AND LAND MANAGEMENT BRANCH
Band 5
Victoria
David Greer

00090377
A/EXECUTIVE DIRECTOR
TRANSIT AND CROWN AGENCY
PROGRAMS
Band 5
Victoria
Andrea Mercer
(Silas Brownsey)

00041416
EXECUTIVE DIRECTOR
PACIFIC GATEWAY
Band 5
Victoria
A/ David Greer
VACANT

00073197
SENIOR MANAGER
FINANCIAL SERVICES
Business
Victoria
Greg Humphrey

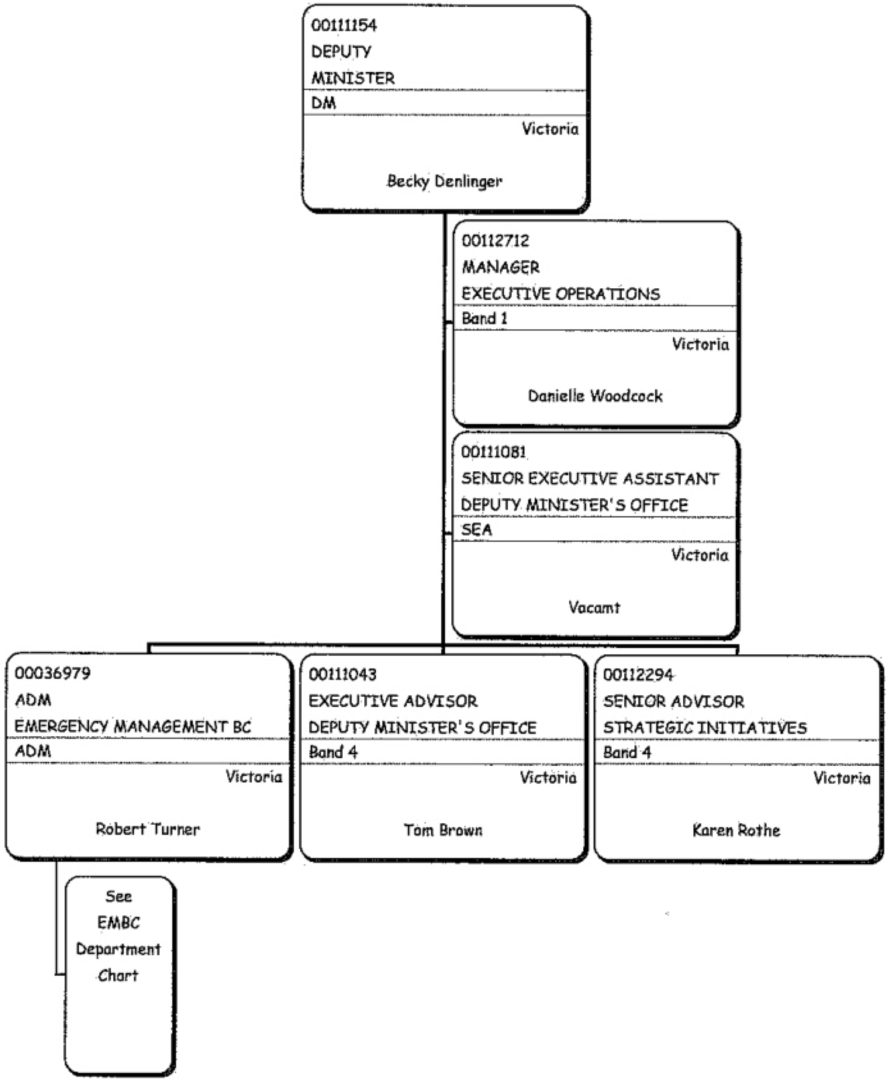
See
Properties and
Land Management
Chart

See
Transit
Chart

See
Pacific Gateway
Chart

See
Finance
Chart

MINISTRY OF TRANSPORTATION AND INFRASTRUCTURE
ORGANIZATION CHART
DEPUTY MINISTER'S OFFICE - Emergency Management
Last Modified 2017-06-16



00111154
DEPUTY
MINISTER
DM
Victoria
Becky Denlinger

00112712
MANAGER
EXECUTIVE OPERATIONS
Band 1
Victoria
Danielle Woodcock

00111081
SENIOR EXECUTIVE ASSISTANT
DEPUTY MINISTER'S OFFICE
SEA
Victoria
Vacamt

00036979
ADM
EMERGENCY MANAGEMENT BC
ADM
Victoria
Robert Turner

00111043
EXECUTIVE ADVISOR
DEPUTY MINISTER'S OFFICE
Band 4
Victoria
Tom Brown

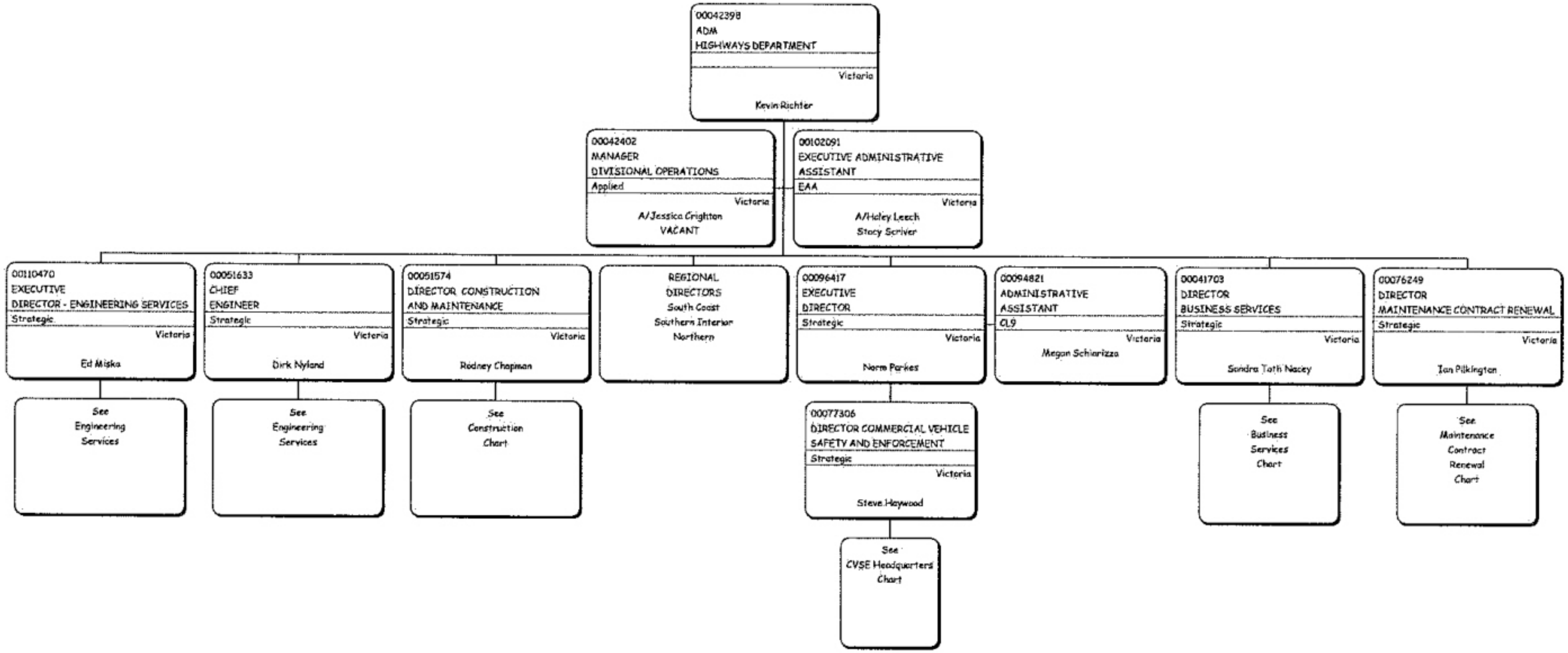
00112294
SENIOR ADVISOR
STRATEGIC INITIATIVES
Band 4
Victoria
Karen Rothe

See
EMBC
Department
Chart

Deputy_Minister_Office_EM.opx

MINISTRY OF TRANSPORTATION AND INFRASTRUCTURE
ORGANIZATION CHART
HIGHWAYS DEPARTMENT - OVERVIEW

Last Modified - 2017-04-03



00042398
ADM
HIGHWAYS DEPARTMENT
Victoria
Kevin Richter

00042402
MANAGER
DIVISIONAL OPERATIONS
Applied
Victoria
A/Jessica Crighton
VACANT

00102091
EXECUTIVE ADMINISTRATIVE
ASSISTANT
EAA
Victoria
A/Haley Leech
Stacy Scriver

00110470
EXECUTIVE
DIRECTOR - ENGINEERING SERVICES
Strategic
Victoria
Ed Miska

See
Engineering
Services

00051633
CHIEF
ENGINEER
Strategic
Victoria
Dirk Nyland

See
Engineering
Services

00051574
DIRECTOR CONSTRUCTION
AND MAINTENANCE
Strategic
Victoria
Rodney Chapman

See
Construction
Chart

REGIONAL
DIRECTORS
South Coast
Southern Interior
Northern

00096417
EXECUTIVE
DIRECTOR
Strategic
Victoria
Norm Parkes

00077306
DIRECTOR COMMERCIAL VEHICLE
SAFETY AND ENFORCEMENT
Strategic
Victoria
Steve Haywood

See
CVSE Headquarters
Chart

00094821
ADMINISTRATIVE
ASSISTANT
CL9
Victoria
Megan Schiarizza

00041703
DIRECTOR
BUSINESS SERVICES
Strategic
Victoria
Sandra Toth Nacey

See
Business
Services
Chart

00076249
DIRECTOR
MAINTENANCE CONTRACT RENEWAL
Strategic
Victoria
Ian Pilkington

See
Maintenance
Contract
Renewal
Chart

Infrastructure and Major Projects - Interview Pointers

- This is a data collection project to inform the Deputy Minister's office of the current state of records and information management across headquarters programs.

- This is being done in anticipation of changes coming under the Information Management Act, and to support the ministry IM strategic planning.

- Please convey the current state of your program area's records and information management situation as accurately as possible.

- No program area has perfect records and information management. Identifying weak areas on program, ministry and corporate levels will enable targeted and effective changes to be planned.

- There is no wrong answer - your program area will not be penalized for the information it shares.

- Anticipate 1.0 to 1.5 hours for a full interview with conversation, as well as an additional .5 hour for measuring physical file volume.

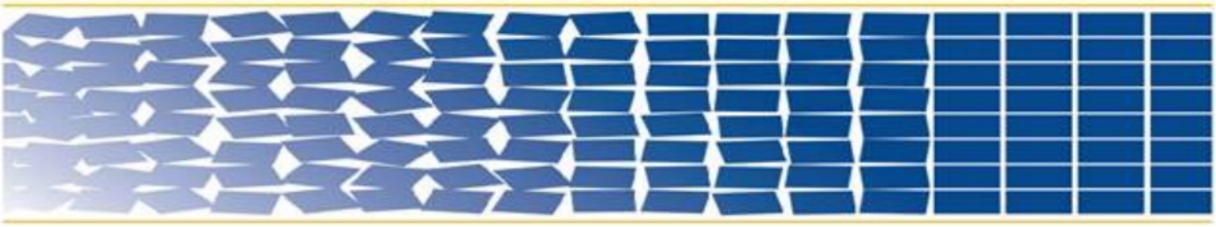
- The interview covers the following subjects, each with a handful of questions:
  A. Physical records
  B. Email Records
  C. Electronic Documents
  D. Structured Databases
  E. Information Schedules
  F. Records Management Procedures and Practice
  G. Corporate Records and Information Training and Support
  H. Ministry Specific Questions
  I. Measurement of Onsite Physical Files

- If you are not sure of an answer please give information about the context, much of the value will be in the conversation.

- We appreciate your time and willingness to participate!

BRITISH COLUMBIA

GOVERNMENT RECORDS SERVICE
A BRANCH of SHARED SERVICES BC



Ministry of Transportation and Infrastructure Information Management Assessment

INTRODUCTION

This project is to collect information about the current Information and Records Management practices.

Please consider how you manage your work unit’s business records.

The collected information will be summarized and used to develop strategies and associated projects to improve practices. In addition to the questionnaire, a physical inventory of records volume will be conducted.

Thank you for your time and sharing of your insights.

For Records Management questions, direct to Trevor.Youdale@gov.bc.ca

Government Records Service - Corporate Information and Records Management Office

Ministry of Transportation and Infrastructure

Date

Interviewers:

General Information

Division

Branch

Work unit(s)

Location

Number of staff

Branch mandate or description of responsibilities

Attendees:	Name	Position

INTERVIEW

A - Physical Records

1. Do you keep paper copies of current records? (YES / NO)

a) Identify main categories of paper records currently created:

b) Comments:

2. Are your paper records tracked in any records management systems other than CRMS or TRIM (e.g., Index cards, Excel, databases)? (YES / NO)

a) Identify systems used:

b) Identify record series tracked in alternative systems:

c) Comments:

3. Are there any legal or business reasons for them to be in paper format? (YES / NO / UNKNOWN)

a) Reasons for paper format:

b) Comments:

A - Physical Records (cont'd)

4. Is the branch planning any digitization or scanning projects? (YES / NO)

a) Record series captured or in consideration:

b) Comments:

Do you have any additional Comments?

B - Email Records

1. To what extent are business emails stored in a shared location accessible by appropriate branch staff? (MINIMAL / SOMEWHAT / MOSTLY)

   a) What is the branch practice for capturing and sharing emails?

   b) Comments:

Temperature Check: *Please identify the primary challenges associated with managing email records in your branch (e.g., Running out of space, duplication and tracking of threads, finding relevant email, storing on backups, etc.):*

Do you have any additional Comments?

C – Electronic Documents

1. To what extent are branch electronic documents stored in a shared location accessible by appropriate branch staff? (MINIMAL / SOMEWHAT / MOSTLY)

a) Identify top three locations [by approximate volume] where branch electronic documents are stored (e.g., TRIM, LAN, Sharepoint):

1. _______________ 2. ______________ 3. ______________

b) Identify addresses of active and legacy LAN drives owned by branch:

c) Comments:

2. Are branch electronic documents on LANs associated with ARCS/ORCS classifications at the document or folder level? (YES / NO)

a) Is final disposition applied to those electronic documents that are classified under approved schedules?

b) Describe the disposition process followed

c) Additional Comments:

C – Electronic Documents (Cont'd)

3. To what extent does your branch keep both electronic and paper copies of the same document? (MINIMAL / SOMEWHAT / MOSTLY)

a) In what circumstances?

b) Does staff know which is the official document? (YES / NO)

c) Comments:

Temperature Check: *Please identify the primary challenges associated with managing electronic records in your branch:*

Do you have any additional Comments?

D - Structured Databases

1. Does branch use Line-of-Business systems? (YES / NO)

    a) Identify systems [use full name plus acronym]:

    b) Is your branch the primary owner of these systems? Please specify:

    c) Comments:

2. Do any of the systems store electronic documents? (YES / NO)

    a) Which systems store electronic documents?

    b) Which record series?

    c) Comments:

3. Do any business systems house the official copy of electronic documents? (YES/NO)

    a) Identify system:

    b) Are duplicates of the information managed elsewhere (e.g., LAN, paper)?

    c) Is the final disposition of electronic documents managed in the system?

    d) Comments:

4. Who is the current IMB business portfolio contact for the systems?

    a) Identify IMB contacts for systems:

    b) Comments:

D - Structured Databases (Cont’d)

Temperature Check: *Please identify the primary challenges associated with managing structured data in your branch. (e.g., Disposition, document storage, version/audit control, does it address business needs?)*

Do you have any additional Comments?

E - Information Schedules

1. Does your branch have an Operational Records Classification Schedule (ORCS) for the records it creates? (YES / NO)

   a) Identify information schedules / classifications used (title or #):

   b) Is it used across branch?

   c) Comments:

2. Does the information schedule being used reflect current business functions? (YES / NO / UNKNOWN)

   a) Identify any known gaps or problem areas in information scheduling (if known):

   b) Comments:

Temperature Check: *Please identify the primary challenges associated with information schedules and classification of records in your branch. (e.g., ORCS no longer reflects business functions, low employee knowledge of information schedules)*

Do you have any additional Comments?

F - Records Management Procedures and Practice

1. Do offices have branch-specific business procedures for information and records management? (YES / NO)

a) Are these procedures documented and easy to reference?

b) Comments:

2. Can your branch easily find its business critical information and records? (YES / NO)

a) Identify top ~~three~~ categories of business critical information created by your branch regardless of format (electronic or paper):

b) Considering these categories, fill in the chart below

~~Top 3~~ Business Critical Record Series	Large Quantity of Paper Onsite? Y/N	High Med Low Business Access?	Frequent Public Access Y/N? (Routine, FOI, Litigation)	Good Candidate for Paper Scanning Y/N?
1.				
2.				
3.				

c) Are there any additional series of paper records that should be considered a possibility for scanning?

F - Records Management Procedures and Practice (Cont'd)

4. To what extent do branch employees know how to classify their business critical records according to ARCS/ORCS? (MINIMAL / SOMEWHAT / MOSTLY)

a) Is classification done individually or centrally?

b) Do naming conventions exist for business critical records?

c) Comments:

5. Does the branch have specific employees tasked with Information and Records management functions or responsibilities? (YES/NO)

a) Identify position(s) and Current staff:

b) Describe assigned functions/responsibilities:

c) Comments:

6. To what extent does your branch send out communication regarding internal standards and records management processes? (MINIMAL / SOMEWHAT / MOSTLY)

a) To what extent are new employees trained in branch practice?

b) Are you aware of the policy for departing employees?

c) To what extent are the records of departing employees managed proactively?

d) Comments:

Temperature Check: *Please identify the primary challenges associated with records procedures and practices in your branch.*

Do you have any additional Comments?

G – Corporate Records and Information Training and Support

1. Is there an expectation in your branch that staff take the corporate training available for information and records management? (YES/NO)

a) Estimate % of staff who have taken online courses IM available through the learning center:

b) Estimate % of staff who have taken the classroom IM courses in government information and records management available through the learning center:

c) What kind of training and was it helpful?

d) Comments:

2. Do employees know who to contact at Government Records Services for support with records and information management issues such as TRIM administration, general records advice, sector specific advice, information schedule development, record ownership changes, destruction approvals or sending records offsite?

a) Who are primary internal, sector and/or corporate contacts?

b) Are employees aware of online records and information management resources (e.g., Website, SharePoint, Intranets)? (YES/NO)

If yes, please identify resources used:

c) Comments:

G – Corporate Records and Information Training and Support (Cont'd)

3. Are branch employees aware that changes to information and records management requirements are coming under the new Information Management Act? (YES/NO)

a) Which issues should take priority in your branch if it is to meet the expectation of operating digitally in the near future?

b) Comments:

Temperature Check: *Please identify the primary challenges associated with information and records management training and support in your branch.*

Do you have any additional Comments?

H – Ministry Specific Questions

Major Projects issues to be worked into questions:

Contract records

Locations, access, security, reliability, accuracy, risk, tracking, granular document control, litigation, performance monitoring, timely access, back-up, as built, dependencies.

1. Do any work units in your branch have [TBD] records? (YES/NO)

    a) If yes, what % of total records are [TBD] records?

    b) Comments:

I – Additional Questions (some ideas for review with MoTI)

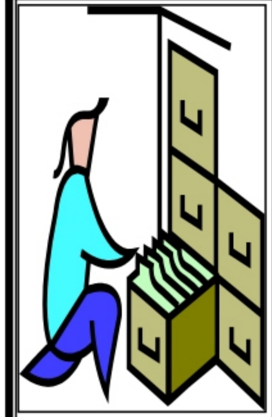
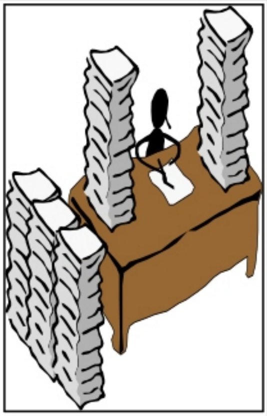
1. Is the information you need, readily available to you? If no, what are the challenges you are facing to access this information?
2. How long do you spend looking for records?
3. Do you know how long to keep records?
4. What happens to your records when you are “finished” with them?
5. Are you aware there is a formal process for disposing of records?
6. Do you search for files created by others? If so, how?
7. Do you consider how you will share a document with others when you are creating and saving files?
8. If not, how do others access your information when you’re not here?
9. Is there any internal review or regular discussion your records management practices and procedure?
10. If there was a resource available, such as an information management expert, would it improve your records management ability?
11. Describe your desired future state for records management? What would you change? What problems do you wish were gone? What challenges resolved?

Comments

Temperature Check: *Please identify any ministry-specific challenges associated with information and records management training and support.*

Do you have any additional Comments?

How do we measure the physical inventory of records?

Vertical Cabinet	Lateral Cabinet	Personal Desks	File Storage Boxes	Open File Shelves ***PLEASE COUNT NUMBER OF TOTAL UNITS FOR SPACE PLANNERS***	Other:
					Bookshelves Floor Table Shelf Drawer Map Cabinet Rolled Maps or Plans
Office vertical cabinets = 3 linear feet per drawer. Please note if they use hanging folders	Office lateral cabinets = 3 linear feet per drawer. Please note if they use hanging folders	Estimate volume of physical files in linear feet. Pedestal cabinets = 1 to 2 linear feet per drawer.	File storage box = 1 linear foot per box.	Measure width of file shelves to estimate volume in linear feet (approx. 2.5-3 feet/shelf)	Make note of specifics and estimate volume.

