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

Privacy

#	Criteria	Maturity Scale: 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.

Privacy		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Governance and Accountability						
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						
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.

Privacy		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Governance and Accountability						
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.
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.

Privacy		Maturity Scale				
#	Criteria	1 - Initial	2 - Repeatable	3 - Defined	4 - Managed	5 - Optimized
1. Governance and Accountability						
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.
8.2	**Information Incident Tracking** The ministry regularly and consistently tracks key information about information incidents within their responsibility.	The ministry does not track information about information incidents that are their responsibility.	The ministry tracks only basic information about information incidents that are their responsibility, or tracks this information inconsistently.	The ministry regularly and consistently tracks key information about information incidents within their responsibility.	The Ministry tracks key information about information incidents and has developed incident response plans specific to their business context. The Ministry monitors its incident reporting and processes, analyzes trends and root causes, and identifies remediation steps as required.	The Ministry exercises its incident response plans on a regular basis. The internal and external information environments are monitored and evaluated for issues affecting incident risks and responses; changes and improvements to the incident response plans are made where necessary. Regular reports are provided to executive on the Ministry's performance.

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 adherance 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 highe 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						
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 i 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 digita 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 tern retention or systematic monitoring of formats and record repositories to help ensure long term usability.
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.	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 suc procedures into existing business processes.
5.3	**Records Transfers to Non-IMA Bodies** The Ministry has documented procedures in place t 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 system 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
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.

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.

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.

Interview #	Division	Branch	Date	Interviewee	Role	Interview Type	Interviewers	Notes	Folder Location
1	CS	IMB	2019-03-15	Stan Andersen	Ministry Coordinator	Planning	DK/CL/BJ/BI	IMPR planning status update	Planning
2	CS	IMB	2019-03-21	Gary Mierzuak	MISO	Planning	DK/CL/BJ/BI	IMPR planning status update	Planning
3	CS	IMB	2019-03-26	Heather Dunlop	MPO	Planning	SL/DK/CL/BJ/BI	IMPR planning status update	Planning
4	CS	IMB		Heather Dunlop	MPO	Planning			Planning
5	CS	IMB		Gary Mierzuak	MISO	Planning			Planning
6	CIRMO	GRS			RO	Planning			Planning
7	CIRMO	IAO			FOI Manager	Planning			Planning
8	CIRMO	PCT			Privacy Operations	Planning			Planning
9	CIRMO	PCT			Privacy Policy	Planning			Planning
10	CIRMO	PCT			Investigations Unit	Planning			Planning

Division	Branch	Interviewee	Title	Interview Type	Notes
CIRMO	GRS	Susan Laidlaw	Executive Director		
CIRMO	SPP	Mark Sime	A/Director		
CIRMO	SPL	Melissa Sexsmith	A/Executive Director		
CIRMO	DivOps	Mirella Standbridge	Director		
CIRMO	IAO	Chad Hoskins	Executive Director		
CIRMO	PCT	Matt Reed	Executive Director		
SBC	DivOps	Debbie MacLean	Manager		
SBC	SS & LBC	Adriana Poveda	A/Executive Director		
SBC	RegOps	Ron Hinshaw	Executive Director		
SBC	SD	Bao Diep	A/Executive Director		
SBC	Reg	Carol Prest	Executive Director		
SBC	IDIM	Sophia Howse	Executive Director		
SBC	SI	Jeremy Moss	Director		
CS	DivOps	Kiran Grills	A/Manager		
CS	IM	Chris Hauff	Executive Director & MCIO		
CS	FAS	Tim Owen	Executive Director & CFO		
CS	CPP	Brad Williams	Executive Director		
CS	SHR	Sharlane Callow	Executive Director		
PS	DivOps	Angelina Furtado	Manager		
PS	SPO	Tracee Schmidt	Executive Director		
PS	PS	Robert O'Neill	Executive Director		
PS	SS	Dawson Brenner	Executive Director		
PS	SS - PDC	Gary Heuer	Sr. Director		
PS	SS - BCMP	Don Swagar	Sr. Director		
PS	SS - QP	Spencer Tickner	Director		
PS	SS - AIR	Leslie Walden	Director		
PS	SS - DCV	Leslie Walden	Director		
PS	PT	Kerry Pridmore	Executive Director		
PS	FPR	Wendy Turcotte	Director		
PS	CMC	DeAndra Chmelyk	Director		
ICT	DivOps	Kimberly Rosche	Manager		
ICT	SI	Roman Mateyko	Executive Director		
ICT	CMN	Michael Rolston	Executive Director		
ICT	NBC	Howard Randell	Executive Director		
ICT	CI	Colleen McCormick	Director		
ICT	PM	Ivan Rincon	Executive Director		
RP	DivOps	Judy Turner	Manager		
RP	REBS	Lorraine McMillan	Director		
RP	WDS	Diane St. Hilair	A/Executive Director		
RP	SRES	Yvonne Deibert	A/Executive Director		
RP	CS	John Hammond	A/Executive Director		
RP	AccomMgmt	Lorne DeLarge	Executive Director		
RP	AssetMgmt	Jon Burbee	Executive Director		
RP	FCMS	Graham Taylor	Executive Director		
RP	FPR	May Yu	Director		
OCIO	ES - DS	Michael Gergel	Executive Director		
OCIO	ES - NCCS	Colin Coughlin	A/Executive Director		
OCIO	ES - SM	Terry Whitney	Executive Director		
OCIO	ES - IS	Gary Perkins	Executive Director & CISO		
OCIO	ES - ASP	Paul Roberts	A/Executive Director		
OCIO	ES - HS	Stuart Restall	Executive Director		
OCIO	ES - DSAO	Nadine Criddle	Executive Director		
OCIO	ES - DSAO	Caroline Hergt	A/Executive Director		
OCIO	DIO	Corinne Timmerman	Executive Director		
OCIO	DSO - BCDE	Peter Watkins	Executive Director		
OCIO	DSO - CSI	Rumon Carter	Executive Director		
OCIO	DSO - EDI	John Jordan	Executive Director		
OCIO	DSO - EA	Mac Campbell	A/Executive Director		
OCIO	DSO - SPP	[Lisa Koorbatoff] ??	Sr. Director		

Division	Branch	Interviewee	Title	Interview Type	Notes
OCIO	DSO - FADSS	Marcela Grove	A/Director		
OCIO	IDD - IDD	Hayden Lansdell	Executive Lead		
OCIO	IDD - DSA	Jeremy Coad	Executive Director		
OCIO	IDD - SCI	Sue Wheatley	Executive Director		
OCIO	IDD - DSS	Genevieve Lambert	Executive Director		
OCIO	IDD - PL	Beth Collins	Director		
DMO	ExecOps	Jeannette Cook	Director		
DMO	ExecOps	Jennifer Peddle	Information & Privacy Coord		

Abbreviations	
Abbreviation	**Ministry/Division/Branch**
CS	Corporate Services Division
IMB	Information Management Branch

IMPR Team	
Abbreviation	**Name**
SL	Stephen Li
BJ	Brittany Jackson
DK	Darlene Kotchonoski
BI	Benson Izunwanne
CL	Carman Lam

Information Management Practice Review Interview Questions

Worksheet

General		Staff Questions	Response	Privacy	Records Mgmt	Info Access	Info Prot	Comment
General		Do you (or your staff) manage contracts?		4.4, 5.1, 5.2, 5.3, 5.4		4.2	1.12, 1.17	Where questions are identified as OPTIONAL staff that do not have responsibility in these areas the questions may not be applicable given their job related duties.
General		Have you (or your staff) created or reviewed a Privacy Impact Assessment?		3.1				
General		Have you (or your staff) ever been involved in a Freedom of Information request?			5.2	1.2, 2.2, 3.1, 4.1		
General		Have you (or your staff) ever created or reviewed an Information Sharing Agreement, Research Agreement, Common or Integrated Program Agreement		4.1, 4.2, 4.3, 6.4				
General		Have you or your staff been involved in transferring records to other public bodies under the IMA?			6.2, 6.3			