✓ **Keep notes about context and specifics to reference later if you are unsure**

Branch/Region/District:						
Location/Address:						
Date of Inventory:						
Completed by:						
Office or Room	Storage Unit Type	If Open File Shelf type give # of units	Hanging Folders? (Y/N)	Organized Content? (Y/N)	Total Linear Feet of Records	Notes
Branch/Region/District:						
Location/Address:						
Date of Inventory:						
Completed by:						
Office or Room	Storage Unit Type	If Open File Shelf type give # of units	Hanging Folders? (Y/N)	Organized Content? (Y/N)	Total Linear Feet of Records	Notes

Branch/Region/District:

Location/Address:

Date of Inventory:

Completed by:

Office or Room	Storage Unit Type	If Open File Shelf type give # of units	Hanging Folders? (Y/N)	Organized Content? (Y/N)	Total Linear Feet of Records	Notes

MoTI Major Projects IM Assessment – sequence, resources, issues

Approximate Sequence

1. Background research – intel from IMB (e.g. systems, shares, issues, sharepoint, personal drives)
2. Design questionnaire in consultation with departments leadership
3. Communications strategy
4. Meeting with department senior management – identify support (ownership), key issues (may affect questionnaire)
5. Schedule interviews – VI and mainland
6. Kick-off communications
7. Send interview questionnaire in advance
8. Conduct interviews
9. Follow-up with interviewees or other areas for more information / data verification
10. Data analysis / compile results
11. Create summary data and area summaries
12. Provide finding to client
13. Present findings to management / facilitate issues meeting with management

Information resources

Consult IMB on issues, concerns, input, lists of systems, shares, etc

Client documentation – reports, mandates, policies,

Issues?

Contract language, management, monitoring, records

Processes – roles and responsibilities, staff change,

Litigation

Access

Digitization

MoTI Current State Assessment – Interview Methodology

Overall approach

Department schedules interviews.

GRS conducts interviews with client. Two interviewers: one primary, and one scribing.

Interview starts with description of purpose as below.

Interview should aim for a comfortable, candid, relaxed, and positive experience, which encourages client to speak to their practices and areas of most concern.

Post interview, client should receive a thank note, and interview notes should be finalized into usable format for data collection and analysis.

Purpose – important information to provide to client at start

- ❖ This assessment is part of strategy to improve information management practices within the ministry. This assessment serves to:
    - o Inform the ministry and relevant departments of the current state of information management.
    - o Identify the issues and concerns of the program areas to support working toward improvement.
    - o Raise awareness information management within the ministry.
    - o Provide an opportunity to speak to information management challenges and practices.

- ❖ Please convey the current state of your program area's records and information management situation as accurately as possible.

- ❖ No program area has perfect records and information management. Identifying weak areas on program, ministry and corporate levels will enable targeted and effective changes to be planned.

- ❖ There is no wrong answer - your program area will not be penalized for the information it shares.

- ❖ The term 'information management' is used somewhat interchangeably with 'records management'. Some questions will speak to a particular from of information, for example, email. The scope is all recorded information that you and your branch, creates, receives, and uses in the course of your program and individual role, including email, documents, systems data.

- ❖ Anticipate 1.0 to 1.5 hours for a full interview with conversation.

- The interview covers the following subjects, each with a handful of questions:
    A. Electronic documents
    B. Email
    C. Physical records
    D. Data in systems
    E. Procedures and practices
    F. Corporate Training and Support

- If you are not sure of an answer please give information about the context, much of the value will be in the conversation.

- We appreciate your time and willingness to participate!

Ministry of Transportation and Infrastructure, Infrastructure & Major Projects
Information Management Current State Assessment - Interview Questions

Date:	**Branch:**
Interviewer Name(s):	**Interviewee Name:** **Function in Branch:**

Introduction

Tell me about your job. What do you do? What tools do you use to do your job? Are you part of a team or do you work independently?

s.13

A) Electronic Documents

How do you create, share, find and delete documents like spreadsheets (Excel), reports (Word and PDF), images, drawings, etc.

Question:	Y	N
1. Do you use naming standards for electronic folders and/or documents? If yes, please describe.		
2. Where do you store your electronic documents? (e.g. TRIM, LAN, SharePoint, USB, etc.):		
3. Are the documents you need readily available to you?		
4. Are these documents accessible to everyone with a need to use them?		
5. Do you consider how you will share a document with others when you are creating and saving documents?		
6. Do you know which electronic documents to keep?		
7. Are you confident that you can identify transitory electronic documents? If no, can you think of anything that would help you identify a transitory record?		

s.13

Question:	**Y**	**N**
8. Do you know how long you need to keep electronic documents?		
9. What happens to your electronic documents when you are "finished" with them?		
10. Do you keep both electronic and paper copies of the same documents? a) In what circumstances? b) Do you know which copy you would use or share as the final version?		
11. Please identify your primary challenges associated with electronic documents (e.g. storage, naming, searching, finding, sharing, duplication, destruction).		
Additional Comments: (Inquire with the interviewee about concerns, best practices and ideas for improvement)		

s.13

B) Email:

~~B)~~ How do you organize, share, find and delete emails and attachments.

Question:	Y	N
1. Do you have naming standards for email subject lines? If yes, please describe.		
2. Do you have team/branch email rules (e.g. use of fields, attachments)? If yes, please describe.		
3. Do you store your email anywhere other than in outlook?		
4. Do you have folders in outlook to categorize your email?		
5. If yes, do these folders help you find your email quickly?		
6. Are your email records stored in a shared location accessible by other branch staff?		
7. How do others access significant email records if you are unavailable?		
8. Please identify your primary challenges associated with email (e.g. storage, naming, searching, finding, sharing, duplication, destruction).		

Question:	**Y**	**N**
Additional Comments: (Inquire with the interviewee about concerns, best practices and ideas for improvement)		

C) Physical Records - Paper

How do you create, store, scan and find physical records like file folders, annotated maps and drawings, signed contracts, field books, etc. Including CRMS and TRIM. s.13

s.13

Question:	**Y**	**N**
1. Do you keep records in paper format? If yes, how are your files organized?		
2. Do you use naming conventions, labels, other identifiers, for paper records? Please describe.		
3. Are your paper records tracked in any systems (e.g. TRIM, file lists)? If yes, please describe.		
4. Do you have a legal or business reason for keeping paper records? If yes, please describe.		

s.13

s.13

Question:	**Y**	**N**
5. Are there scanning projects being planned for any paper records? If yes, please describe.		
6. Can you identify paper records that would be good candidates for scanning? If yes, please describe.		
7. Can you identify any paper records that could instead be received or kept in electronic format? If yes, please describe.		
8. Please identify your primary challenges associated with paper records. (e.g. storage, naming, searching, finding, sharing, duplication, destruction).		
Additional Comments: (Inquire with the interviewee about concerns, best practices and ideas for improvement)		

s.13

[redacted]

Ministry of Transportation and Infrastructure, Infrastructure & Major Projects
Information Management Current State Assessment - Interview Questions

D) Data in Systems

How do you access, enter, and analyze data from apps and systems like SharePoint websites, Traffic GIS, Development Approvals System (DAS), eApprovals, CLIFF, etc. s.13

s.13

Question	Y	N
1. Do you use business specific applications/systems, such as a database? If yes, what are the systems, and is your branch the primary owner?		
2. Do any of the systems store documents? If yes, please describe.		
3. Do any of the systems store the official copy of documents or data? Are there copies found elsewhere (e.g. LAN, paper)? If yes, please describe.		
4. Is there system administration documentation that describes the system and related documents and data (i.e. inputs, processes, and outputs)? If yes, where is it stored?		
5. Are documents and data routinely purged from the system, or exported and captured elsewhere as the official records? If yes, please describe.		

s.13

s.13

s.13

Question	**Y**	**N**
6. Who is the current Information Management Branch business portfolio contact for the systems?		
7. Please identify your primary challenges associated with business specific systems. (e.g., searching, using (reliability), producing, sharing, reporting, exporting).		
Additional Comments: (Inquire with the interviewee about concerns, best practices and ideas for improvement)		

E) Procedures and Practices

~~E)~~ Where/Who do you go to when you're not sure how to manage or find government information? How do you monitor yourself to ensure you manage records in a consistent way? How do you use official BC Government RM policy and procedure, and do you have any great office processes?

Question	**Y**	**N**
1. Do you have branch-specific business procedures for information management? If yes, a) Are these procedures documented and readily available? b) Are colleagues aware of these procedures?		

s.13

Question	**Y**	**N**
2. Can you easily find business critical information?		
3. How long do you spend looking for information on an average day? On a good day? On a bad day?		
4. List some of your challenges in finding information.		
5. Do you know how to classify your business critical information according to ARCS/ORCS?		
6. Does your branch have specific employees tasked with information management functions or responsibilities? If yes, a) Identify position(s) and/or current staff: b) What are their assigned functions/responsibilities?		
7. Would it be helpful if your branch sent out communications regarding internal information management standards and processes?		
8. Did you receive any **branch specific** information management		

s.13

Question	**Y**	**N**
training when you started with the branch?		
9. Do you know where to find policy regarding information management and departing employees?		
10. Please identify the primary challenges associated with your branch information management procedures and practices.		
Additional Comments: (Inquire with the interviewee about concerns, best practices and ideas for improvement)		

F) Corporate Training and Support

~~F)~~ Do you use GRS training services? Do you have contact information for your RM questions about schedules (ARCS/ORCS), EDRMS (TRIM) and Physical Records Storage? What training and coaching do you wish you had?

Question	**Y**	**N**
1. Are you aware that there is corporate training on information management offered by a central agency, Government Records Services?		
2. Have you taken corporate training on information management? If yes, what kind of training and was it helpful?		

Question	Y	N
3. Do you know who to contact for support (e.g. TRIM, advice, records destruction, off-site storage)? If yes, who are your contacts?		
4. Are you aware of online resources? If yes, please identify resources used.		
5. Are you aware of new digital requirements are coming under the new *Information Management Act*?		
6. What challenges would your branch face in operating digitally in the near future?		
7. Please identify your primary challenges associated with information management training and support.		
8. These are the current training offerings for information management offered by Government Records Service. Please provide your ranking of their value for yourself, using a scale of 1-5, with 5 being the greatest.		

Question	Y	N

Course	Ranking 1-5
Orientation to records management	
E-mail best practices	
LAN organization (shared drives)	
TRIM Information Worker	
TRIM End User	
TRIM on-site disposal procedures	
TRIM off-site transfer procedures	
On-site destruction of records	

9. What is your preferred way to access and receive training and support – for example do you prefer in-person training, individual support, self–directed learning and /or e-learning?

Additional Comments: (Inquire with the interviewee about concerns, best practices, and ideas for improvement or new course offerings)

Closing Question:
Describe your desired future state for information management? *(What would you change? What problems do you wish were gone? What challenges resolved?)*

Ministry of Transportation and Infrastructure, Infrastructure & Major Projects
Information Management Current State Assessment - Interview Questions

Date:	**Branch:**
Interviewer Name(s):	**Interviewee Name:** **Function in Branch:**

Names & Methodology

[5 min?]

Introduction

Tell me about your job. What do you do? What tools do you use to do your job? Are you part of a team or do you work independently?

[10 min?]

Ministry of Transportation and Infrastructure, Infrastructure & Major Projects
Information Management Current State Assessment - Interview Questions

A) Electronic Documents

How do you create, share, find and delete documents like spreadsheets (Excel), reports (Word and PDF), images, drawings, etc.

Question:	**Y**	**N**
1. Do you use naming standards for electronic folders and/or documents? If yes, please describe.		
2. Where do you store your electronic documents? (e.g. TRIM, LAN, SharePoint, USB, etc.):		
3. Are the documents you need readily available to you?		
4. Are these documents accessible to everyone with a need to use them?		
5. Do you consider how you will share a document with others when you are creating and saving documents?		
6. Do you know which electronic documents to keep?		
7. Are you confident that you can identify transitory electronic documents? If no, can you think of anything that would help you identify a transitory record?		
8. Do you know how long you need to keep electronic documents?		

Question:	**Y**	**N**
9. What happens to your electronic documents when you are “finished” with them?		
10. Do you keep both electronic and paper copies of the same documents? a) In what circumstances? b) Do you know which copy you would use or share as the final version?		
11. Please identify your primary challenges associated with electronic documents (e.g. storage, naming, searching, finding, sharing, duplication, destruction).		
Additional Comments: (Inquire with the interviewee about concerns, best practices and ideas for improvement)		

[17 min?]

Ministry of Transportation and Infrastructure, Infrastructure & Major Projects
Information Management Current State Assessment - Interview Questions

B) Email

How do you organize, share, find and delete emails and attachments.

Question:	Y	N
1. Do you have naming standards for email subject lines? If yes, please describe.		
2. Do you have team/branch email rules (e.g. use of fields, attachments)? If yes, please describe.		
3. Do you store your email anywhere other than in outlook?		
4. Do you have folders in outlook to categorize your email?		
5. If yes, do these folders help you find your email quickly?		
6. Are your email records stored in a shared location accessible by other branch staff?		
7. How do others access significant email records if you are unavailable?		
8. Please identify your primary challenges associated with email (e.g. storage, naming, searching, finding, sharing, duplication, destruction).		

Question:	**Y**	**N**
Additional Comments: (Inquire with the interviewee about concerns, best practices and ideas for improvement)		

[24 min?]

C) Physical Records - Paper

How do you create, store, scan and find physical records like file folders, annotated maps and drawings, signed contracts, field books, etc. Including CRMS and TRIM.

Question:	**Y**	**N**
1. Do you keep records in paper format? If yes, how are your files organized?		
2. Do you use naming conventions, labels, other identifiers, for paper records? Please describe.		
3. Are your paper records tracked in any systems (e.g. TRIM, file lists)? If yes, please describe.		
4. Do you have a legal or business reason for keeping paper records? If yes, please describe.		

Question:	**Y**	**N**
5. Are there scanning projects being planned for any paper records? If yes, please describe.		
6. Can you identify paper records that would be good candidates for scanning? If yes, please describe.		
7. Can you identify any paper records that could instead be received or kept in electronic format? If yes, please describe.		
8. Please identify your primary challenges associated with paper records. (e.g. storage, naming, searching, finding, sharing, duplication, destruction).		
Additional Comments: (Inquire with the interviewee about concerns, best practices and ideas for improvement)		

[31 min?]

D) Data in Systems

How do you access, enter, and analyze data from apps and systems like SharePoint websites, Traffic GIS, Development Approvals System (DAS), eApprovals, CLIFF, etc.

Question	Y	N
1. Do you use business specific applications/systems, such as a database? If yes, what are the systems, and is your branch the primary owner?		
2. Do any of the systems store documents? If yes, please describe.		
3. Do any of the systems store the official copy of documents or data? Are there copies found elsewhere (e.g. LAN, paper)? If yes, please describe.		
4. Is there system administration documentation that describes the system and related documents and data (i.e. inputs, processes, and outputs)? If yes, where is it stored?		
5. Are documents and data routinely purged from the system, or exported and captured elsewhere as the official records? If yes, please describe.		

Question	**Y**	**N**
6. Who is the current Information Management Branch business portfolio contact for the systems?		
7. Please identify your primary challenges associated with business specific systems. (e.g., searching, using (reliability), producing, sharing, reporting, exporting).		
Additional Comments: (Inquire with the interviewee about concerns, best practices and ideas for improvement)		

[38 min?]

E) Procedures and Practices

Where/Who do you go to when you're not sure how to manage or find government information? How do you monitor yourself to ensure you manage records in a consistent way? How do you use official BC Government RM policy and procedure, and do you have any great office processes?

Question	**Y**	**N**
1. Do you have branch-specific business procedures for information management? If yes, a) Are these procedures documented and readily available? b) Are colleagues aware of these procedures?		

Ministry of Transportation and Infrastructure, Infrastructure & Major Projects
Information Management Current State Assessment - Interview Questions

Question	**Y**	**N**
2. Can you easily find business critical information?		
3. How long do you spend looking for information on an average day? On a good day? On a bad day?		
4. List some of your challenges in finding information.		
5. Do you know how to classify your business critical information according to ARCS/ORCS?		
6. Does your branch have specific employees tasked with information management functions or responsibilities? If yes, a) Identify position(s) and/or current staff: b) What are their assigned functions/responsibilities?		
7. Would it be helpful if your branch sent out communications regarding internal information management standards and processes?		

Question	**Y**	**N**
8. Did you receive any **branch specific** information management training when you started with the branch?		
9. Do you know where to find policy regarding information management and departing employees?		
10. Please identify the primary challenges associated with your branch information management procedures and practices.		
Additional Comments: (Inquire with the interviewee about concerns, best practices and ideas for improvement)		

[45 min?]

F) Corporate Training and Support

Do you use GRS training services? Do you have contact information for your RM questions about schedules (ARCS/ORCS), EDRMS (TRIM) and Physical Records Storage? What training and coaching do you wish you had?

Question	**Y**	**N**
1. Are you aware that there is corporate training on information management offered by a central agency, Government Records Services?		

Ministry of Transportation and Infrastructure, Infrastructure & Major Projects
Information Management Current State Assessment - Interview Questions

Question	Y	N
2. Have you taken corporate training on information management? If yes, what kind of training and was it helpful?		
3. Do you know who to contact for support (e.g. TRIM, advice, records destruction, off-site storage)? If yes, who are your contacts?		
4. Are you aware of online resources? If yes, please identify resources used.		
5. Are you aware of new digital requirements are coming under the new *Information Management Act*?		
6. What challenges would your branch face in operating digitally in the near future?		
7. Please identify your primary challenges associated with information management training and support.		

Question	Y	N

8. These are the current training offerings for information management offered by Government Records Service. Please provide your ranking of their value for yourself, using a scale of 1-5, with 5 being the greatest.

Course	Ranking 1-5
Orientation to records management	
E-mail best practices	
LAN organization (shared drives)	
TRIM Information Worker	
TRIM End User	
TRIM on-site disposal procedures	
TRIM off-site transfer procedures	
On-site destruction of records	

9. What is your preferred way to access and receive training and support – for example do you prefer in-person training, individual support, self–directed learning and /or e-learning?

Additional Comments: (Inquire with the interviewee about concerns, best practices, and ideas for improvement or new course offerings)

[52 min?]

Closing Question:
Describe your desired future state for information management? *(What would you change? What problems do you wish were gone? What challenges resolved?)*

This worksheet was created as part of a MoTI IM Assessment project.

The data in this worksheet was collected by Gislene Guenard and Bruce N. Smith in 2017-Q4 and 2018-Q1.

1 hour interviews were conducted in person and notes were take by both interviewers on paper with pens, then the information was transcribed here shortly after the interview (+/- 1 business week).

The paper draft notes may contain additional acronyms or ideas for planning purposes, a selection of these could be scanned according to good digitization standards and stored for further interim analysis, if business leads decide they have information of value.

Any draft notes selected as having value will be saved here:

Page 150 of 444 to/à Page 151 of 444

Withheld pursuant to/removed as

s.13

Page 152 of 444

Withheld pursuant to/removed as

s.13 ; s.22

Page 153 of 444 to/à Page 159 of 444

Withheld pursuant to/removed as

s.13

Ministry of Transportation and Infrastructure, Infrastructure & Major Projects
Information Management Current State Assessment - Interview Questions

Date:	**Branch:**
Interviewer Name(s):	**Function in Branch:**

This assessment is part of an IM Strategy prioritized by your DMO.

The assessment will help:

- Give voice to staff requests and questions
- Capture a baseline and measure change
- Enable evidence-based decision-making
- Prioritize improvements
- Raise awareness of Information and Records Management (IM / RM)

No one has perfect IM, and these results will be rolled up into anonymous reports. So don't worry and respond freely.

We know that some of the yes/no questions depend on context, and there is some repetition in the questions. It's by design to provide a clear outline of the current state without taking too much of your time. Just answer as best you can.

Introduction:

Tell us a bit about your job.

What do you do? What tools do you use to do your job? Are you part of a team or do you work independently?

A) Electronic Documents

How do you create, share, find and delete documents like spreadsheets (Excel), reports (Word and PDF), images, drawings, etc.

Question:	Y	N	Other
Are the documents you need readily available to you?			
Do you store documents in a location so that they can easily be shared with colleagues?			
Do you know how long you need to keep electronic documents?			
Are you confident that you can identify transitory electronic documents?			
Do you keep both electronic and paper copies of the same documents?			
Do you use naming standards for electronic folders and/or documents? Please describe:			
Where do you store your electronic documents? (e.g. TRIM, LAN, SharePoint, USB, etc.):			
What happens to your electronic documents when you are “finished” with them?			
Please identify your primary challenges associated with electronic documents (e.g. storage, naming, searching, finding, sharing, duplication, destruction).			

B) Email

How do you organize, share, find and delete emails and attachments.

Question:	**Y**	**N**	**Other**
Do you have naming standards for email subject lines?			
Do you have team/branch email rules (e.g. use of fields, attachments)?			
Do you store your email anywhere other than in outlook?			
Do you have folders in outlook to categorize your email?			
If yes, do these folders help you find your email quickly?			
Are your email records stored in a shared location accessible by other branch staff?			
How do others access significant email records if you are unavailable?			
Please identify your primary challenges associated with email (e.g. storage, naming, searching, finding, sharing, duplication, destruction).			

C) Physical Records - Paper

How do you create, store, scan and find physical records like file folders, annotated maps and drawings, signed contracts, field books, etc. Including CRMS and TRIM.

Question:	**Y**	**N**	**Other**
Do you keep records in paper format?			
Do you use naming conventions, labels, other identifiers, for paper records?			
Are your paper records tracked in any systems (e.g. TRIM, file lists)?			
Do you have a legal or business reason for keeping paper records?			
Are there scanning projects being planned for any paper records?			
Can you identify paper records that would be good candidates for scanning? Please describe:			
Please identify your primary challenges associated with paper records. (e.g. storage, naming, searching, finding, sharing, duplication, destruction).			

D) Data in Systems

How do you access, enter, and analyze data from apps and systems like SharePoint websites, Traffic GIS, Development Approvals System (DAS), eApprovals, CLIFF, Databases, etc.

Question	Y	N	Other
Do you use business specific applications / software, such as a database? Please describe:			
Do any of the systems store documents?			
Do any of the systems store the official copy of documents or data?			
Are documents and data routinely purged from the system, or exported and captured elsewhere as the official records?			
Who is the current Information Management Branch business portfolio contact for the systems?			
Please identify your primary challenges associated with business specific systems. (e.g., searching, using (reliability), producing, sharing, reporting, exporting).			