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
P1.1	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?	N/A - Delegation of MPO role is not applicable to manager	N/A - Delegation of MPO role is not applicable to staff		MPO Job Description or email	
P1.2	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?	N/A -Deputy Delegation of Duties is not applicable to manager	N/A -Deputy Delegation of Duties is not applicable to staff		deputy delegation instrument	
P1.3	1.3	MPO Delegation of Duties - If the MPO has delegated any duties, powers or functions (such as MPO delegating to an Analyst the review and sign off of PIAs), a formal PMAP delegation instrument is documented, in	Have you, in turn, delegated any duties to others? If so, has a PMAP Delegation Instrument been completed? May I get a copy?	N/A -MPO Delegation of Duties is not applicable to manager	N/A -MPO Delegation of Duties is not applicable to staff		MPO delegation instrument	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
		place, and current. Delegation instruments are maintained and communicated to CIRMO						
P1.4	1.4	Privacy Policies/Procedures - Ministry-specific privacy policies and procedures, incorporating Ministry-specific privacy requirements, have been developed and deployed, where appropriate.	Are there any Ministry-specific privacy policies or procedures in place? IF so, are they approved, up-to-date and communicated to staff?	Have you implemented any privacy policies or procedures specific to your work (beyond the government policies and procedures)?	Are there any Ministry-specific privacy policies or procedures in place for the work that you do?		ministry specific policies/ procedures	
P2.1	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.	What percentage of ministry employees have completed IM117? How often is IM117 staff training refreshed? Do you augment staff awareness with emails, posters or similar?	How often have you taken IM117? Is privacy training regularly scheduled? How do you raise awareness about privacy issues to your staff (e.g., emails, posters, newsletters, team	How often have you taken IM117? Is privacy training regularly scheduled? Have you seen any emails, posters, newsletters etc. talking about privacy or raising awareness of privacy issues?		training stats	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
				meetings, etc.)? Do you have a sample?				
P2.2	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 that 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?	Do your staff require privacy-specific training (beyond IM 117)? What kind of training is provided?	OPTIONAL: Do you require privacy-specific training (beyond IM 117). What kind of training is provided?		training procedures, names of courses, employees, stats	
P3.1	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 a process for PIAs in your ministry? If so, how do you keep staff updated and aware of the process (e.g., SharePoint, newsletters, emails regarding policies, procedures for completion of PIA, etc.)	Have you ever done a Privacy Impact Assessment. What is the process OR how would you find out the process for doing a PIA in your ministry?	OPTIONAL: Have you ever done a Privacy Impact Assessment. What is the process OR how would you find out the process for doing a PIA in your ministry?		PIA process, communication tools	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
P3.2	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, cancelled and in-progress PIAs? How do you keep track of outstanding items for follow-up?	N/A - Inventory of PIAs is not applicable to manager OPTIONAL: Have you or your staff worked on a PIA - Were you able to keep informed about the approval progress of your PIA?	N/A - Inventory of PIAs is not applicable to staff OPTIONAL: If the staff person has worked on a PIA - Were you able to keep informed about the approval progress of your PIA?		PIA inventory	
P3.3	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	How do you determine that PIAs are completed prior to the start of any proposed enactment, system, project, program or activity? Is there a ministry-wide process to make you aware of upcoming projects or activities that may require PIAs?	Do you know when a PIA must be completed? How would you find out the process for doing a PIA in your ministry?	Do you know when a PIA must be completed? How would you find out the process for doing a PIA in your ministry?		documented process	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
		are sent to CIRMO for retention and entry into the Personal Information Directory (PID).						
P4.1	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? Ensure that you are involved in the development and/or updating of these agreements?	Have your staff ever worked on a ISA, RA, CPA or IPA? OPTIONAL: How were you informed that the Agreement was approved? Were you able to check your Agreements in the Personal Information Directory?	N/A - Reporting ISAs, RAs, CPAs and IPAs to CIRMO is not applicable to staff OPTIONAL: If the staff person has worked on a ISAs, RAs, CPAs and IPA - How were you informed that the Agreement was approved? Were you able to check your Agreements in the Personal Information Directory?		documented process	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
P4.2	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.	Do you have a process to require that ISAs are reported to CIRMO for entry into the PID?	Have your staff ever worked on a ISA? OPTIONAL: How were you informed that the ISA was approved? Were you able to check your ISA in the Personal Information Directory?	N/A - Reporting ISAs to CIRMO is not applicable to staff OPTIONAL: If the staff person has worked on a ISA? How were you informed that the ISA was approved? Were you able to check your ISA in the Personal Information Directory?		documented process	
P4.3	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 have an inventory of completed, cancelled or in-progress RAs? How do you keep track of outstanding items for follow-up?	Have your staff ever worked on RAs? OPTIONAL: Did anyone ever follow up with you regarding the RA? How were you informed that the RA was	N/A -Inventory of Research Agreements is not applicable to staff OPTIONAL: If the staff person has worked on RAs, - Did anyone ever follow up with		RA inventory and management process	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
				approved?	you regarding the RA? How were you informed that the RA was approved?			
P4.4	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.	Do you have a process to monitor compliance with privacy requirements as outlined in agreements?	Do you or your staff manage Agreements with other parties? OPTIONAL: How is the privacy compliance for other parties monitored? Is there a path for escalation or corrective measures built into the Agreement?	N/A - Monitoring Compliance with Privacy and Security Requirements in Agreements is not applicable to staff OPTIONAL: If the staff person has worked on Agreements - How is the privacy compliance for other parties monitored? Is there a path for escalation or corrective measures built into the Agreement?		documented process	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
P5.1	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	Do contract managers (responsible business units) make you aware of contracts involving personal information? What process is used to confirm that Privacy Protection Schedules are included in service provider contracts that contain personal information?	Do you or your staff manage service providers? OPTIONAL: Do you and/or your staff make the MPO aware of contracts involving personal information?	If the staff person manages contracts OPTIONAL: If you manage contracts containing personal information, do you have a defined process that ensures PPS are included in each contract?		documented process	
P5.2	5.2	Inventory of Access to Personal Information - The MPO maintains an up to date inventory of service providers or volunteers with access to personal information within the Ministry's custody and control.	Do you have an inventory of service providers or volunteers with access to personal information within your ministry's custody and control? How do you keep the inventory up to date?	Do you or your staff manage service providers or volunteers OPTIONAL: If you manage contracts containing personal information, do you have a defined process that	If the staff person manages service providers or volunteers OPTIONAL: If you manage contracts containing personal information, do you have a defined		Inventory of Personal information	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
				ensures PPS are included in each contract?	process that ensures PPS are included in each contract?			
P5.3	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.	Do you have a process to confirm that service providers and volunteers have had mandatory privacy training (IM117) prior to providing services?	Do you or your staff manage service providers or volunteers OPTIONAL: Do you have a process to confirm that service providers and volunteers have had mandatory privacy training (IM117) prior to providing services?	If the staff person manages service providers OPTIONAL: Do you have a process to confirm that service providers and volunteers have had mandatory privacy training (IM117) prior to providing services?		documented process	
P5.4	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).	Do you have a process to monitor service provider compliance with privacy requirements? Is there a process to define how the service provider	OPTIONAL: If service providers are managed - Do you have a process to monitor service provider compliance	OPTIONAL: If the staff person manages service providers - Do you have a process to monitor service		documented process	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
			should address instances of non-compliance? (E.g., call 7-7000)	with privacy requirements? Is there a process to define how the service provider should address instances of non-compliance?	provider compliance with privacy requirements? Is there a process to define how the service provider should address instances of non-compliance?			
P6.1	6.1	Create and Maintain Personal Information Inventory - A procedure exists to create and maintain a Personal Information Inventory, and to create it within one year of the Personal Information Inventory Policy being published	Future requirement being defined as part of the Privacy Management and Accountability Policy.	N/A - Personal Information Inventories and Directory are not applicable to managers	N/A - Personal Information Inventories and Directory are not applicable to staff		documented procedure	