E) Procedures and Practices

Where or who do you go to when you're not sure how to manage or find government information? How do you monitor yourself to ensure you manage records in a consistent way? How do you use official BC Government RM policy and procedure, and do you have any great office processes?

Question	Y	N	Other
Did you receive any **branch specific** information management training when you started with the branch?			
Do you have branch-specific business procedures for information management?			
Can you easily find information required for your daily operational responsibilities?			
Do you know how to classify your business critical information according to ARCS/ORCS?			
Does your branch have specific employees tasked with information management functions or responsibilities?			
Would it be helpful if your branch communicated internal information management standards and processes?			
How long do you spend looking for information on an average day? On a good day? On a bad day?			
List some of your challenges in finding information.			

F) Corporate Training and Support

Do you use GRS training services? Do you have contact information for your RM questions about schedules (ARCS/ORCS), EDRMS (TRIM) and Physical Records Storage? What training and coaching do you wish you had?

Question	**Y**	**N**	**Other**
Are you aware that there is corporate training on information management offered by a central agency?			
Have you taken corporate training on information management?			
Do you know who to contact for support (e.g. TRIM, advice, records destruction, off-site storage)?			
Are you aware of online resources?			
Are you aware of new digital requirements are coming under the new *Information Management Act*?			
What challenges would your branch face in operating digitally in the near future?			
Please identify your primary challenges associated with information management training and support.			

Please rank the following GRS courses for yourself. 1 is low and 5 is high.

Course	Ranking 1-5
Orientation to records management	
E-mail best practices	
LAN organization (shared drives)	
TRIM Information Worker	
TRIM End User	
TRIM on-site disposal procedures	
TRIM off-site transfer procedures	
On-site destruction of records	

What is your preferred way to access and receive training and support?

For example: in-person training, individual support, self–directed learning, e-learning.

Closing Question:

Describe an improved future state for information management.

What would you change? What problems do you wish were gone? What challenges resolved? What would make your job easier?

Any additional comments?

[ministry name], [division/branch name]
Information Management Assessment - Interview Questions

Date:	**Branch:**
Interviewer Name(s):	**Function in Branch:**

The assessment will help:

- Give voice to staff requests and questions
- Capture a baseline and measure change
- Enable evidence-based decision-making
- Prioritize improvements
- Raise awareness of Information and Records Management (IM / RM)

This assessment is part of an [for example: initiative prioritized by your Deputy Minister who wants to improve IM across the Ministry].

No one has perfect IM, and these results will be rolled up into anonymous reports. So don't worry and respond freely.

We know that some of the yes/no questions depend on context, and there is some repetition in the questions. It's by design to provide an outline of the current state without taking too much of your time. Just answer as best you can.

Introduction:

Tell us a bit about your job.

What do you do?
What tools do you use to do your job?
What teams do you work with or do you work independently?

A) Electronic Documents

How do you create, share, find and delete documents like spreadsheets (Excel), reports (Word and PDF), images, drawings, etc.

Question:	**Y**	**N**	**Other**
Are the documents you need readily available to you?			
Do you store documents in a location so that they can easily be shared with colleagues?			
Do you know how long you need to keep electronic documents?			
Are you confident that you can identify transitory electronic documents?			
Do you keep both electronic and paper copies of the same documents?			
Do you use naming standards for electronic folders and/or documents? Please describe:			
Where do you store your electronic documents? (e.g. TRIM, LAN, SharePoint, USB, etc.):			
What happens to your electronic documents when you are “finished” with them?			
Please identify your primary challenges associated with electronic documents (e.g. storage, naming, searching, finding, sharing, duplication, destruction).			

B) Email

How do you organize, share, find and delete emails and attachments.

Question:	Y	N	Other
Do you have naming standards for email subject lines?			
Do you have team/branch email rules (e.g. use of fields, attachments)?			
Do you store your email anywhere other than in outlook?			
Do you have folders in outlook to categorize your email?			
If yes, do these folders help you find your email quickly?			
Are your email records stored in a shared location accessible by other branch staff?			
How do others access significant email records if you are unavailable?			
Please identify your primary challenges associated with email (e.g. storage, naming, searching, finding, sharing, duplication, destruction).			

C) Physical Records - Paper

How do you create, store, scan and find physical records like file folders, annotated maps and drawings, signed contracts, field books, etc. Including CRMS and TRIM.

Question:	**Y**	**N**	**Other**
Do you keep records in paper format?			
Do you use naming conventions, labels, other identifiers, for paper records?			
Are your paper records tracked in any systems (e.g. TRIM, file lists)?			
Do you have a legal or business reason for keeping paper records?			
Are there scanning projects being planned for any paper records?			
Can you identify paper records that would be good candidates for scanning? Please describe:			
Please identify your primary challenges associated with paper records. (e.g. storage, naming, searching, finding, sharing, duplication, destruction).			

D) Data in Systems

How do you access, enter, and analyze data from apps and systems like SharePoint websites, eApprovals, CLIFF, Databases, [client specific applications], etc.

Question	**Y**	**N**	**Other**
Do you use business specific applications / software, such as a database? Please describe:			
Do any of the systems store documents?			
Do any of the systems store the official copy of documents or data?			
Are documents and data routinely purged from the system, or exported and captured elsewhere as the official records?			
Who is the current [Information Management Branch] business portfolio contact for the systems?			
Please identify your primary challenges associated with business specific systems. (e.g., searching, using (reliability), producing, sharing, reporting, exporting).			

E) Procedures and Practices

Where or who do you go to when you're not sure how to manage or find government information? How do you monitor yourself to ensure you manage records in a consistent way? How do you use official BC Government RM policy and procedure, and do you have any great office processes?

Question	Y	N	Other
Did you receive any **branch specific** information management training when you started with the branch?			
Do you have branch-specific business procedures for information management?			
Can you easily find information required for your daily operational responsibilities?			
Do you know how to classify your business critical information according to ARCS/ORCS?			
Does your branch have specific employees tasked with information management functions or responsibilities?			
Would it be helpful if your branch communicated internal information management standards and processes?			
How long do you spend looking for information on an average day? On a good day? On a bad day?			
List some of your challenges in finding information.			

F) Corporate Training and Support

Do you use GRS training services? Do you have contact information for your RM questions about schedules (ARCS/ORCS), EDRMS (TRIM) and Physical Records Storage? What training and coaching do you wish you had?

Question	**Y**	**N**	**Other**
Are you aware that there is corporate training on information management offered by a central agency?			
Have you taken corporate training on information management?			
Do you know who to contact for support (e.g. TRIM, advice, records destruction, off-site storage)?			
Are you aware of online resources?			
Are you aware of new digital requirements are coming under the new *Information Management Act*?			
What challenges would your branch face in operating digitally in the near future?			
Please identify your primary challenges associated with information management training and support.			

Please rank the following GRS courses for yourself. 1 is not useful, 5 is very useful, or not applicable.

Course	Ranking 1-5
Orientation to records management	
E-mail best practices	
LAN organization (shared drives)	
TRIM Information Worker	
TRIM End User	
TRIM on-site disposal procedures	
TRIM off-site transfer procedures	
On-site destruction of records	

What is your preferred way to access and receive training and support?

For example: in-person training, individual support, self–directed learning, e-learning.

Closing Question:

Describe an improved future state for information management.

What would you change? What problems do you wish were gone? What challenges resolved? What would make your job easier?

Any additional comments?

Practice Review Program

Interview Questions for All Domains

Privacy, Compliance and Training Branch

Introduction and Purpose

Introduce Auditors conducting interview

We are from the Privacy, Compliance and Training Branch in the Ministry of Finance's Corporate Information and Records Management Office. We are here to meet with you today to gather information in relation to an **audit** that we are conducting.

We are conducting a **baseline audit** of your ministry's information management practices.

The purpose of a baseline audit is to assess the maturity of your ministry's information management practices against a number of evaluation criteria that cover privacy, records management, FOI/information access, and the protection of information.

Process

In terms of process, we will be asking you questions and taking notes and may ask you clarifying questions. If at any point you wish to take a break please let us know.

We are meeting with a number of individuals from your ministry in order to gather a fulsome understanding of your ministry's information management practices. As part of this we may ask you to send emails or other documents following this meeting, and may need to meet with you again if we find that we have any additional questions.

At the conclusion of this process we will be preparing a final report which will be submitted to your deputy minister along with other executives from your ministry as directed by your deputy. Our report will document our overall assessment and scoring of maturity at the ministry level. Our report will not name or identify the ministry staff who were involved in this process, and will not be making any assessments of individual level practices.

However, before the report is finalized, it will be shared with designated ministry representatives to ensure the ministry has an opportunity for review and to let us know if we missed anything or were incorrect in any way. If we are unclear on something or want to be sure, we may also ask you to review and confirm information or a conclusion we may arrive at.

Finally, any information you provide today will be maintained in confidence and will be used only for the purposes of this audit/assessment, or as may be required by law or government policy (e.g. FOI request, subject to redactions).

Do you have any questions before we begin?

PRACTICE REVIEW PROGRAM – PRIVACY QUESTIONS FOR MPO

Interviewee Name:	**Ministry Privacy Officer**
Interviewer Name	
Date:	

#	Criteria	Questions	Response	Documents/Evidence	Summary
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 defined.	Does your job description specify all required privacy related duties?	-		
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.	Has your DM delegated any privacy duties specifically to you? If so, has a FOIPPA Delegation Instrument been completed? May I get a copy?			
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 in place, and current. Delegation instruments are maintained and communicated to CIRMO.	Have you, in turn, delegated any duties to others? If so, has a PMAP Delegation Instrument been completed? May I get a copy?			
1.4	**Privacy Policies/Procedures**	Does your ministry require any ***Ministry-***			

#	Criteria	Questions	Response	Documents/Evidence	Summary
	Ministry-specific privacy policies and procedures, incorporating Ministry-specific privacy requirements, have been developed and deployed, where appropriate.	***specific*** privacy policies, in addition to PMAP? If so, are these policies in effect? Copy or link please			
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.	Have all ministry employees completed IM117 shortly after being hired, and is refresher training provided every two years? Is regular training scheduled and do you augment staff awareness with emails, posters or similar? Copies pls.			
2.2	**Role Based Privacy Training** A process is in place to develop and deliver additional privacy training (beyond IM117) to employees.	For staff members who require additional, ***privacy-specific*** training (beyond IM 117), do you have a process in place to identify them and to schedule required training? Is this process documented? Copy pls.			
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.	Have you developed and communicated your ministry's process for PIA requirements? If so, what communication channels are used to keep ministry employees updated and aware of these materials (policies, procedures for completion of PIA, etc.) Copies pls. STAFF: Have you been provided with written information/instructions regarding PIAs?			

#	Criteria	Questions	Response	Documents/Evidence	Summary
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.	Do you maintain an inventory of completed or in-progress PIAs? How do you keep track of outstanding items for follow-up? Copies pls.			
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).	Have you developed a process to ensure that your ministry's employees are completing PIAs as defined in PMAP Section 2.3? Has this process been documented and is it regularly followed? Copy pls. How are you made aware of upcoming projects or activities that may require PIAs? What awareness materials or activities do you use to educate staff about PIAs? Copies pls. STAFF: Are you aware that PIAs must be completed prior to the start of any new project, activity or initiative?			
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.	Do you have a process to identify when ISAs, RAs, CPAs and IPAs are required? How is the process communicated to staff? How do you ensure that you are involved in the development and/or updating of these agreements? Copies pls.			
4.2	**ISAs are reported to the CIRMO**	What documented process do you use to			

#	Criteria	Questions	Response	Documents/Evidence	Summary
	The MPO has a process in place to ensure ISAs are reported to CIRMO for entry into the Personal Information Directory (PID) once completed.	ensure that ISAs are reported to CIRMO for entry into the PID? Copy pls			
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.	Do you maintain an inventory of completed or in-progress RAs? How do you keep track of outstanding items for follow-up? Copies pls.			
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.	How do you ensure that parties are in compliance with privacy requirements as outlined in agreements? Do you have a documented process? Copy pls.			
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.	What process is used to ensure that PP Schedules are included in all service provider contracts that contain personal information? Do all contract managers (responsible business units) make you aware of these contracts? How is this process communicated to employees? Copy pls. MANAGER: If you manage contracts containing personal information, do you have a defined process that ensures PPS are included in each contract? Copy pls.			

#	Criteria	Questions	Response	Documents/Evidence	Summary
5.2	**Inventory of Access to PI** 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.	What is your process for maintaining an inventory of service providers or volunteers with access to personal information within your ministry's custody and control? What control process is in place to ensure inventory is kept up to date and all changes are reflected in the inventory? Copies pls			
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.	How do you ensure that all service providers and volunteers have had mandatory privacy training ***prior to*** providing services? Is this a documented process? Copies pls			
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)	How do you monitor service provider compliance with privacy requirements? Do you have a documented process in place to address instances of non-compliance? (E.g. call 7-7000)			
6.1	**Create and Maintain Personal Information Inventory** A procedure exists to create and maintain a Personal Information Inventory, and to	Future state. General question only re awareness and preparedness			

#	Criteria	Questions	Response	Documents/Evidence	Summary
	create it within one year of the Personal Information Inventory Policy being published.				
6.2	**Reporting to CIRMO** A procedure exists for the creation and reporting to CIRMO of Personal Information Banks as required.	Do you have documented policy or procedures for the creation and reporting of PIBs? How is the procedure for managing PIB communicated to the employees? How do you ensure that employees have the awareness of and accessibility to the policy or procedures? Copies pls.			
6.3	**Health Information Banks** *For the Ministry of Health:* A procedure exists for the creation and reporting (to CIRMO) of Health Information Banks.	**Health only:** What is your process for ensuring that HIBs are created appropriately and reported to CIRMO? How do you ensure that employees have awareness of and accessibility to the policy or procedures?			
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.	Is there a documented process for reviewing the PID annually? How do you ensure that all **PIAs, ISAs, PIBs** and where applicable **HIBs** are submitted and recorded accurately? What is the process to correct entries? Copies pls.			
7.1	**Reporting Foreign Demands** A procedure is in place for reporting foreign demands for disclosure to the CIRMO.	Do you have a policy and/or documented procedure related to the reporting of foreign demands to CIRMO as per Section 30.2 of FOIPPA? Copies pls.			

#	Criteria	Questions	Response	Documents/Evidence	Summary
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.	How do you communicate to staff that all information incidents are to be reported immediately to CIRMO? How do you track incidents to ensure that all instructions from CIRMO are followed and that subsequent recommendations are implemented? If this process is documented, pls provide a copy STAFF AND MANAGER: Are you familiar with the process for reporting information incidents?			

PRACTICE REVIEW PROGRAM – RECORDS QUESTIONS

Interviewee Name:	
Interviewer Name	
Date:	

Records Management					
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.	Do you know if there is a dedicated RM person in your ministry? How are RM responsibilities communicated to staff? Have you seen any written procedures or guidance on your own responsibilities for records management? (S) Copies pls			
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.	Do you have any ***Ministry-specific*** policies or procedures related to records management? (other than Core Policies) If so, how are these RM policies/procedures communicated to staff? Copies pls (M)			

2.1	**Mandatory Employee Training** Employees have completed mandatory training related to records management (IM117).	- Other than IM117, have you or any of your staff taken any records management training? If so, what training? - How is completion of staff training monitored? If there are any gaps how is it addressed? - How do you confirm that staff understands their RM responsibilities?			
2.2	**Role Specific Training** Individuals have received additional, role-specific records management training where appropriate.	Some roles require specialized training in Records Management. If your role has this requirement, have your received the appropriate training? (S)			
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.	Does your area use TRIM to organize its records? If not, how are your records organized so that they are managed according to their function and to approved retention requirements? Do you have any documented procedures about records classification, and if so, how are these communicated to staff? (M) Copies pls s.13			

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.				
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**.**	Are your records scheduled and if so, do you have a documented process to ensure that records are reviewed for currency of existing schedules? How do you identify information not covered by an approved schedule? If you have records that are not scheduled, do you have a documented process to request schedules? Copies pls (M)			
5.2	**Records Retention Holds and Disposition** The ministry has procedures to retain, dispose of, transfer, or archive government information based on official policies, specifications, schedules, guidelines, and procedures published by GRS. In the case of a legal hold or FOI request, the ministry has processes in place to ensure that such	How do you ensure that records are retained according to the appropriate schedules? In the case of a legal hold or FOI request, do you have a documented process to ensure that those records are not destroyed? Copies pls (M) s.13			

	records are not destroyed.	s.13			
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.	- Do you have specific procedures related to business requirements to identify and protect digital records scheduled for archiving? Copies pls			
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.	Does your ministry have documented procedures for the transfer of records to bodies covered by the IMA? If so, do those procedures include guidance to maintain the chain of custody and continuity of control for records during transfer? Copies pls (M)			
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.	Does your ministry transfer records to third parties that are non-IMA bodies? If so, do you have a process in place to ensure that that transfers are completed in accordance with an appropriate legal instrument? Copies pls. (M)			
7.1	**Manage Information in Recordkeeping**	How do you ensure that all government			

	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.	records held in your ministry are kept in approved record keeping systems? Do you have a process in place to remind staff that non-transitory government information held in Outlook (e.g.) is to be transferred for retention in a secure approved recordkeeping system? Copies pls (M)			
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.	Do you have documented procedures for the management and storage of physical records, both on and offsite? Copies pls (M)			
7.3	**Inventory of Ministry Systems and Repositories** The ministry maintains an inventory of ministry systems and repositories that manage and/or store government information	Do you maintain an up-to-date inventory of the information systems and repositories in use in your ministry? Copy pls (M)			

PRACTICE REVIEW PROGRAM –INFORMATION ACCESS QUESTIONS

Interviewee Name:	
Interviewer Name	
Date:	

ACCESS					
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 is informed and aware of the appropriate response to FOI requests (e.g., how to conduct a comprehensive and timely search for responsive records~~.),~~ s.13	Are you familiar with the procedures around Information Access and the Duty to Assist? (S) Does your Ministry have documented procedures for Information Access and the DtA? How is your staff informed of their FOI accountabilities and responsibilities ?(M)			
1.2	**Information Access Accountability** Accountabilities for FOI requests are assigned, and roles and responsibilities are clearly defined.	Is there designated person/role within your ministry who is accountable for responding to FFOI requests? (M)			
2.1	**Employee Training**	- Other than IM117 have staff received			

	Employees have completed mandatory (IM117) training related to FOI/ Information Access.	any additional training on processing FOI information requests? - How are staff made aware of their FOI responsibilities, e.g. duty to assist, other FOI policies/procedures?			
2.2	**Role Specific Training** Individuals have received additional, role-specific FOI/Information Access training where appropriate (e.g. ministerial staff, FOI co-ordinators).	If your role requires you to have additional FOI- related training, have you received such training? (S) If you have a staff member who requires additional FOI-related training, how do you ensure such training is provided? (M)			
3.1	**Dedicated Public Servant** A dedicated Public Servant is designated as the person responsible and accountable for responding to all FOI requests involving a Minister's office. The DPS must retain a current list of all Ministerial staff that is shared on an ongoing basis with IAO.	Question should be directed to Minister's office only.			
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.	Does your ministry have a documented process for tracking, monitoring and escalation where indicated of your responses to FOI requests? (M)			

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.	Do you manage service providers and/or contractors? If so, how do you ensure that they are in compliance with ministry procedures regarding FOI requests? Is there a documented process that shows how compliance is monitored? (M)			

PRACTICE REVIEW PROGRAM – INFORMATION PROTECTION QUESTIONS

Interviewee Name:	
Interviewer Name	
Date:	

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.	MISO Do you have a documented Information Security Program? If so, are responsibilities for the program documented and assigned?			
1.2	**Employee Training** Employees have completed training related to the protection of government information (IM117 and IM118).	- Other than IM117, have any or all of your staff received additional information protection / security training?			
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				
1.4	**External Parties** Assessment of risks from external party	MISO and Management Are risk assessments conducted before			

	access to government information, information systems or information processing facilities are performed and appropriate security controls implemented prior to granting access.	granting access to external parties to government information? TW: how is the RA conducted?			
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.	MISO Does your Ministry/area maintain an inventory of all information systems and assets? TW: is this inventory different from the inventory in Records Mgmt 7.3?			
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.	Other than confidentiality agreements, acceptable use policy, etc., do you have any additional documented processes regarding employee accountabilities for the protection of personal and sensitive information? How do you confirm/ensure that staff understands their responsibilities? (M)			
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.	In addition to Core Policies, do you have any other documented procedures to guide staff about reducing the risk to information due to unauthorized access or loss? **(M)** MISO - How do you ensure all data and software is erased from the equipment prior to disposal? -			

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.	MISO Do you have a documented process (beyond referring to Core Policies) to advise staff about what to how to prevent malicious code infections on information systems and infrastructure? (e.g.' Don't click on that attachment' posters or reminder emails?)			
1.9	**Security Classification** Records are organized so that security classifications can be applied to protect different classes of information based on their sensitivity.	MPO/MISO/Manager - Do you classify or categorize your records by sensitivity? s.13			
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.	How do you manage portable media? Do you maintain an inventory of such devices? How do you ensure that any such media are encrypted, and information contained therein is transferred as soon as possible to appropriate government record keeping systems? Is the process documented and made available to staff? (M)			
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.	How do you secure your unattended computer equipment (desktop, laptop, cell phone, etc.) to prevent unauthorized access or theft? Do you ensure that your workstation is locked? Do you maintain a clean desk policy? (S)			

	-Users must ensure the safety of sensitive information from unauthorized access, loss or damage.				
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.	Do you have a documented process covering the full range of access management and does it apply to both staff and contractors? Do you periodically (at least annually) monitor access to systems to ensure that only authorized and appropriate personnel have access to information systems? Do you have a documented on-boarding and off-boarding process to ensure that access is granted, changed or revoked in a timely manner? (M) or (SME)			
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	Are security controls identified for new or changes to the existing information systems? (e.g. risk assessment conducted?) Do you have a documented process to ensure that security risk and controls are identified prior to implementation or modification of new or existing systems? (MISO)			

	former STRA) process, and controls are implemented and reviewed prior to implementation.				
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.	MISO - Are regular assessment conducted to evaluate risks associated with information system vulnerabilities? - How do you ensure that vulnerabilities are remediated? s.13			
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.	MPO/MISO - Do you monitor, review and retain audit logs for exceptions and information security events like tempering and unauthorized access? s.13			
1.16	**Business Continuity Management** Business continuity management processes and plans have been developed tested,	Do you have a documented, up-to-date BCP in your Ministry? If so, when last was it tested? (M) and (MISO)			

	maintained, updated and they include provisions to maintain security and information protection in the case of an incident.				
1.17	**Monitoring Service Provider Compliance with Information Protection requirements** The Ministry has a process to monitor service provider compliance for information protection requirements.	Do you manage service providers/contractors? If so, is there a documented process to monitor and track their compliance to information protection requirements? (M)			

Practice Review Program

Interview Questions for Records Management

Introduction and Purpose

Introduce Auditors conducting interview

We are from the Privacy, Compliance and Training Branch in the Ministry of Finance's Corporate Information and Records Management Office. We are here to meet with you today to gather information in relation to an **audit** that we are conducting.

We are conducting a **baseline audit** of your ministry's information management practices.

The purpose of a baseline audit is to assess the maturity of your ministry's information management practices against a number of evaluation criteria that cover privacy, records management, FOI/information access, and the protection of information.

Process

In terms of process, we will be asking you questions and taking notes and may ask you clarifying questions. If at any point you wish to take a break please let us know.

We are meeting with a number of individuals from your ministry in order to gather a fulsome understanding of your ministry's information management practices. As part of this we may ask you to send emails or other documents following this meeting, and may need to meet with you again if we find that we have any additional questions.

At the conclusion of this process we will be preparing a final report which will be submitted to your deputy minister along with other executives from your ministry as directed by your deputy. Our report will document our overall assessment and scoring of maturity at the ministry level. Our report will not name or identify the ministry staff who were involved in this process, and will not be making any assessments of individual level practices.

However, before the report is finalized, it will be shared with designated ministry representatives to ensure the ministry has an opportunity for review and to let us know if we missed anything or were incorrect in any way. If we are unclear on something or want to be sure, we may also ask you to review and confirm information or a conclusion we may arrive at.

Finally, any information you provide today will be maintained in confidence and will be used only for the purposes of this audit/assessment, or as may be required by law or government policy (e.g. FOI request, subject to redactions).

Do you have any questions before we begin?

PRACTICE REVIEW PROGRAM – RECORDS QUESTIONS

Interviewee Name:	**Jackie Henry, Brittany Hawkins**
Interviewer Name	**Trevor Youdale, Bev Qualizza**
Date:	**April 23, 2021**

Records Management				**Score**	
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.	Do you know if there is a dedicated RM person in your ministry? How are RM responsibilities communicated to staff? Have you seen any written procedures or guidance on your own responsibilities for records management? (S) Copies pls	s.13		
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.	Do you have any ***Ministry-specific*** policies or procedures related to records management? (other than Core Policies) If so, how are these RM policies/procedures communicated to staff? Copies pls (M)			

2.1	**Mandatory Employee Training** Employees have completed mandatory training related to records management (IM117).	- Other than IM117, have you or any of your staff taken any records management training? If so, what training? - How is completion of staff training monitored? If there are any gaps how is it addressed? - How do you confirm that staff understands their RM responsibilities?
2.2	**Role Specific Training** Individuals have received additional, role-specific records management training where appropriate.	Some roles require specialized training in Records Management. If your role has this requirement, have your received the appropriate training? (S)

s.13

s.13

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.	Does your area use EDRMS to organize its records? If not, how are your records organized so that they are managed according to their function and to approved retention requirements? Do you have any documented procedures about records classification, and if so, how are these communicated to staff? (M) Copies pls [email?]
3.2	**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.	

s.13

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.	
4.2	**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.	

s.13

5.1	**Records Retention Holds and Disposition** The ministry has procedures to retain, dispose of, transfer, or archive government information based on official policies, specifications, schedules, guidelines, and procedures published by GRS. In the case of a legal hold or FOI request, the ministry has processes in place to ensure that such records are not destroyed.	How do you ensure that records are retained according to the appropriate schedules? In the case of a legal hold or FOI request, do you have a documented process to ensure that those records are not destroyed? Copies pls (M)
5.2	**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	Does your ministry have documented procedures for the transfer of records to bodies covered by the IMA? If so, do those procedures include guidance to maintain the chain of custody and continuity of control for records during

	Act. This includes procedures to monitor such transfers.	transfer? Copies pls (M)
5.4	**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.	Do you have documented procedures for the management and storage of physical records, both on and offsite? Copies pls (M)
6.1	**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.	How do you ensure that all government records held in your ministry are kept in approved record keeping systems? Do you have a process in place to remind staff that non-transitory government information held in Outlook (e.g.) is to be transferred for retention in a secure approved recordkeeping system? Copies pls (M)

s.13

s.13

6.1	**Inventory of Ministry Systems and Repositories** The ministry maintains an inventory of ministry systems and repositories that manage and/or store government information	Do you maintain an up-to-date inventory of the information systems and repositories in use in your ministry? Copy pls (M)

Practice Review Program

Interview Questions for Records Management

Introduction and Purpose

Introduce Auditors conducting interview

We are from the Privacy, Compliance and Training Branch in the Ministry of Finance's Corporate Information and Records Management Office. We are here to meet with you today to gather information in relation to an **audit** that we are conducting.

We are conducting a **baseline audit** of your ministry's information management practices.

The purpose of a baseline audit is to assess the maturity of your ministry's information management practices against a number of evaluation criteria that cover privacy, records management, FOI/information access, and the protection of information.

Process

In terms of process, we will be asking you questions and taking notes and may ask you clarifying questions. If at any point you wish to take a break please let us know.

We are meeting with a number of individuals from your ministry in order to gather a fulsome understanding of your ministry's information management practices. As part of this we may ask you to send emails or other documents following this meeting, and may need to meet with you again if we find that we have any additional questions.

At the conclusion of this process we will be preparing a final report which will be submitted to your deputy minister along with other executives from your ministry as directed by your deputy. Our report will document our overall assessment and scoring of maturity at the ministry level. Our report will not name or identify the ministry staff who were involved in this process, and will not be making any assessments of individual level practices.

However, before the report is finalized, it will be shared with designated ministry representatives to ensure the ministry has an opportunity for review and to let us know if we missed anything or were incorrect in any way. If we are unclear on something or want to be sure, we may also ask you to review and confirm information or a conclusion we may arrive at.

Finally, any information you provide today will be maintained in confidence and will be used only for the purposes of this audit/assessment, or as may be required by law or government policy (e.g. FOI request, subject to redactions).

Do you have any questions before we begin?

PRACTICE REVIEW PROGRAM – RECORDS QUESTIONS

Interviewee Name:	**Jackie Allen, Brittany Hawkins**
Interviewer Name	**Trevor Youdale, Bev Qualizza**
Date:	**April 23, 2021**

Records Management				**Score**	
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.	Do you know if there is a dedicated RM person in your ministry? How are RM responsibilities communicated to staff? Have you seen any written procedures or guidance on your own responsibilities for records management? (S) Copies pls	s.13		
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.	Do you have any ***Ministry-specific*** policies or procedures related to records management? (other than Core Policies) If so, how are these RM policies/procedures communicated to staff? Copies pls (M)			

2.1	**Mandatory Employee Training** Employees have completed mandatory training related to records management (IM117).	- Other than IM117, have you or any of your staff taken any records management training? If so, what training? - How is completion of staff training monitored? If there are any gaps how is it addressed? - How do you confirm that staff understands their RM responsibilities?
2.2	**Role Specific Training** Individuals have received additional, role-specific records management training where appropriate.	Some roles require specialized training in Records Management. If your role has this requirement, have your received the appropriate training? (S)

s.13

s.13

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.	Does your area use EDRMS to organize its records? If not, how are your records organized so that they are managed according to their function and to approved retention requirements? Do you have any documented procedures about records classification, and if so, how are these communicated to staff? (M) Copies pls [email?]
3.2	**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.	

s.13

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.	
4.2	**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.	

s.13

5.1	**Records Retention Holds and Disposition** The ministry has procedures to retain, dispose of, transfer, or archive government information based on official policies, specifications, schedules, guidelines, and procedures published by GRS. In the case of a legal hold or FOI request, the ministry has processes in place to ensure that such records are not destroyed.	How do you ensure that records are retained according to the appropriate schedules? In the case of a legal hold or FOI request, do you have a documented process to ensure that those records are not destroyed? Copies pls (M)
5.2	**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	Does your ministry have documented procedures for the transfer of records to bodies covered by the IMA? If so, do those procedures include guidance to maintain the chain of custody and continuity of control for records during

	Act. This includes procedures to monitor such transfers.	transfer? Copies pls (M)	s.13
5.4	**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.	Do you have documented procedures for the management and storage of physical records, both on and offsite? Copies pls (M)	
6.1	**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.	How do you ensure that all government records held in your ministry are kept in approved record keeping systems? Do you have a process in place to remind staff that non-transitory government information held in Outlook (e.g.) is to be transferred for retention in a secure approved recordkeeping system? Copies pls (M)	

6.2	**Inventory of Ministry Systems and Repositories** The ministry maintains an inventory of ministry systems and repositories that manage and/or store government information	Do you maintain an up-to-date inventory of the information systems and repositories in use in your ministry? Copy pls (M)

s.13

9:30am	**Introduction and Territorial Acknowledgements (5 mins)** **Trevor Youdale**
9:35am	Icebreaker/Poll (5 mins) Kirby Constable
9:40am	Emilie Message/Remarks (5 mins) Emilie Hillier
9:45am	ARI ISTS Project Update (15 mins) Elizabeth Vander Beesen
10:00am	IM Assessment Framework – PREM Lessons Learned (10 mins) Trevor Youdale, Brittany Jackson, and Bev Qualizza
10:10am	BREAK (5 mins)
10:15am	FOI Perspectives on RM (10-15 mins) Cindy Kukucska (IAO) and Kris Ghag (IAO)
10:30am	*BREAK OUT GROUP* Improving Ministry RM practices through FOI (20 mins)
10:45am	IST Onboarding Project Update(10 mins) Brittany Jackson, Danielle Appleby
10:55am	Final remarks, Q&A (5 mins)

Acknowledgement

We acknowledge and respect the Coast Salish Lekwungen speaking Peoples on whose traditional territories the office stands and the Songhees, Esquimalt and WASNC peoples whose historical relationships with the land continue to this day.

PREM IM Assessment

IST All Staff
October 20, 2021

BRITISH COLUMBIA

Ministry of Citizens' Services

Goals for today's presentation

To provide:

- An overview of the IM Assessment Project in the Office of the DM to the Premier
- Information on the IM Assessment Framework
- Updates and lessons learned

OCIO

OCIO CIRMO

OCIO CONN

OCIO DPD

OCIO ES

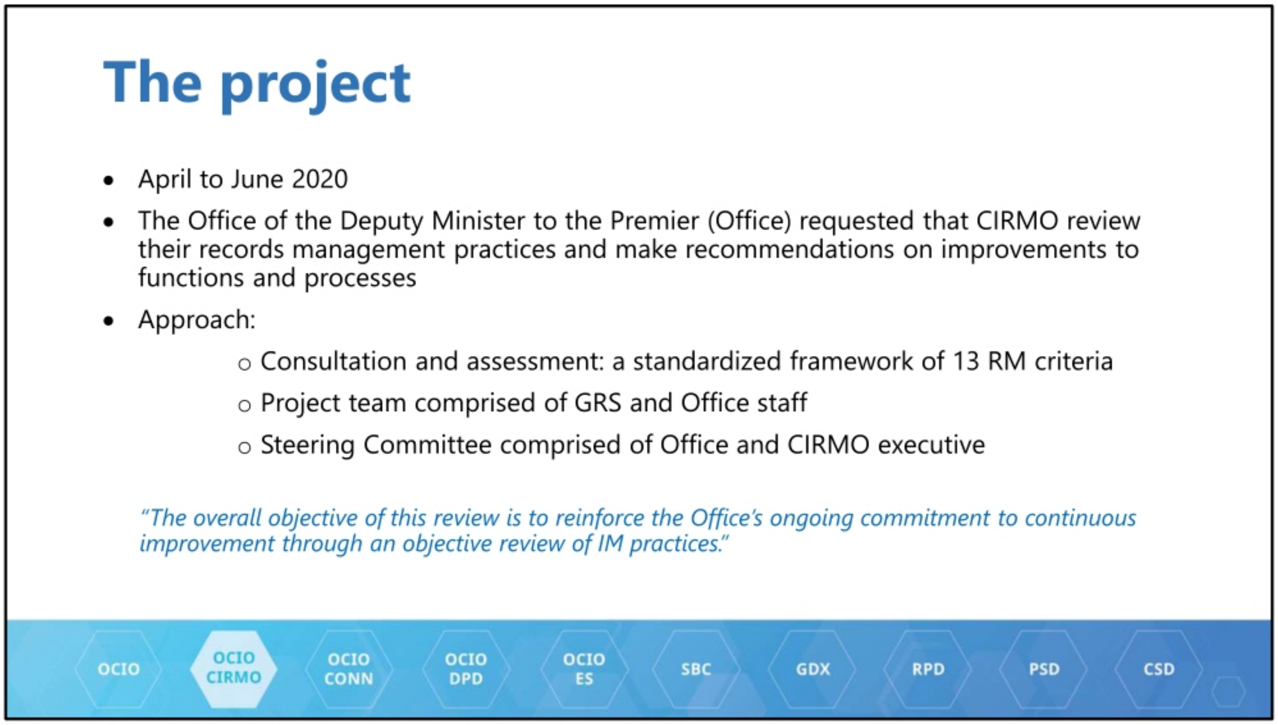
SBC

GDX

RPD

PSD

CSD

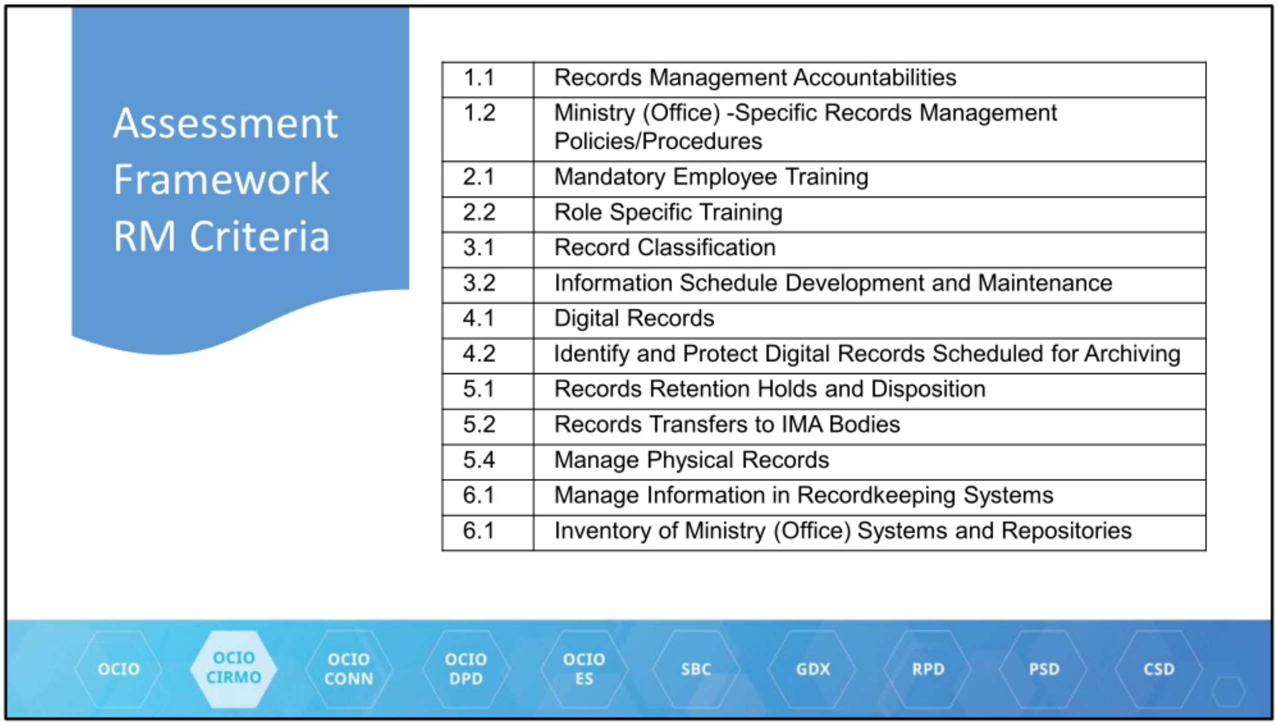


The project

- April to June 2020
- The Office of the Deputy Minister to the Premier (Office) requested that CIRMO review their records management practices and make recommendations on improvements to functions and processes
- Approach:
  - Consultation and assessment: a standardized framework of 13 RM criteria
  - Project team comprised of GRS and Office staff
  - Steering Committee comprised of Office and CIRMO executive

"The overall objective of this review is to reinforce the Office's ongoing commitment to continuous improvement through an objective review of IM practices."

Practice Review Framework (2019) – developed by CIRMO (PCT)60 criteria based on legislation and policy requirements for access, privacy, records management, and protection. RM = 13 of 14 criteria (14th was irrelevant to office regarding transfer of records to non-IMA body)



Assessment Framework RM Criteria

1.1	Records Management Accountabilities
1.2	Ministry (Office) -Specific Records Management Policies/Procedures
2.1	Mandatory Employee Training
2.2	Role Specific Training
3.1	Record Classification
3.2	Information Schedule Development and Maintenance
4.1	Digital Records
4.2	Identify and Protect Digital Records Scheduled for Archiving
5.1	Records Retention Holds and Disposition
5.2	Records Transfers to IMA Bodies
5.4	Manage Physical Records
6.1	Manage Information in Recordkeeping Systems
6.1	Inventory of Ministry (Office) Systems and Repositories

Practice Review Framework (2019) – developed by CIRMO (PCT)60 criteria based on legislation and policy requirements for access, privacy, records management, and protection. RM = 13 of 14 criteria (14th was irrelevant to office regarding transfer of records to non-IMA body)

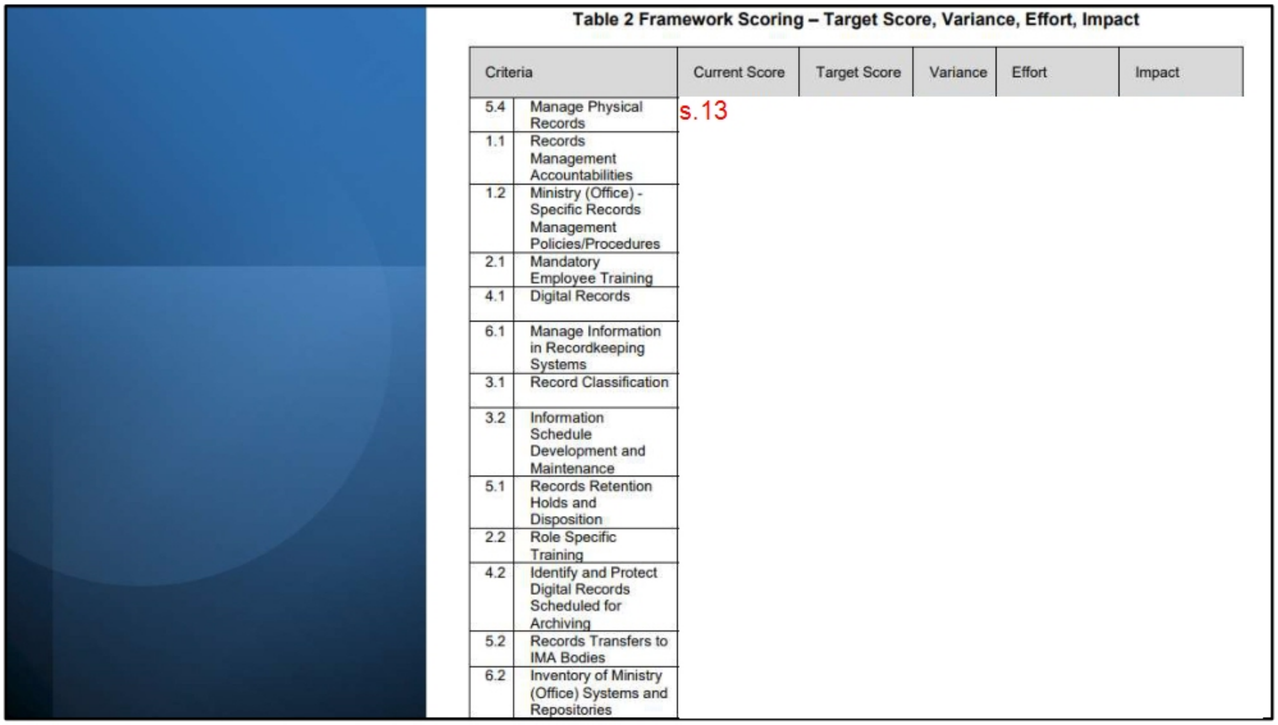
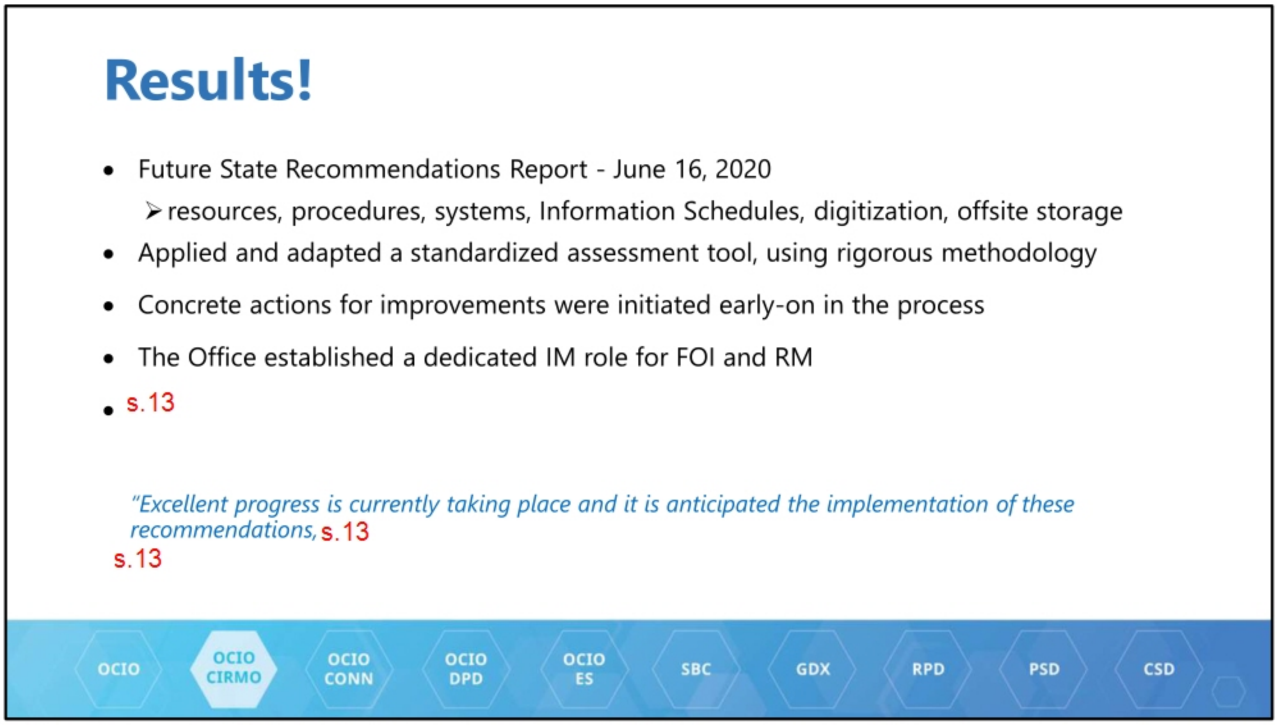


Table 2 Framework Scoring – Target Score, Variance, Effort, Impact

Criteria		Current Score	Target Score	Variance	Effort	Impact
5.4	Manage Physical Records	s.13				
1.1	Records Management Accountabilities					
1.2	Ministry (Office) - Specific Records Management Policies/Procedures					
2.1	Mandatory Employee Training					
4.1	Digital Records					
6.1	Manage Information in Recordkeeping Systems					
3.1	Record Classification					
3.2	Information Schedule Development and Maintenance					
5.1	Records Retention Holds and Disposition					
2.2	Role Specific Training					
4.2	Identify and Protect Digital Records Scheduled for Archiving					
5.2	Records Transfers to IMA Bodies					
6.2	Inventory of Ministry (Office) Systems and Repositories					

Practice Review Framework (2019) – developed by CIRMO (PCT)60 criteria based on legislation and policy requirements for access, privacy, records management, and protection. RM = 13 of 14 criteria (14th was irrelevant to office regarding transfer of records to non-IMA body)



Results!