P6.2	6.2	Reporting to CIRMO - A procedure exists for the creation and reporting to CIRMO of Personal Information Banks as required.	Do you have policies or procedures for the creation and reporting of PIBs? How do you make employees aware of the policies or procedures?	Have you created a Personal Information Bank? OPTIONAL: Who guided you through	N/A - Reporting to CIRMO is not applicable to staff		documented procedure	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
				the process or was there a documented procedure?				
P6.3	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?	Health only: Have you created a Health Information Bank? OPTIONAL: Who guided you through the process or was there a documented procedure?	N/A - Health Information Banks) is not applicable to staff		documented procedure	
P6.4	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.	Do you have a policy or procedure to review the PID annually? How do you determine that all PIAs, ISAs, PIBs and where applicable HIBs are submitted and recorded accurately? What is the process to correct entries?	N/A - Monitoring of Personal Information Directory (PID) is not applicable to managers	N/A - Monitoring of Personal Information Directory (PID) is not applicable to staff		documented process	
P7.1	7.1	Reporting Foreign Demands - A	Is there a ministry policy and/or	N/A -Foreign Demands for	N/A -Foreign Demands for		documented	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
		procedure is in place for reporting foreign demands for disclosure to CIRMO.	procedure requiring that foreign demands be reported to CIRMO?	Disclosure have a very low occurrence (May 2018) and as such are not currently applicable to managers	Disclosure have a very low occurrence (May 2018) and as such are not currently applicable to staff		procedure	
P8.1	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.	Is there a ministry policy and/or procedure supporting Information Incident Management? Are there ministry communications on how and when to report information incidents? How do you track and follow up on incidents?	What is the process for reporting an information incident? Do you periodically communicate about how and when to report information incidents? OPTIONAL: Do you have any samples of your communications to staff?	What is the process for reporting an information incident? Does the Ministry periodically communicate about how and when to report information incidents?		documented process	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
R1.1	1.1	Records Management Accountabilities - The Ministry has articulated employees' responsibilities for records management and business areas have clearly assigned accountabilities to employees with additional role specific records management duties, as appropriate. There is a clear understanding of respective roles and responsibilities and the names of such person(s) or group(s) and their responsibilities are communicated to internal personnel.		How are RM responsibilities communicated to staff? Have you seen any written procedures or guidance on your own responsibilities for records management?	How are RM responsibilities communicated to staff? Have you seen any written procedures or guidance on your own responsibilities for records management?		documented responsibilities	
Rec. Mgmt	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? If so, how are these RM policies/proce	Do you have any Ministry-specific policies or procedures related to records management? How does the Ministry provide		ministry specific policies or procedures	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
				dures communicated to staff?	updates about RM policies/procedures?			
Rec. Mgmt	2.1	Mandatory Employee Training - Employees have completed mandatory training related to records management (IM117).					training stats	
Rec. Mgmt	2.2	Role Specific Training - Individuals have received additional, role-specific records management training where appropriate.		Do you have any staff members that require additional, RM-specific training (beyond IM 117). How do you identify them and schedule the training?	Do you require additional, RM-specific training (beyond IM 117) in your job? How did the ministry identify that you needed extra training?		documented process	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
Rec. Mgmt	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.		How are your records organized and managed? How do you maintain records of decisions? Do you have any documented procedures about records classification? How are RM requirements communicated to staff?	How are your records organized and managed? Does the Ministry have any documented procedures about records classification, and if so, how are they communicated to you?		documented procedure	
Rec. Mgmt	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.		Future Requirement - GRS has published a draft for discussion.	Future Requirement - GRS has published a draft for discussion		digitization procedures	
Rec.	5.1	Information Schedule	How many	Are your	N/A -		documented	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