- Future State Recommendations Report - June 16, 2020
  - ➢ resources, procedures, systems, Information Schedules, digitization, offsite storage
- Applied and adapted a standardized assessment tool, using rigorous methodology
- Concrete actions for improvements were initiated early-on in the process
- The Office established a dedicated IM role for FOI and RM
- s.13

"Excellent progress is currently taking place and it is anticipated the implementation of these recommendations, s.13

s.13

OCIO
OCIO CIRMO
OCIO CONN
OCIO DPD
OCIO ES
SBC
GDX
RPD
PSD
CSD

Actions underway – s.13

s.13

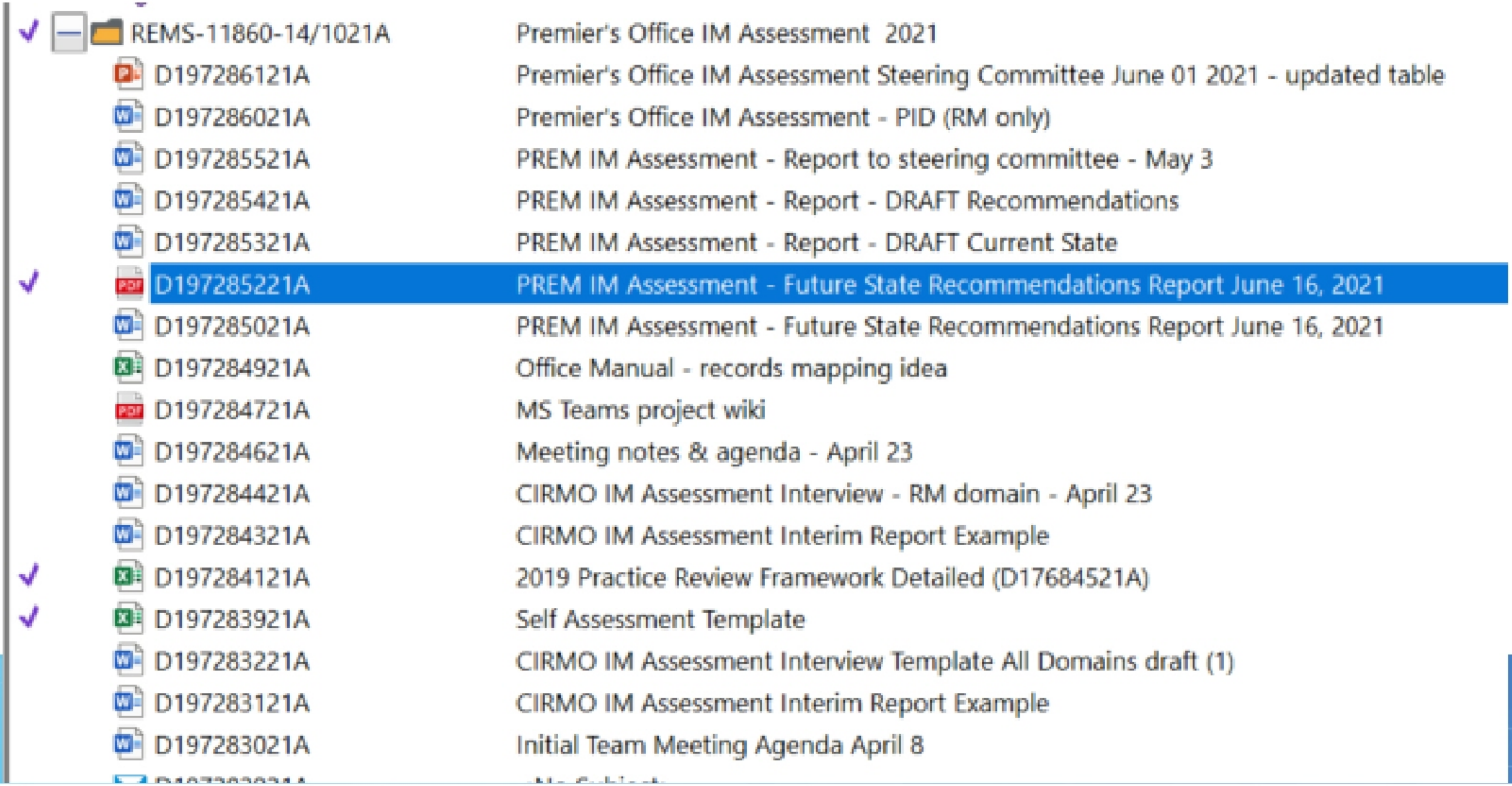
Results – report recommendations

s.13

Through consultation with the Office, to address identified gaps and support the Office

in progressing toward a high maturity level, this report makes s.13 recommendations:

More information



✓	REMS-11860-14/1021A	Premier's Office IM Assessment 2021
	D197286121A	Premier's Office IM Assessment Steering Committee June 01 2021 - updated table
	D197286021A	Premier's Office IM Assessment - PID (RM only)
	D197285521A	PREM IM Assessment - Report to steering committee - May 3
	D197285421A	PREM IM Assessment - Report - DRAFT Recommendations
	D197285321A	PREM IM Assessment - Report - DRAFT Current State
✓	D197285221A	PREM IM Assessment - Future State Recommendations Report June 16, 2021
	D197285021A	PREM IM Assessment - Future State Recommendations Report June 16, 2021
	D197284921A	Office Manual - records mapping idea
	D197284721A	MS Teams project wiki
	D197284621A	Meeting notes & agenda - April 23
	D197284421A	CIRMO IM Assessment Interview - RM domain - April 23
	D197284321A	CIRMO IM Assessment Interim Report Example
✓	D197284121A	2019 Practice Review Framework Detailed (D17684521A)
✓	D197283921A	Self Assessment Template
	D197283221A	CIRMO IM Assessment Interview Template All Domains draft (1)
	D197283121A	CIRMO IM Assessment Interim Report Example
	D197283021A	Initial Team Meeting Agenda April 8

Update on recent activities and observations on impact of the project

OCIO | OCIO CIRMO | OCIO CONN | OCIO DPD | OCIO ES | SBC | GDX | RPD | PSD | CSD

Page 226 of 444 to/à Page 240 of 444

Withheld pursuant to/removed as

s.13

Premier's Office

Information Management Assessment

Steering Committee Meeting

May 3, 2021

BRITISH COLUMBIA

Ministry of Citizens' Services

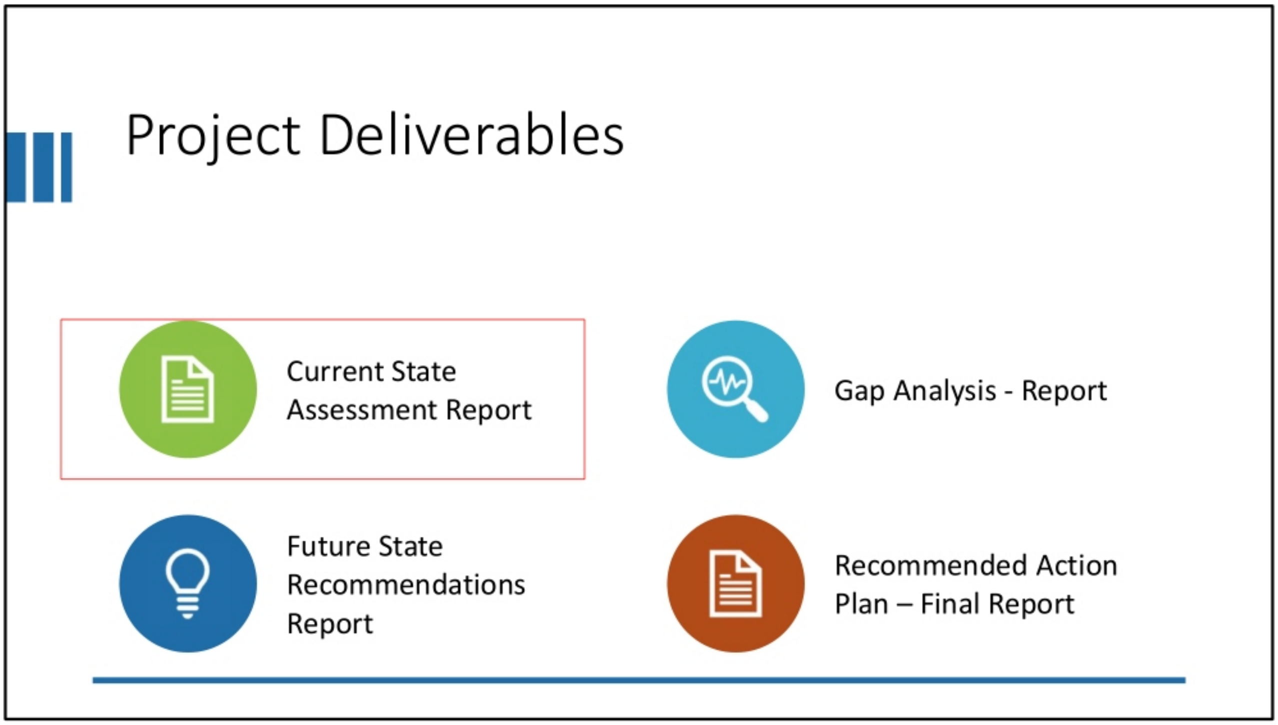
Welcome

AGENDA

Working Group Report Out to Steering Committee

Discussion

Next Steps



Project Deliverables

- Current State Assessment Report
- Gap Analysis - Report
- Future State Recommendations Report
- Recommended Action Plan – Final Report

Series of 4 reports that build upon themselves

CRITERIA

- Working group members include Premier's office staff and have reviewed the report
-
- 14 RM Criteria for assessment within 6 Topical Areas

Topical Areas for Review

- RM Governance
- Education and Awareness
- Information Schedules
- Digital Records
- Records Retention
- Record Keeping Systems

Rating System

RATING SYSTEM	
Level 1	Initial
Level 2	Repeatable
Level 3	Defined
Level 4	Managed
Level 5	Optimized

s.13

Criterion for Review

1.1	**Records Management Accountabilities**
1.2	Ministry-Specific Records Management Policies/Procedures
2.1	Mandatory Employee Training
2.2	Role Specific Training
3.1	Record Classification
3.2	Information Schedule Development and Maintenance
4.1	Digital Records
4.2	Identify and Protect Digital Records Scheduled for Archiving
5.1	Records Retention Holds and Disposition
5.2	Records Transfers to IMA Bodies
5.4	Manage Physical Records
6.1	Manage Information in Recordkeeping Systems
6.1	Inventory of Ministry Systems and Repositories

Initial Ratings

Records Management Criteria		Score
1.1	Records Management Accountabilities	s.13
1.2	Ministry-Specific Records Management Policies/Procedures	
2.1	Mandatory Employee Training	
2.2	Role Specific Training	
3.1	Record Classification	
3.2	Information Schedule Development and Maintenance	
4.1	Digital Records	
4.2	Identify and Protect Digital Records Scheduled for Archiving	
5.1	Records Retention Holds and Disposition	
5.2	Records Transfers to IMA Bodies	
5.4	Manage Physical Records	
6.1	Manage Information in Recordkeeping Systems	
6.1	Inventory of Ministry Systems and Repositories	

Noteworthy Practices

s.13

s.13

Further Discussion

Next Steps

May 14. 2021 Final Current State Assessment and Gap Analysis Report

May 18, 2021 Steering Committee Meeting

May 31, 2021 Initial Report Future State Recommendations Report

Timeline Overview

- April 16, 2021 Project Kick-off Meeting/Consultation Begins
- May 3, 2021 Initial Current State Assessment Report May 4, 2021
- May 4, 2021 Steering Committee Meetings bi-weekly
- May 17, 2021 Final Current State Report and Gap Analysis Report
- May 31, 2021 Initial Report Future State Recommendations Report
- June 1-3, 2021 Steering Committee Feedback on Future State Recommendations
- June 14, 2021 Recommended Action Plan Report

Premier's Office

Information Management Assessment

Steering Committee Meeting

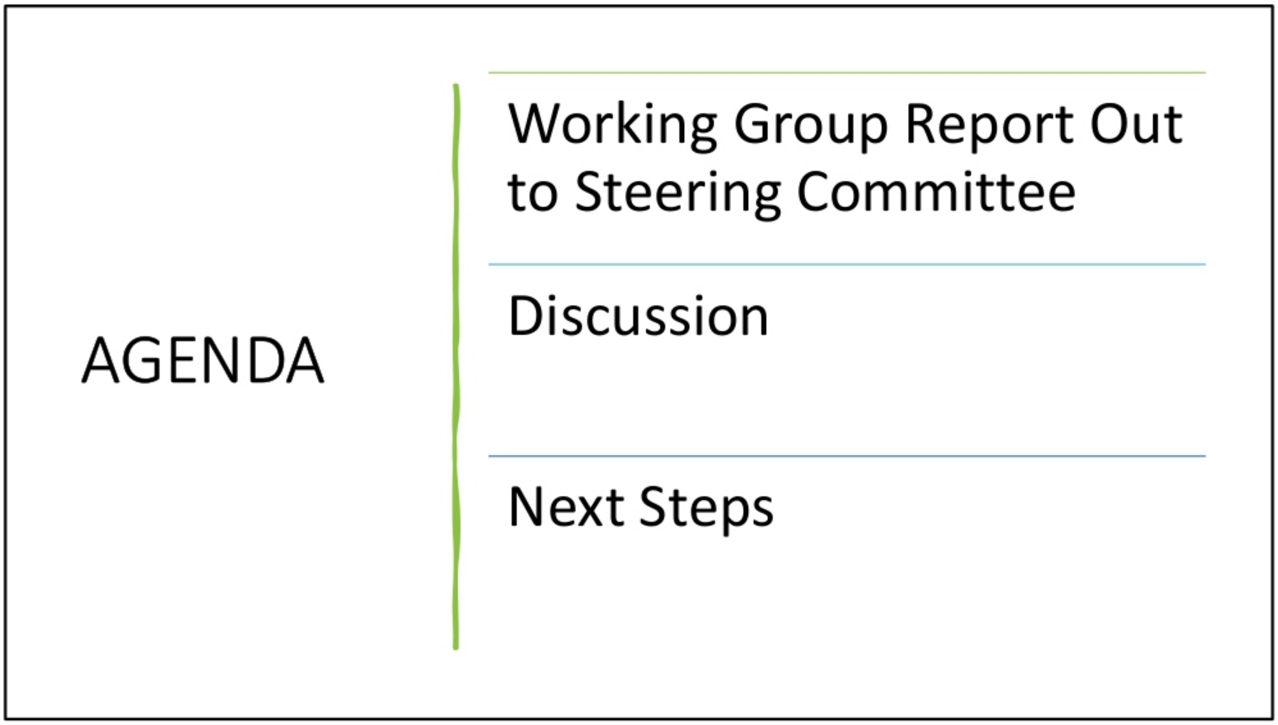
June 1, 2021

BRITISH COLUMBIA

Ministry of Citizens' Services

Welcome

Introduce Trevor as SME for the project



AGENDA

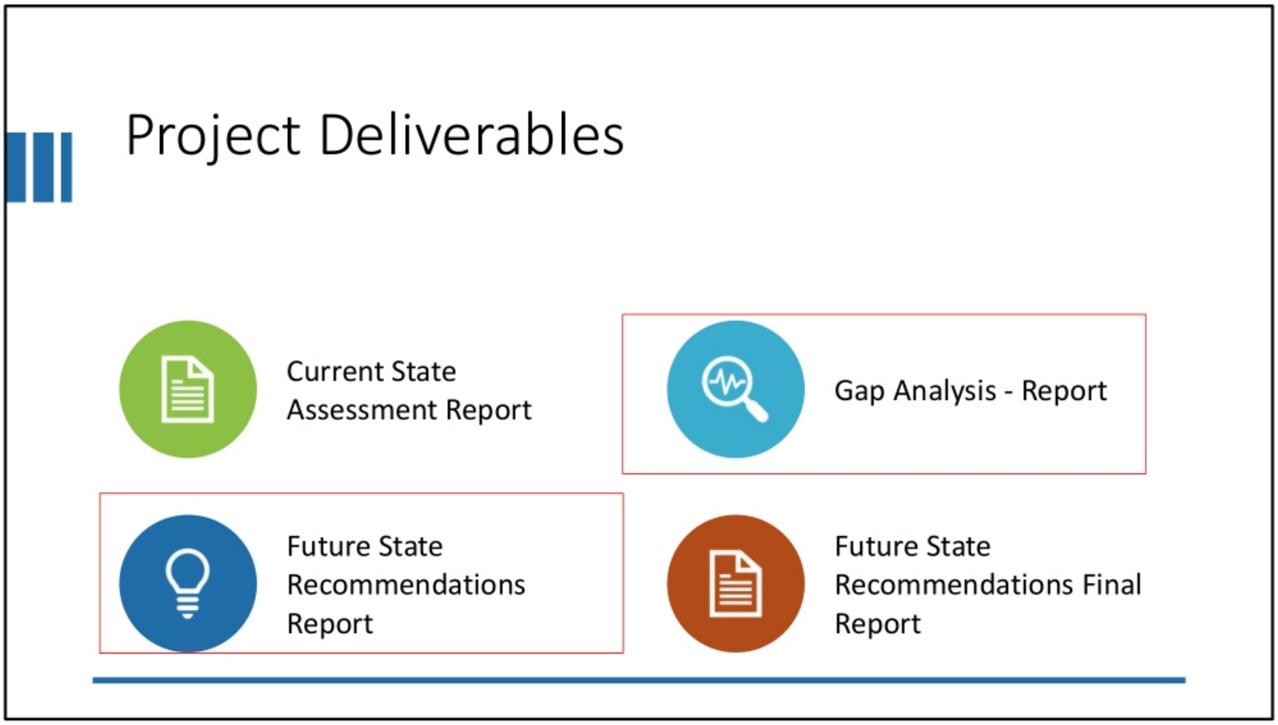
Working Group Report Out to Steering Committee

Discussion

Next Steps

We found as part of the assessment process it naturally leads to conversations of what recommendations for improvement should be and so we have accelerated the timelines of the project.

For our report out today we have the GAP analysis as well as future state recommendations. At the end of the agenda we would propose to provide some additional time for you to provide any additional feedback you may wish to be reflected in our report prior to the wrap up of the assessment process.

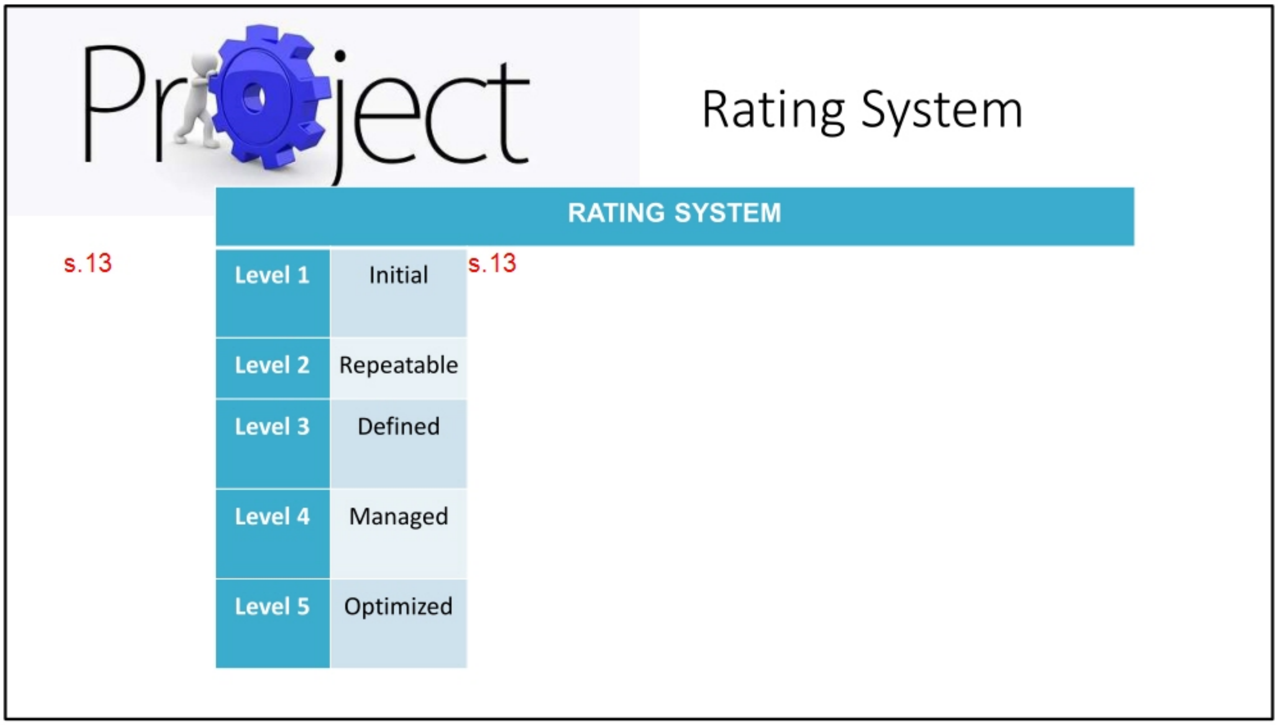


Project Deliverables

- Current State Assessment Report
- Gap Analysis - Report
- Future State Recommendations Report
- Future State Recommendations Final Report

Series of 4 reports that build upon themselves

We’ve combined the Gap Analysis report and the Future State Recommendations Report



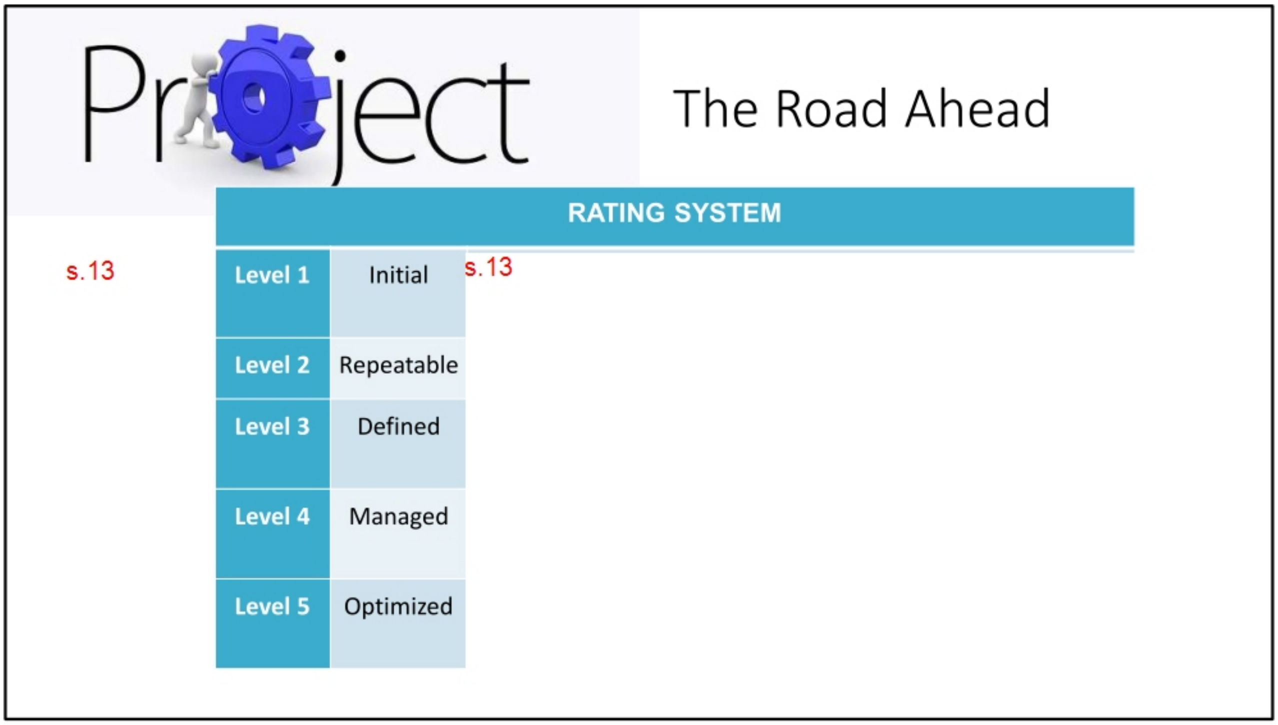
Rating System

s.13

RATING SYSTEM		
Level 1	Initial	s.13
Level 2	Repeatable	
Level 3	Defined	
Level 4	Managed	
Level 5	Optimized	

Review: s.13

s.13



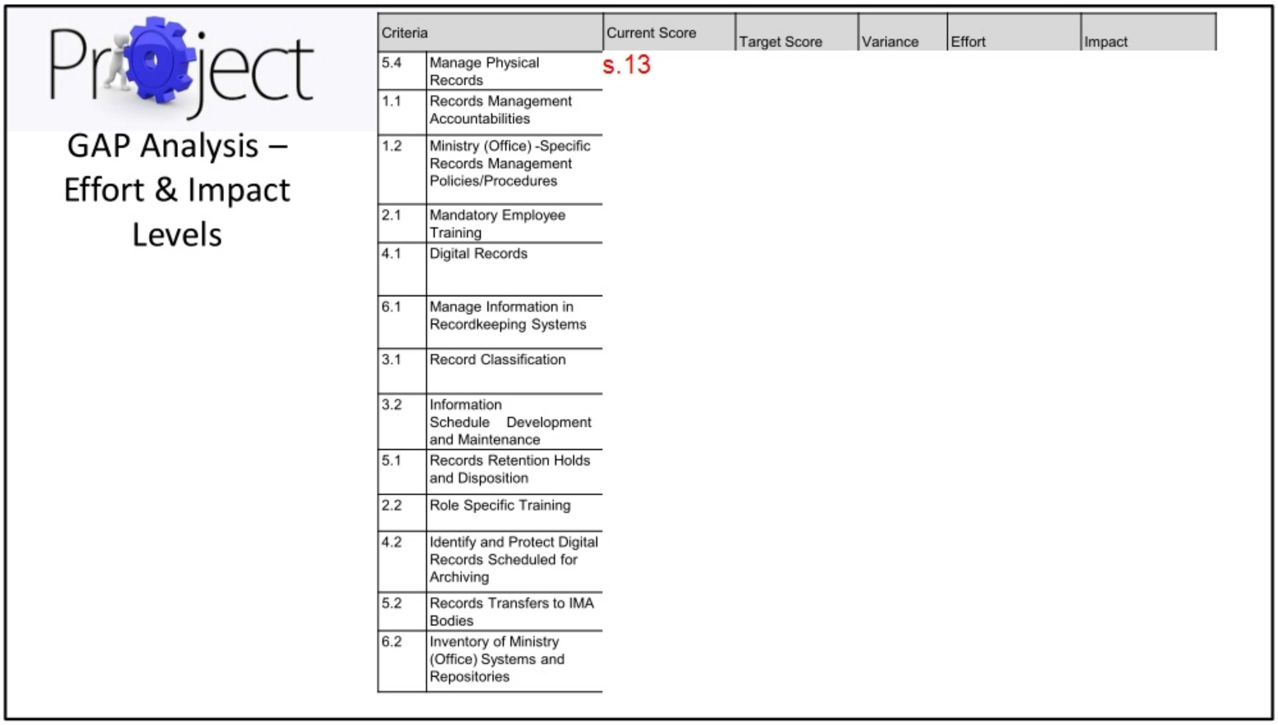
Project

The Road Ahead

s.13

RATING SYSTEM		
Level 1	Initial	s.13
Level 2	Repeatable	
Level 3	Defined	
Level 4	Managed	
Level 5	Optimized	

s.13



GAP Analysis – Effort & Impact Levels

Criteria		Current Score	Target Score	Variance	Effort	Impact
5.4	Manage Physical Records	s.13				
1.1	Records Management Accountabilities					
1.2	Ministry (Office) -Specific Records Management Policies/Procedures					
2.1	Mandatory Employee Training					
4.1	Digital Records					
6.1	Manage Information in Recordkeeping Systems					
3.1	Record Classification					
3.2	Information Schedule Development and Maintenance					
5.1	Records Retention Holds and Disposition					
2.2	Role Specific Training					
4.2	Identify and Protect Digital Records Scheduled for Archiving					
5.2	Records Transfers to IMA Bodies					
6.2	Inventory of Ministry (Office) Systems and Repositories					

The criteria which were evaluated are listed on this chart.

s.13

We have s.13 recommendations on ideas to improve your records management program with an emphasis on actions and next steps. I will turn the conversation over to Trevor Youdale to walk us through the recommendations.

Recommendation s.13

s.13

Report expresses s.13 recommendations for records management improvement

s.13

Recommendation s.13

s.13

Topical Areas:

s.13

Recommendation s.13

s.13

Considerations:

s.13

Recommendation s.13

s.13

Considerations:

s.13

Recommendation s.13

s.13

Considerations:

s.13

Recommendation s.13

s.13

Considerations:

s.13

Recommendation

s.13

s.13

Considerations:

s.13

Recommendation

s.13

s.13

Considerations:

s.13

Recommendation s.13

s.13

Considerations:

s.13

Next Steps

June 1 – 7 Steering Committee Feedback Opportunity – Current Report

June 14, **2021 Future State** Recommendations Final Report

June 29, **2021** Final Project Steering Committee (as needed)

Premier's Office

Information Management Assessment

Corporate Records and Information Management Office (CIRMO)

April 2021

BRITISH COLUMBIA

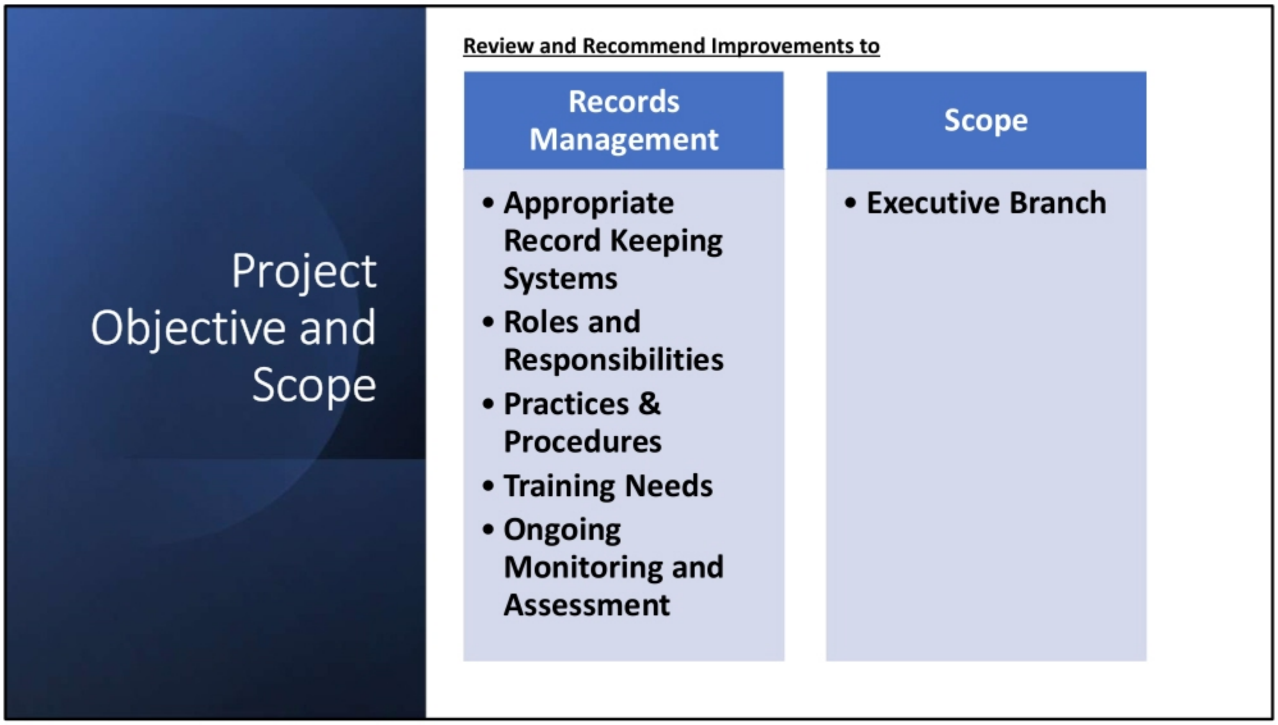
Ministry of Citizens' Services

Introductions

AGENDA

- Introductions
- Sponsor Message
- Project Objective and Scope
- Project Structure
- Project Approach
- Project Deliverables
- Project Timelines
- Next Steps
- Discussion

Sponsor’s Kick-off Message



Project Objective and Scope

Review and Recommend Improvements to

Records Management

- **Appropriate Record Keeping Systems**
- **Roles and Responsibilities**
- **Practices & Procedures**
- **Training Needs**
- **Ongoing Monitoring and Assessment**

Scope

- **Executive Branch**

Out of Scope: IGRS and Cabinet Operations
Assessment of Privacy and Security Practices
Implementation of the Recommendations

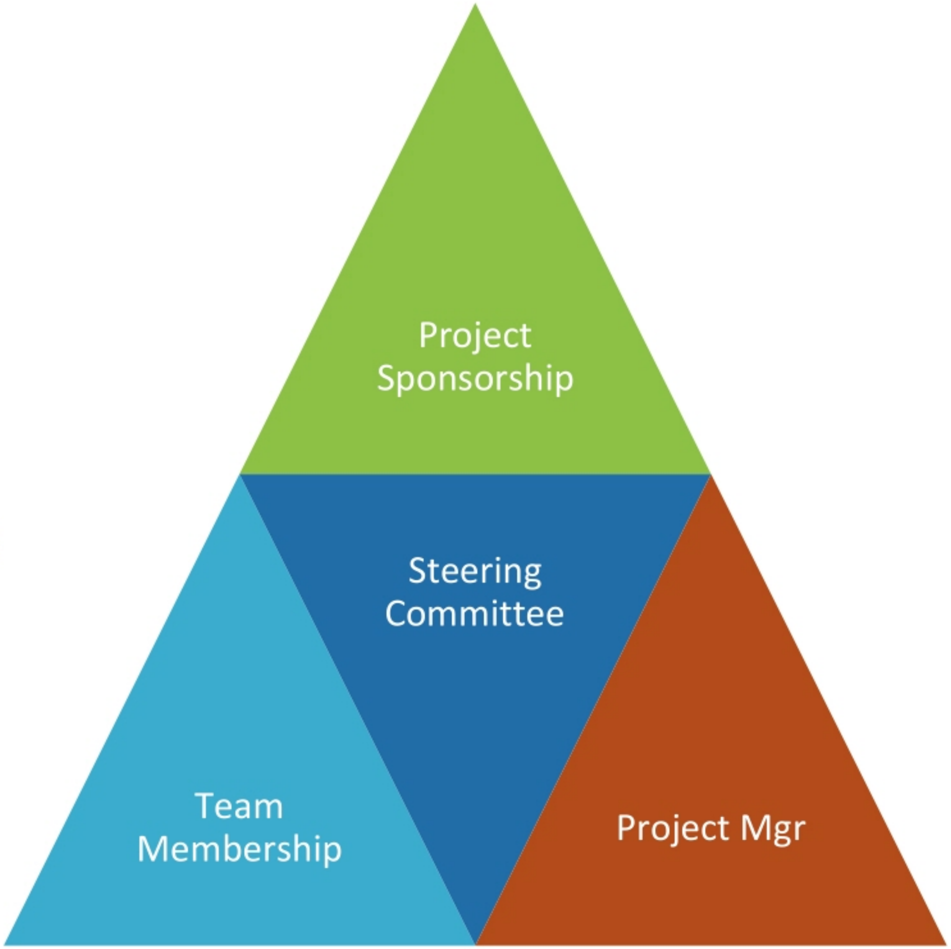
Project Structure

Project Sponsorship
Premier's Office

Christina Zacharuk

Team Membership
Premier's Office - CIRMO

Jackie Allen
Brittany Hawkins
Trevor Youdale
Bev Qualizza

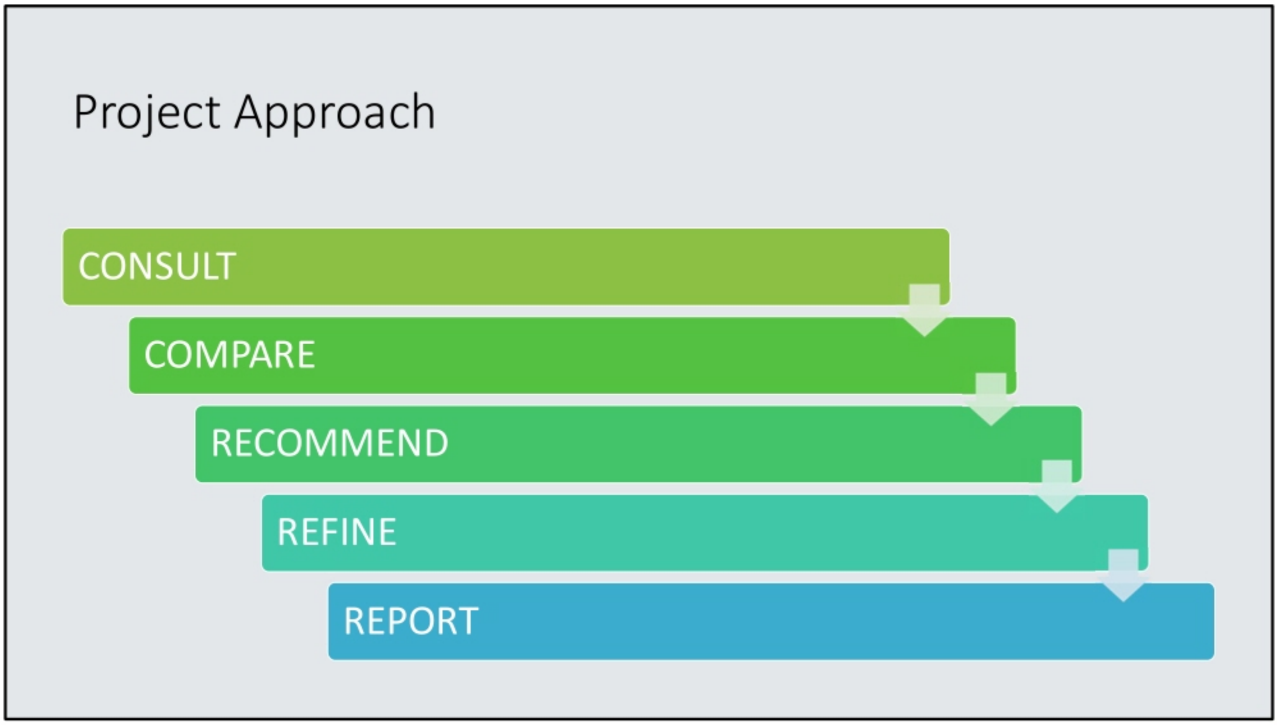


Steering Committee
Premier's Office - CIRMO

Christina Zacharuk
Jill Kot
Jackie Allen
Kerry Pridmore
Susan Laidlaw

Project Manager
CIRMO

Jeff Barber



Project Approach

CONSULT

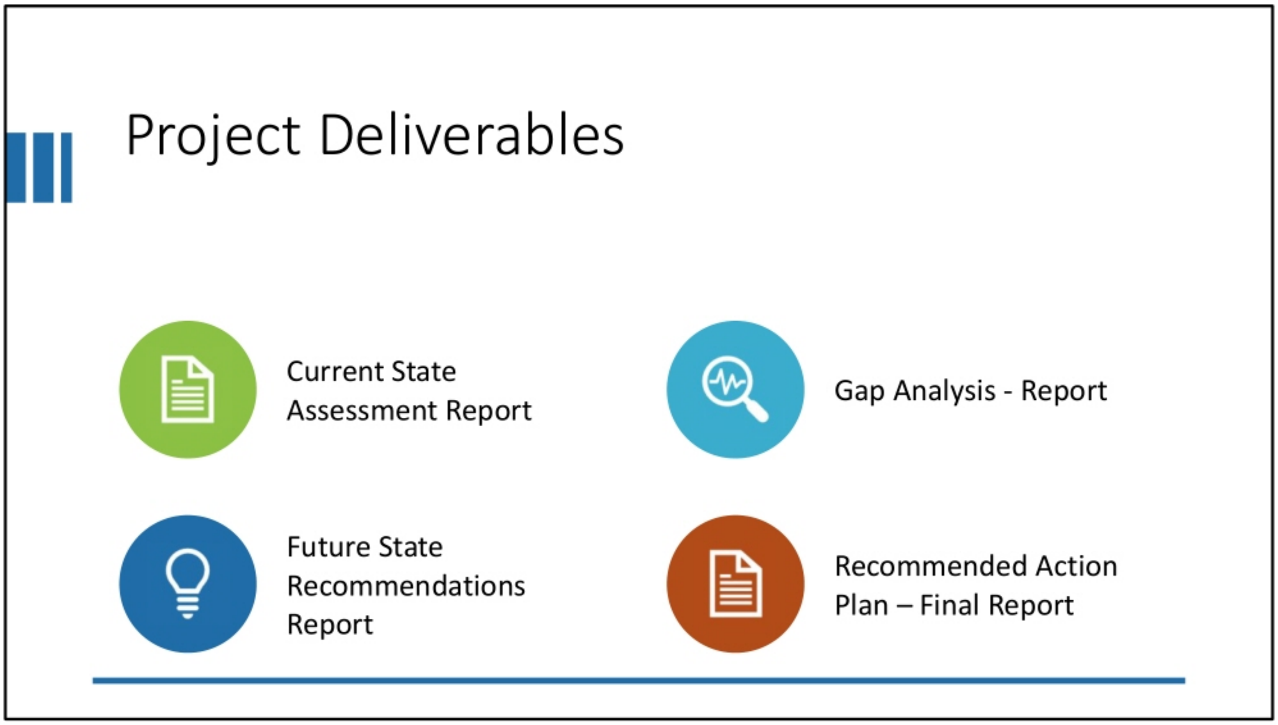
COMPARE

RECOMMEND

REFINE

REPORT

Team Members will consult with the Premier's Office
Compare current practices to recommended practices
Recommend changes to the steering committee
Refine our recommendations as needed
And it will be all done through a series of reports