Mgmt		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.	approved schedules exist for the ministry? When were the existing schedules last updated? How many schedules are pending/in-progress? How long have they been in-situ?	records scheduled? Do you have a process to update and review the schedule? How do you identify information not covered by an approved schedule?	Information Schedule Development and Maintenance not applicable to staff unless they have been involved in the Record Scheduling process. OPTIONAL: Are your records scheduled? Do you have a process to update and review the schedule? How do you identify information not covered by an approved schedule?		process	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
Rec. Mgmt	5.2	Records Retention, Holds and Disposition - The ministry has procedures to dispose of, transfer, or archive government information based on official policies, specifications, schedules, guidelines, and procedures published by the Government Records Service. In the case of a legal hold or FOI request, the ministry has processes in place to ensure that such records are not destroyed. Where records are scheduled, retention is limited to the scheduled time period and no longer. Unscheduled records are retained.	Does the ministry have procedures implementing RM policies?	Does the ministry have any procedures implementing the government-wide Records Management policies? How do you ensure that records are retained according to the appropriate schedules? In the case of a legal hold or FOI request, what is the process to ensure that those records are not destroyed?	Does the ministry have any procedures implementing Records Management policies? How do you ensure that records are retained according to the appropriate schedules? In the case of a legal hold or FOI request, what is the process to ensure that those records are not destroyed?		documented procedure	
Rec. Mgmt	6.1	Identify and Protect Digital Records Scheduled for Archiving - The ministry has documented procedures for identifying, protecting,	How is GRS making your clients aware of the need to develop ministry procedures to Identify and Protect Digital	Future requirement - Are there any Ministry policies or procedures to identify and protect digital	N/A Future Requirement - Identify and Protect Digital Records Scheduled for Archiving not applicable		documented process	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
		and maintaining the usability and integrity of digital records scheduled for transfer to archives.	Records Scheduled for Archiving?	records scheduled for archiving?	unless they are involved in digital record management			
Rec. Mgmt	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.	How many Records Transfers did the Ministry conduct within the last (5?) years.	Have you or your staff been involved in transferring records to other public bodies under the IMA? OPTIONAL: 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	N/A: Records Transfers to IMA Bodies not applicable to staff. OPTIONAL: If the staff person was involved in preparing materials for transfer - 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		documented procedure	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
				transfer?	continuity of control for records during transfer?			
Rec. Mgmt	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.	How many Records Transfers did the Ministry conduct within the last (5?) years.	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?	N/A: Records Transfers to IMA Bodies not applicable to staff. If the staff person was involved in preparing materials for transfer OPTIONAL: Does your ministry have documented procedures for the transfer of records to public bodies covered by the IMA? If so, do those procedures include guidance to maintain the chain of custody and		documented procedure	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
					continuity of control for records during transfer?			
Rec. Mgmt	7.1	Manage Information in Recordkeeping Systems - The ministry manages government information through its lifecycle using recordkeeping system(s) as appropriate. Systems are used to meet records management requirements, including schedules as mandated in the IMA.	What Divisions/Branches in the Ministry are not using approved record keeping systems? Do you have a process to identify and approve the record keeping systems in use?	In terms of record keeping systems how do you manage records of decisions; transitory records; email; created while working outside the workplace? Do you or does the ministry have a process to remind staff that non-transitory government information held in Outlook (e.g.) is to be transferred for retention in a secure approved	In terms of record keeping systems how do you manage the records you work with? For example how do you manage records of decisions; transitory records; email; created while working outside the workplace?		documented procedure	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
				recordkeeping system?				
Rec. Mgmt	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.	Does the Ministry contact you to manage off-site storage? How many boxes were sent to offsite storage in the last (5?) years? How long are the boxes being maintained in storage - is there a disposal process	Do your business areas or does the Ministry have any documented procedures for the management and storage of physical records, both on and offsite?	N/A: Manage Physical Records not applicable to staff If staff deal with physical records as part of their work. OPTIONAL: Does the ministry have any documented procedures for the management and storage of physical records, both on and offsite?		documented procedure	