Project Deliverables

- Current State Assessment Report
- Gap Analysis - Report
- Future State Recommendations Report
- Recommended Action Plan – Final Report

Series of 4 reports that build upon themselves

Timeline Overview

- April 16, 2021 Project Kick-off Meeting/Consultation Begins
- May 3, 2021 Initial Current State Assessment Report May 4, 2021
- May 4, 2021 Steering Committee Meetings bi-weekly
- May 17, 2021 Final Current State Report and Gap Analysis Report
- May 31, 2021 Initial Report Future State Recommendations Report
- June 1-3, 2021 Steering Committee Feedback on Future State Recommendations
- June 14, 2021 Recommended Action Plan Report

Next Steps

April 16, 2021 Project Kick-off Meeting/Consultation Begins

May 3, 2021 Initial Current State Assessment Report

May 4, 2021 Steering Committee Meetings Bi-weekly

Discussion

Premier's Office

Information Management Assessment

Steering Committee Meeting

June 1, 2021

BRITISH COLUMBIA

Ministry of Citizens' Services

Welcome

AGENDA

Working Group Report Out to Steering Committee

Discussion

Next Steps

Project Deliverables

- Current State Assessment Report
- Gap Analysis - Report
- Future State Recommendations Report
- Recommended Action Plan – Final Report

Rating System

s.13

RATING SYSTEM	
Level 1	Initial
Level 2	Repeatable
Level 3	Defined
Level 4	Managed
Level 5	Optimized

s.13

The Road Ahead

s.13

RATING SYSTEM	
Level 1	Initial
Level 2	Repeatable
Level 3	Defined
Level 4	Managed
Level 5	Optimized

s.13

GAP Analysis - Improvement Effort Levels

Records Management Criteria		Current Score	Target Score	Variance	Effort (low, medium, high)
5.4	Manage Physical Records	s.13			
1.1	Records Management Accountabilities				
1.2	Ministry-Specific Records Management Policies/Procedures				
2.1	Mandatory Employee Training				
4.1	Digital Records				
6.1	Manage Information in Recordkeeping Systems				
3.1	Record Classification				
3.2	Information Schedule Development and Maintenance				
5.1	Records Retention Holds and Disposition				
2.2	Role Specific Training				
4.2	Identify and Protect Digital Records Scheduled for Archiving				
5.2	Records Transfers to IMA Bodies				
6.2	Inventory of Ministry Systems and Repositories				

Recommendation

s.13

s.13

s.13

Recommendation s.13

s.13

Recommendation

s.13

s.13

Recommendation

s.13

s.13

Recommendation

s.13

s.13

Recommendation

s.13

s.13

Recommendation s.13

s.13

s.13

Recommendation

s.13

Recommendation

s.13

s.13

Next Steps

June 1 – 7 Steering Committee Feedback Opportunity – Current Report

June 14, **2021** Recommended Action Plan – Final Report

June 29, **2021** Final Project Steering Committee (as needed)

Timeline Overview

April 16, 2021 Project Kick-off Meeting/Consultation Begins

May 3, 2021 Initial Current State Assessment Report May 4, 2021

May 4, 2021 Steering Committee Meetings bi-weekly

May 17, 2021 Final Current State Report and Gap Analysis Report

May 31, 2021 Initial Report Future State Recommendations Report

June 1-3, 2021 Steering Committee Feedback on Future State Recommendations

June 14, 2021 Recommended Action Plan Report

Premier's Office

Information Management Assessment

Steering Committee Meeting

June 1, 2021

BRITISH COLUMBIA

Ministry of Citizens' Services

Welcome

AGENDA

Working Group Report Out to Steering Committee

Discussion

Next Steps

Project Deliverables

- Current State Assessment Report
- Gap Analysis - Report
- Future State Recommendations Report
- Recommended Action Plan – Final Report

Rating System

s.13

RATING SYSTEM	
Level 1	Initial
Level 2	Repeatable
Level 3	Defined
Level 4	Managed
Level 5	Optimized

s.13

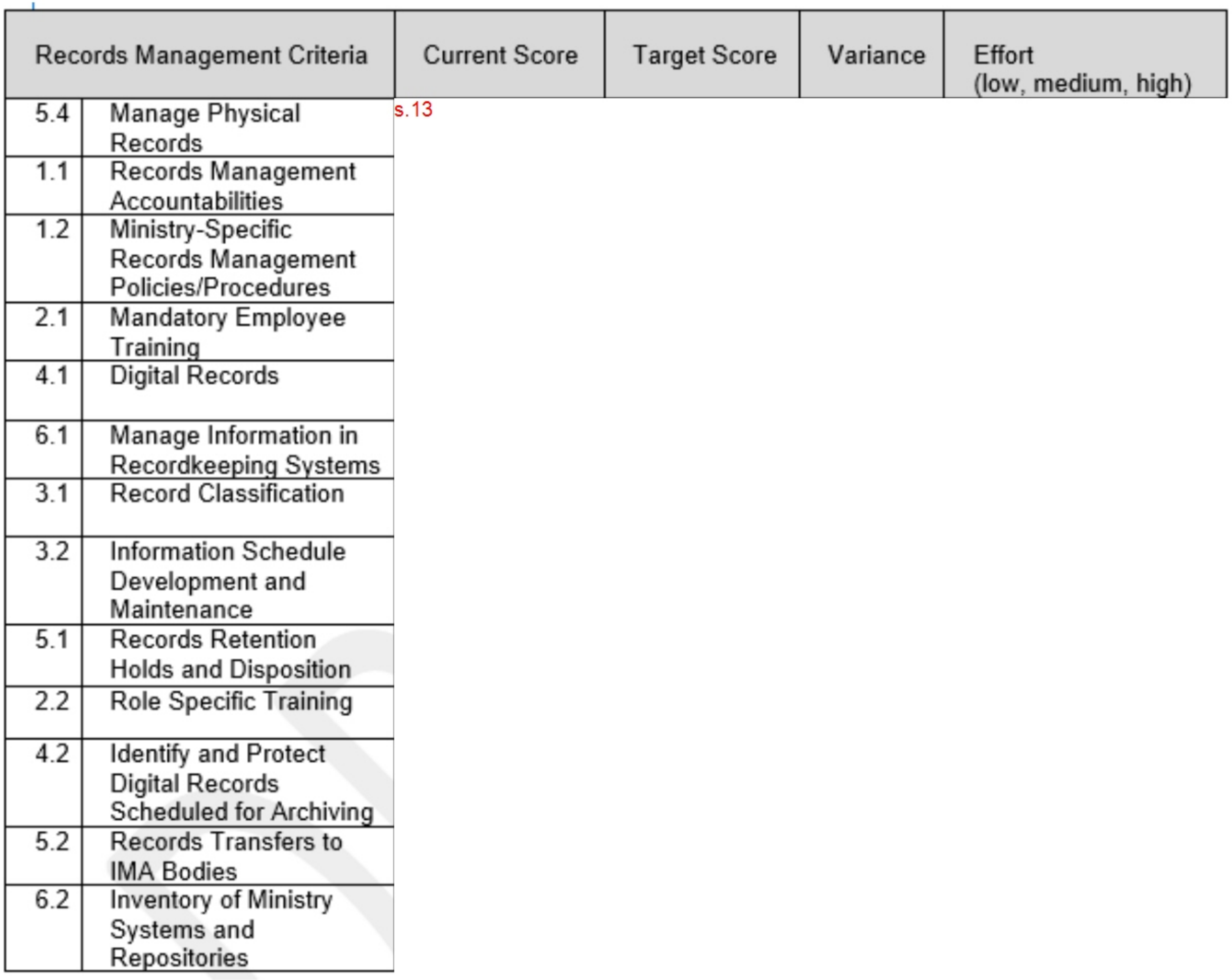
The Road Ahead

s.13

RATING SYSTEM	
Level 1	Initial
Level 2	Repeatable
Level 3	Defined
Level 4	Managed
Level 5	Optimized

s.13

GAP Analysis - Improvement Effort Levels



Records Management Criteria		Current Score	Target Score	Variance	Effort (low, medium, high)
5.4	Manage Physical Records	s.13			
1.1	Records Management Accountabilities				
1.2	Ministry-Specific Records Management Policies/Procedures				
2.1	Mandatory Employee Training				
4.1	Digital Records				
6.1	Manage Information in Recordkeeping Systems				
3.1	Record Classification				
3.2	Information Schedule Development and Maintenance				
5.1	Records Retention Holds and Disposition				
2.2	Role Specific Training				
4.2	Identify and Protect Digital Records Scheduled for Archiving				
5.2	Records Transfers to IMA Bodies				
6.2	Inventory of Ministry Systems and Repositories				

s.13

Recommendation

s.13

s.13

Recommendation s.13

s.13

s.13

Recommendation

s.13

Recommendation

s.13

s.13

Recommendation s.13

s.13

Recommendation

s.13

s.13

Recommendation s.13

s.13

Recommendation

s.13

s.13

Recommendation

s.13

s.13

Next Steps

June 1 – 7 Steering Committee Feedback Opportunity – Current Report

June 14, **2021** Recommended Action Plan – Final Report

June 29, **2021** Final Project Steering Committee (as needed)

Timeline Overview

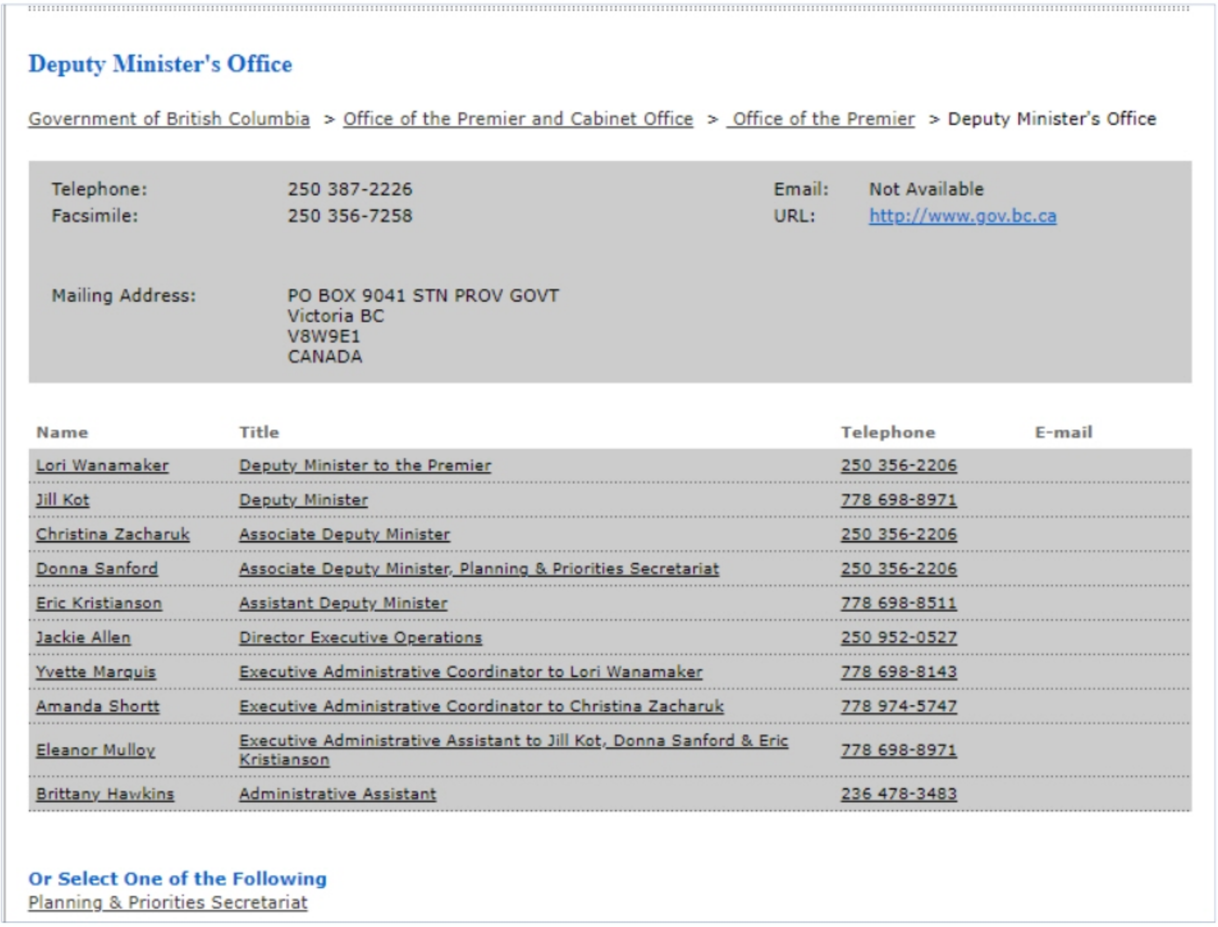
- April 16, 2021 Project Kick-off Meeting/Consultation Begins
- May 3, 2021 Initial Current State Assessment Report May 4, 2021
- May 4, 2021 Steering Committee Meetings bi-weekly
- May 17, 2021 Final Current State Report and Gap Analysis Report
- May 31, 2021 Initial Report Future State Recommendations Report
- June 1-3, 2021 Steering Committee Feedback on Future State Recommendations
- June 14, 2021 Recommended Action Plan Report

Office of Premier - meeting notes from initial conversations with PREM

Two meetings occurred: Monday March 22 & Friday March 26, 2021

Attendees Jackie Allen, Brittany Hawkins, Trevor Youdale

Pre meeting notes by TY about ideas for approach:



Deputy Minister's Office

Government of British Columbia > Office of the Premier and Cabinet Office > Office of the Premier > Deputy Minister's Office

Telephone:	250 387-2226		Email:	Not Available
Facsimile:	250 356-7258		URL:	http://www.gov.bc.ca

Mailing Address:

PO BOX 9041 STN PROV GOVT
Victoria BC
V8W9E1
CANADA

Name	Title	Telephone	E-mail
Lori Wanamaker	Deputy Minister to the Premier	250 356-2206	
Jill Kot	Deputy Minister	778 698-8971	
Christina Zacharuk	Associate Deputy Minister	250 356-2206	
Donna Sanford	Associate Deputy Minister, Planning & Priorities Secretariat	250 356-2206	
Eric Kristianson	Assistant Deputy Minister	778 698-8511	
Jackie Allen	Director Executive Operations	250 952-0527	
Yvette Marquis	Executive Administrative Coordinator to Lori Wanamaker	778 698-8143	
Amanda Shortt	Executive Administrative Coordinator to Christina Zacharuk	778 974-5747	
Eleanor Mulloy	Executive Administrative Assistant to Jill Kot, Donna Sanford & Eric Kristianson	778 698-8971	
Brittany Hawkins	Administrative Assistant	236 478-3483	

Or Select One of the Following
Planning & Priorities Secretariat

- Mapping
- Issues
- Solutions & best practices

1. Main functions and related decisions and records; projects & initiatives

2. Responsibility Centres / OPR for records and documents of decisions

3. Repositories:

- Shared Drives
- Collaboration Tools – SharePoint, MS Teams
- Shared email accounts

Question – roles and responsibilities (mandate letters, strategic plans, business plans)?

Question – prior projects, for example, organizing shared drives?

Question – roles & resp LW, JK, CZ, EK, respective EAC's?

Question – Planning and Priorities Secretariat - what are functions?

RM pain points?

March 22 MS Teams meeting notes:

Jackie described needs/issues:

s.13

s.13

Actions/ideas:

s.13

- Work with EA on file capture process
- Work with exec on retrieval needs – direct or through EA

Additional notes on ideas:

- EVB on ORCS and legacy materials and appraisal
- File formats – list and do they have pst files
- Level of digital only practices

Addition noted on goal ideas:

Short term

- key documents and email are reliable names and captured in a shared drive

s.13

Medium term

s.13

Long term

s.13

March 26 on-site meeting notes:

- JA provided background on recent history for the office
- JA & BH had a copy of the PID
- JA confirmed the Government Directory listing of DMO office staff is accurate
- JA said DMO Planning and Priorities Secretariate (Donna Sanford), Cab Ops and IGRS, is separate and out of scope of this project. i.e. RM project concerns DMO office.
- JA confirmed support relationships between EAC's and exec: Shortt supports Zacharuk; Marquis supports Wannamaker; Mulloy supports Kot & Kristianson)
- EAC's are a critical role in supporting file capture and retrieval
- Jill Kot is managing own records connected with projects under her conduct
- Little to no paper records in their processes
- High interest on BN's and most are for information only (not signed by Lori), except those for IOC appointments.
- s.13
-

s.13

-
-
-
- I said I will connect with them in April (away next week)
- Acknowledged next steps will begin to align with the formal project timelines and activities

Action items

s.13

-
-

Reference info:

CIRMO Project Initiation Document

Project Information

Client	BC Premier's Office
Project Name	Premier's Office Information Management Practice Review
Business Owner	Jackie Allen
Project Sponsor	Jill Kot
Start Date	March 26, 2021

1. Purpose

To review the information management practices currently in place in the Premier's Office, and to make recommendations on improvements to functions and processes.

2. Scope:

In Scope:

- Identification and documentation of the current state of IM within the Premier's Office, including:
    - records management (RM)s.13 roles and responsibilities within the Premier's Office
    - existing RM practices, including electronic and physical filing systems and practices around the retention of documents

  s.13
- Identification of the desired future state, including:
    - RM roles and responsibilities
    - RM practices and procedures

  s.13
    - Appropriate recordkeeping system (e.g. LAN structure, EDRMS Content Manager)
    - Training
    - On-going monitoring and assessment
- Development of recommendations for actions for to reach the desired future state

Out of Scope:

- Assessment of IM practices in other offices
- Assessment of privacy or security practices
- Implementation of recommendations (e.g. filing/records management)

3. Deliverables

a. Current State Assessment
b. Future State Recommendations
c. Gap Analysis
d. Recommended Action Plan

4. Resource Management

Function/Role	Name	% FTE
Project Sponsor	Jill Kot	5%
Project Management	Jeff Barber	10%
Records Subject Matter Experts	Trevor Youdale Bev Qualizza	50%
s.13		
Premier's Office Practice SME	Jackie Allen	25%

5. Key Stakeholders

The following stakeholders' interests must be considered:

Stakeholders	Potential Impact L / M / H	Need to Consult Yes/No	Need to Inform Yes/ No
Deputy to the Premier	s.13		
Other Deputy Ministers' Offices			
Government Chief Information Officer			
Government Chief Records Officer			
s.13			
Government Records Service			

FUNCTION	EXEC DIR	DIR	OTHER RESOURCES	SCOPE OF WORK	SYSTEMS	REQUIREMENTS OF BRANCH	NOTES

CIRMO Project Initiation Document

Project Information

Client	BC Premier's Office
Project Name	Premier's Office Information Management Practice Review
Business Owner	Jackie Allen
Project Sponsor	Jill Kot & Christina Zacharuk
Start Date	March 26, 2021
End Date	June 30, 2021

1. Purpose

To review the information management practices currently in place in the Premier's Office, and to make recommendations on improvements to functions and processes.

2. Scope:

In Scope:

- Identification and documentation of the current state of IM within the Premier's Office, including:
  - records management (RM)s.13 roles and responsibilities within the Premier's Office
  - existing RM practices, including electronic and physical filing systems and practices around the retention of documents

  s.13

- Identification of the desired future state, including:
  - RM roles and responsibilities
  - RM practices and procedures

  s.13
  - Appropriate recordkeeping system (e.g. LAN structure, EDRMS Content Manager)
  - Training
  - On-going monitoring and assessment
- Development of recommendations for actions to reach the desired future state

Out of Scope:

- Assessment of records management practices in other offices (i.e. IGRS, Cabinet Operations or Executive Branch)
- Assessment of privacy or security practices
- Implementation of recommendations (e.g. filing/records management)

3. Deliverables

a. Current State Assessment
b. Future State Recommendations
c. Gap Analysis
d. Recommended Action Plan

4. Resource Management

Function/Role	Name	% FTE	Timeframe
Project Sponsor	Jill Kot & Christina Zacharuk	5%	Apr – Jun 2021
Project Management	Jeff Barber	10%	Apr – Jun 2021
Records Subject Matter Experts	Trevor Youdale Bev Qualizza	50%	Apr – Jun 2021
s.13			
Premier's Office Practice SMEs	Jackie Allen Brittany Hawkins	25%	Apr – Jun 2021

5. Key Stakeholders

The following stakeholders' interests must be considered:

Stakeholders	Potential Impact L / M / H	Need to Consult Yes/No	Need to Inform Yes/ No
Deputy to the Premier	s.13		
Other Deputy Ministers' Offices			
Government Chief Information Officer			
Government Chief Records Officer			
s.13			
Government Records Service			

Approved by:: Susan Laidlaw, Executive Director, Government Records Service March 30, 2021

CIRMO Project Initiation Document

Project Information

Client	BC Premier’s Office
Project Name	Premier’s Office Information Management Practice Review
Business Owner	Jackie Allen
Project Sponsor	Jill Kot & Christina Zacharuk
Start Date	March 26, 2021
End Date	June 30, 2021

1. Purpose

To review the information management practices currently in place in the Premier’s Office, and to make recommendations on improvements to functions and processes.

2. Scope:

In Scope:

- Identification and documentation of the current state of IM within the Premier’s Office, including:
  - records management (RM)s.13 roles and responsibilities within the Premier’s Office
  - existing RM practices, including electronic and physical filing systems and practices around the retention of documents
  - s.13
- Identification of the desired future state, including:
  - RM roles and responsibilities
  - RM practices and procedures
  - s.13
  - Appropriate recordkeeping system (e.g. LAN structure, EDRMS Content Manager)
  - Training
  - On-going monitoring and assessment
- Development of recommendations for actions to reach the desired future state

Out of Scope:

- Assessment of records management practices in other offices (i.e. IGRS, Cabinet Operations or Executive Branch)
- Assessment of privacy or security practices
- Implementation of recommendations (e.g. filing/records management)

3. Deliverables

a. Current State Assessment
b. Future State Recommendations
c. Gap Analysis
d. Recommended Action Plan

4. Resource Management

Function/Role	Name	% FTE	Timeframe
Project Sponsor	Jill Kot & Christina Zacharuk	5%	Apr – Jun 2021
Project Management	Jeff Barber	10%	Apr – Jun 2021
Records Subject Matter Experts	Trevor Youdale Bev Qualizza	50%	Apr – Jun 2021
s.13			
Premier's Office Practice SMEs	Jackie Allen Brittany Hawkins	25%	Apr – Jun 2021

5. Key Stakeholders

The following stakeholders' interests must be considered:

Stakeholders	Potential Impact L / M / H	Need to Consult Yes/No	Need to Inform Yes/ No
Deputy to the Premier	s.13		
Other Deputy Ministers' Offices			
Government Chief Information Officer			
Government Chief Records Officer			
s.13			
Government Records Service			

Approved by:: Susan Laidlaw, Executive Director, Government Records Service March 30, 2021

Report Title

Organization Name(S)

Corporate Information and Records Management Office
Ministry of Citizens' Services

Report Date

BRITISH COLUMBIA
Ministry of Citizens' Services

Table of Contents

Introduction

What is this project about?

About this Report

What is this specific report about?

Summary of Recommendations (Executive Summary etc.)

Heading Level 1

This section of the report provides an overview of the current state of data analysis for each ministry. It also provides supplemental details of recommended early adopter conversion projects not covered in the summary of recommended "early adopter" projects.

Subheading Level 2

Premier's Office IM Assessment – Initial Team Meeting April 8, 2021

Attendees: Elbahir, Cindy; Fern, Chelsea; Youdale, Trevor; Barber, Jeff

Regrets: Qualizza, Beverly

1. Welcome
2. Project Structure: Team Members and Steering Committee Members
3. Project Kick-off Meeting
4. Project Deliverables, Approach, Team Meetings
5. Review Project resources
6. Project Timelines
7. Continued Discussion

- In general Friday's are good for the premier's office in general for scheduling
- We should do our best to be coordinated and keep our contact as limited as necessary to produce our reports, due to nature of the office
- It may be that we can leave some tools for the premier's office throughout the process.
- Question for Jackie Allen: How do you expect us to work with the various contacts within the Premier's office. Jackie has confirmed she is the contact for records management
- Are there client report examples that were created out of an assessment as an example.
- Maybe Audit reports as a model as well
- Trevor will share his meeting notes with Jackie Allen with the team

Actions:

- Cindy to set up a Contacts meeting Trevor, Cindy and Jackie Allen. Formalize contacts s.13 s.13

s.13

- Trevor to circulate or post his RM consultation notes to the MS Teams channel
- Jeff to reach out to Matt Reed and see if we can get some samples assessment reports that have been generated already.
- Jeff As part of prep for project kick-off meeting continue to refine timelines and circulate or post to MS teams Channel prior to kick-off meeting

CIRMO Project Initiation Document

Project Information

Client	BC Premier's Office
Project Name	Premier's Office Information Management Practice Review
Business Owner	Jackie Allen
Project Sponsor	Christina Zacharuk
Start Date	March 26, 2021
End Date	June 30, 2021

1. Purpose

To review the information management practices currently in place in the Premier's Office, and to make recommendations on improvements to functions and processes.

2. Scope:

In Scope:

- Identification and documentation of the current state of IM within the Premier's Office, including:
  - records management (RM)s.13 and responsibilities within the Premier's Office
  - existing RM practices, including electronic and physical filing systems and practices around the retention of documents
- Identification of the desired future state, including:
  - RM roles and responsibilities
  - RM practices and procedures
  - Appropriate recordkeeping system (e.g. LAN structure, EDRMS Content Manager)
  - Training
  - On-going monitoring and assessment
- Development of recommendations for actions to reach the desired future state

Out of Scope:

- Assessment of records management practices in other offices (i.e. IGRS, Cabinet Operations or Executive Branch)
- Assessment of privacy or security practices
- Implementation of recommendations (e.g. filing/records management)

3. Deliverables

a. Current State Assessment
b. Future State Recommendations
c. Gap Analysis
d. Recommended Action Plan

4. Resource Management

Function/Role	Name	% FTE	Timeframe
Project Sponsor	Christina Zacharuk		
Advisor	Jill Kot		
Project Management	Jeff Barber	10%	Apr – Jun 2021
Records Subject Matter Experts	Trevor Youdale Bev Qualizza	50%	Apr – Jun 2021
Premier’s Office Practice SMEs	Jackie Allen Brittany Hawkins	25%	Apr – Jun 2021

5. Key Stakeholders

The following stakeholders’ interests must be considered:

Stakeholders	Potential Impact L / M / H	Need to Consult Yes/No	Need to Inform Yes/ No
Deputy to the Premier	s.13		
Other Deputy Ministers’ Offices			
Government Chief Information Officer			
Government Chief Records Officer			
s.13			
Government Records Service			

Premier’s Office

Information Management Assessment

Corporate Records and Information Management Office (CIRMO)

April 2021

BRITISH
COLUMBIA

Ministry of
Citizens’ Services

Introductions

AGENDA

Introductions

Sponsor Message

Project Objective and Scope

Project Structure

Project Approach

Project Deliverables

Project Timelines

Next Steps

Discussion

Sponsor’s Kick-off Message

Project Objective and Scope

Review and Recommend Improvements to

Records Management

- Appropriate Record Keeping Systems
- Roles and Responsibilities
- Practices & Procedures
- Training Needs
- Ongoing Monitoring and Assessment

Scope

- Executive Branch

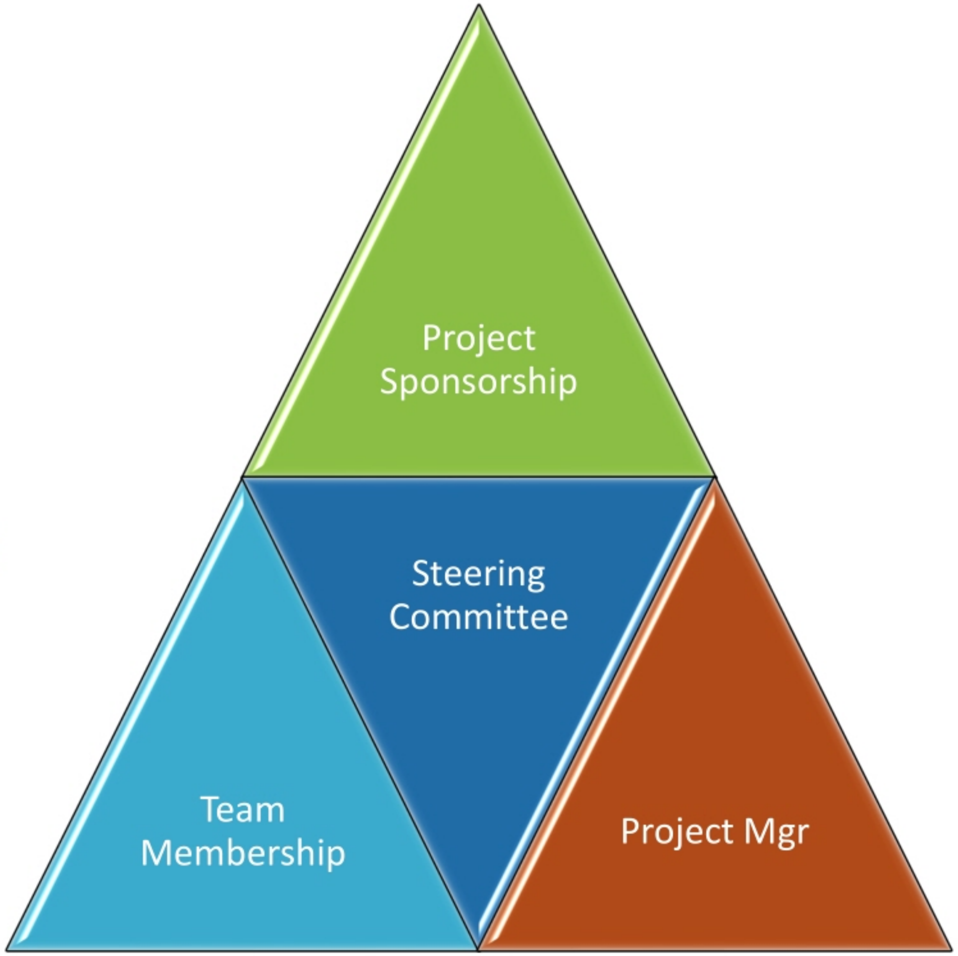
Project Structure

Project Sponsorship
Premier's Office

Christina Zacharuk

Team Membership
Premier's Office - CIRMO

Jackie Allen
Brittany Hawkins
Trevor Youdale
Bev Qualizza



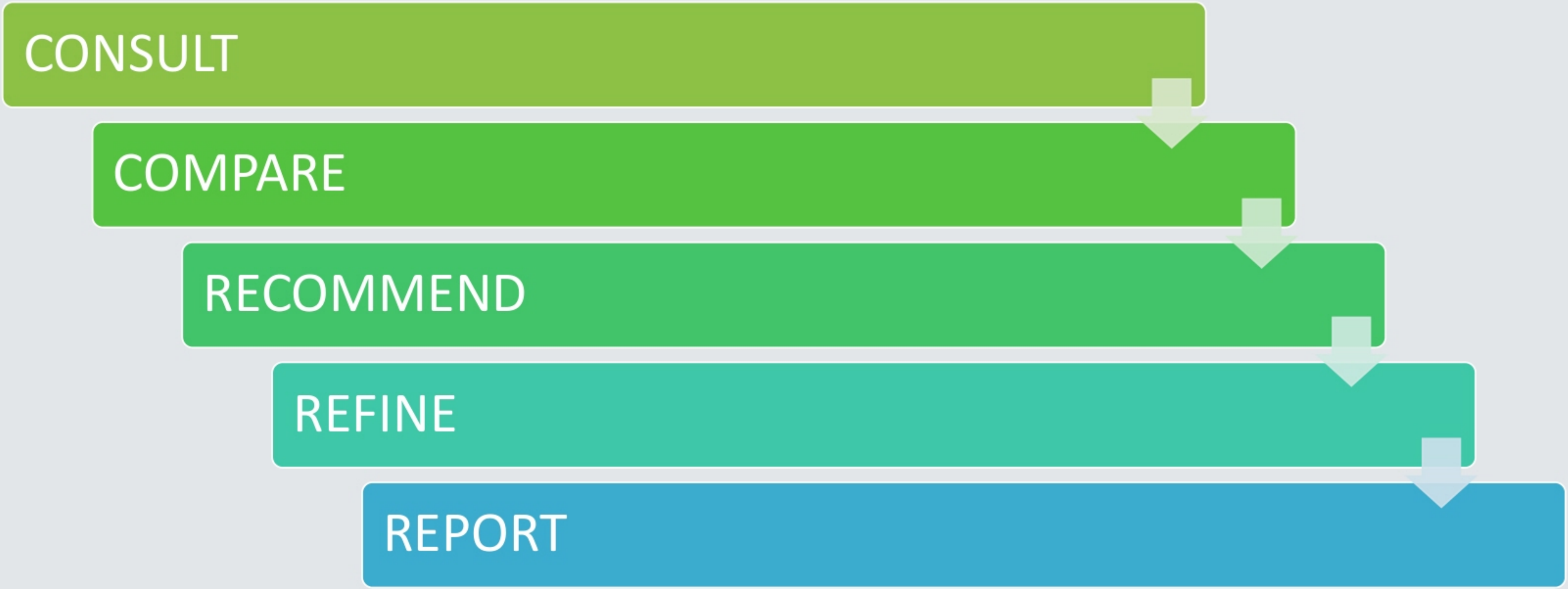
Steering Committee
Premier's Office - CIRMO

Christina Zacharuk
Jill Kot
Jackie Allen
Kerry Pridmore
Susan Laidlaw

Project Manager
CIRMO

Jeff Barber

Project Approach



CONSULT

COMPARE

RECOMMEND

REFINE

REPORT

Project Deliverables

Current State Assessment Report

Gap Analysis - Report

Future State Recommendations Report

Recommended Action Plan – Final Report

Timeline Overview

- April 16, 2021 Project Kick-off Meeting/Consultation Begins
- May 3, 2021   Initial Current State Assessment Report May 4, 2021
- May 4, 2021 Steering Committee Meetings bi-weekly
- May 17, 2021 Final Current State Report and Gap Analysis Report
- May 31, 2021   Initial Report Future State Recommendations Report
- June 1-3, 2021 Steering Committee Feedback on Future State Recommendations
- June 14, 2021   Recommended Action Plan Report

Next Steps

April 16, 2021 Project Kick-off Meeting/Consultation Begins

May 3, 2021 Initial Current State Assessment Report

May 4, 2021 Steering Committee Meetings Bi-weekly

Discussion

PREM IM Assessment – April 23 meeting – Agenda

- Review of draft RM manual – reviewing and answered questions
- IM Assessment - framework scoring exercise – see completed notes
- Review of LAN – high level design – JA scheduled meeting on April 30 to review LAN models and disposition strategies
- Other – discussion on scope of ORCS amendment – clarify Cab Ops and IGRS out of scope; BQ will work with client to draft ORCS update request;s.13 s.13 and BQ will follow-up with client concerning reclassification of case files already in storage.
- Next steps – TY to draft assessment report

IM Assessment summary for Steering Committee - April 3, 2021

Approach

CIRMO has established a standardized framework of Information Management (IM) criteria to assess ministry practices in relation to IM legislation and policy requirements.

This review facilitates the advancement of IM practices by determining the current maturity of ministry processes and identifying continuous improvement activities.

The overall objective of this review is to reinforce the Office's ongoing commitment to continuous improvement through an objective review of IM practices.

About the report

The draft Current State Assessment Report has been prepared for review by the client. This will be followed by a report on gaps and recommendations.

This current state review included interviews conducted with employees, a review of the Office's documentation and record keeping systems, and review of Records Management practices.

s.13

Early Insights

s.13

s.13

Page 351 of 444 to/à Page 420 of 444

Withheld pursuant to/removed as

s.13

AGENDA

PREMIER'S OFFICE INFORMATION MANAGEMENT ASSESSMENT

STEERING COMMITTEE MEETING – MAY 3rd 2021

Attendees: Jill Kot (PREM), Christina Zacharuk (PREM), Kerry Pridmore (CIRMO), Jackie Allen (PREM), Susan Laidlaw (CIRMO), Jeff Barber (CIRMO)

1. WELCOME
2. WORKING GROUP REPORT OUT TO STEERING COMMITTEE
3. DISCUSSION
4. NEXT STEPS

Next Meeting: May 18th, 2021

IM Assessment:
Future State Recommendations Report

Corporate Information and Records Management Office

Information Management Practice Review

of the

Office of the Deputy Minister to the Premier

June 16, 2021

Executive Summary

The Office of the Deputy Minister to the Premier ("the Office") has requested the Corporate Information and Records Management Office (CIRMO) review their records management practices and to make recommendations on improvements to functions and processes.

The review utilized a standardized framework of Information Management (IM) criteria to assess practices in relation to IM legislation and policy requirements.

s.13

Background

The Office of the Deputy Minister to the Premier ("the Office") has requested the Corporate Information and Records Management Office (CIRMO) review their records management practices currently in place, and to make recommendations on improvements to functions and processes.

The mandate of the Chief Records Officer (CRO) in CIRMO includes a requirement for "promoting effective information management across government agencies." In support of this mandate, CIRMO has established a standardized framework of Information Management (IM) criteria to assess practices in relation to IM legislation and policy requirements. The framework assessment tool facilitates the advancement of IM practices by determining the current maturity of processes and identifying continuous improvement activities.

Purpose

The overall objective of this review is to reinforce the Office's ongoing commitment to continuous improvement through an objective review of IM practices. This objective will be accomplished by:

- reviewing and analyzing IM practices within the Office,
- utilizing a Practice Review Framework ("the Framework") of standardized criteria derived from legislation and policy to assess the Offices' IM practices,
- highlighting effective practices and identifying areas for improvement,
- assessing the current maturity of IM practices and recognize ongoing efforts to prepare for future, and
- providing recommendations for improving the overall management of the Office's information.

Benefits to the Office

A review is designed to provide the Office with an objective, risk-based assessment of its IM activities and practices, and practical recommendations for improvements. Benefits include:

- promotion of IM compliance with policies and legislation,
- improvement in records management practices,
- identification of potential areas of IM-associated risk,
- increased employee awareness of IM requirements across all domains, and
- continuous improvement in IM practices.

Scope and Approach

This review included interviews conducted with employees, a review of the Office's documentation and record keeping systems, and review of records management practices. The Office's current practices were in scope of this review, but historical practices were not assessed. The scope of this review did not include the areas of privacy, access to information, and information protection.

To gather evidence that demonstrated the maturity of IM practices, this review was based on the Framework's records management criteria. Findings were summarized within the Framework and rated based on its maturity scale. The maturity scale ranges from:

Level 1	Initial	s.13
Level 2	Repeatable	
Level 3	Defined	
Level 4	Managed	
Level 5	Optimized	

For most criteria, meeting the *Defined* maturity value demonstrates that policy and legislative requirements are communicated, documented, and consistently followed. Scores of *Initial* to *Repeatable* indicate that current practices are not yet mature enough to ensure compliance, although they do not indicate non-compliance. Further, as the risk inherent in some criteria is lower than others, there is minimal concern about lower scores in these areas.

It is also important to note that the Framework was developed with entire ministry organizations in mind and therefore requires interpretation to meaningfully scale down to a small office. For example, it is important to appreciate the value of implicit knowledge, common digital and physical space, and the everyday direct interpersonal communications that occur in a small office. In many cases the term 'office' has been added to Framework criteria titles and substituted for ‘Ministry’ when interpreting each criterion.

Observations

The *Information Management Act* contributes many of the criteria found within the records management domain. Communication of records management roles and responsibilities, administration of general and role-based records management training for employees, and the application of information schedules to records are some of the categories contained within the records management domain. Additional categories assess off siting, destruction and archiving activities, records transfers between government and non-government bodies, and management of digital and physical records.

s.13

s.13

s.13

s.13

Gap Analysis

s.13

s.13

s.13

s.13

s.13

s.13

s.13

Recommendations

s.13

s.13

s.13

s.13

s.13

Conclusion

s.13

Date: June 28, 2021 11:35:29 AM

This page is automatically updated from the Wiki in Microsoft Teams - any changes made here will be overwritten. To edit this page, open it in Microsoft Teams.

Premier's Office Notes

Draft Project Timeline

March 30: Project Project Initiation Document Approved
March 30: Steering Committee being established bi-weekly meetings
March 30: Jeff to reach out to Jackie Allen to set up kick-off meeting
April 06 Jackie Allen confirming Brittany's role and project sponsor address to the team in Project Kickoff meeting. Will confirm if speaking notes are required
April 08: Project Team: Initial Discussion Meeting

April 16: Project Kick-off Meeting - Include messaging from Executive (Jill or Christina)
April 21 Steering Committee (1st Meeting)

Phase 1A Current State Assessment - Records Management

Executive Branch/DMO Consultation
Drafting - Current State Assessment

Current State Initial Report Due Date: April 27th

s.13

Phase 1A & 1B Current State Report out May 04 Steering Committee (2nd Meeting)

Phase 2A Records Management Gap Analysis - Future State Determinations

GRS - consult as needed and determine & document recommended target levels - Executive Branch/DMO

Drafting GAP Analysis Report

GAP Analysis Report Due Date: May 11th

s.13

Phase 2A & 2B GAP Analysis Report out May 18 Steering Committee (3rd Meeting)

Phase 3A Records Management Future State Recommendations

GRS - Develop Future State recommendations from Gap Analysis

Drafting Future State Recommendations Report

Future State Recommendations Report Due Date: May 25th

s.13

Phase 3A & 3B Future State Recommendations - Report out June 01 Steering Committee (4th Meeting)

Gather Feedback from Steering Committee

Steering Committee Feedback Due June 4

Phase 4 Records Management s.13 **Action Plan**

GRS to Develop Recommended Action Plan based on Steering Committee Report out of Phase 3

s.13

Final Report Due June 11

Phase 4 Records Management s.13

Steering Committee (5th Meeting)

Action Plan Report out June 15

June 29 Steering Committee (6th Project Wrap-up)
June 30: Project Completion Date

Project Structure

Steering Committee Members

Name	Title	Organization
Kerry Pridmore	ADM, CIRMO, Chief Records Officer	CITZ
Jill Kot	Deputy Minister	PREM
Christina Zacharuk	Associate Deputy Minister	PREM
Jackie Allen	Director, Executive Operations	PREM
s.13		
Susan Laidlaw	Exectutive Director, Government Records Service	CITZ

Project Team Members

Name	Title	Organization
s.13		
Trevor Youdale	Manager, Client Services - Prem	CITZ
Bev Qualizza	Government Records Officer - Prem	CITZ
Jeff Barber	A/Director, Information Solutions and Transformation	CITZ
Brittany Hawkins - TBD	Administrative Assistant, Deputy Minister's Office	PREM