Rec. Mgmt	7.3	Inventory of Ministry Systems and Repositories - The ministry maintains an inventory of ministry systems and repositories that manage and/or store government	Do you have an up-to-date inventory of the information systems and repositories in use within the ministry?	Does the ministry/division /branch have an inventory of the information systems and repositories in	Does the ministry/division/branch have an inventory of the information systems and repositories in		documented procedure	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
		information.		use? OPTIONAL: How is the inventory managed?	use? OPTIONAL: How is the inventory managed?			
Info 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 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).		Does the Ministry have documented procedures for Information Access and the Duty to Assist applicants? How are staff informed of their FOI accountabilities and responsibilities?	Are you familiar with the procedures around Information Access and the Duty to Assist? How does the ministry communicate about Information access and FOI processes?		documented process and procedure	
Info Access	1.2	Information Access Accountability - Accountabilities for FOI requests are assigned, and roles and responsibilities		Is there a designated person/role accountable for coordinating	Have you ever been involved in a FOI request? Who handles FOI requests in		Job descriptions, defined responsibilities	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
		are clearly defined.		the response to FOI requests? How are FOI roles communicated to staff in the Ministry?	your area?			
Info Access	2.1	Employee Training - Employees have completed mandatory (IM117) training related to FOI/ Information Access.		Refer to Privacy 2.1			training stats	
Info Access	2.2	Role Specific Training - Individuals have received additional, role-specific FOI/Information Access training where appropriate (e.g. ministerial staff, FOI co-ordinators).		Have any of your staff received additional training on processing FOI information requests? How are training needs identified and staff made aware of their FOI responsibilities, e.g. duty to assist, other FOI policies/proce	OPTIONAL: Does the staff person process FOI requests? Have you received any additional training on processing FOI information requests? How does the Ministry make you aware of the FOI responsibilitie s, e.g. duty to assist, other		documented process to identify staff and training stats	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
				dures?	FOI policies/procedures?			
Info Access	3.1	Dedicated Public Servant - A dedicated Public Servant is designated as the person in charge of all requests involving a Minister's office. This person is accountable for contacting all staff directly, in writing, with the details of the request and directing that staff search for responsive records and respond within a set time period. This individual must also retain a current list of all Ministerial staff that is shared on an ongoing basis with IAO.	Dedicated Public Servant - A dedicated Public Servant is designated as the person in charge of all requests involving a Minister's office. This person is accountable for contacting all staff directly, in writing, with the details of the request and directing that staff search for responsive records and respond within a set time period. This individual must also retain a current list of all Ministerial staff that is shared on an ongoing basis with IAO.	How are FOI requests communicated in the Ministry? Who coordinates the FOI requests for the ministry? E.g., Deputy Minister's Office, Minister's Office?	N/A: Dedicated Public Servant not applicable to staff		job description, list of ministry contacts for FOI requests	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
Info Access	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.		Executive Director/Director - Does the ministry have a documented process for tracking, monitoring and escalating FOI requests? Is a regular report on the status of FOI requests made to management?	N/A: Monitoring of FOI Requests not applicable to staff		documented process	
Info Access	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 service providers are in compliance with ministry procedures regarding FOI requests? Is there a documented process that	If the staff person manages service providers OPTIONAL: How do you have a process to monitor service provider compliance with FOI requirements? Is there a process to define how to		documented process	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
				shows how compliance is monitored?	address instances of non-compliance?			
Info Prot	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.	Do you have a documented Information Security Program? If so, are responsibilities for the program documented and assigned?	N/A: Security Program not applicable to manager	N/A: Security Program not applicable to staff		Defensible Security	
Info Prot	1.2	Employee Training - Employees have completed training related to the protection of government	See Privacy 2.1				training stats	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
		information (IM117 and IM118).						
Info Prot	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	For staff members that require additional, security-specific training (beyond IM 117 and IM 118), is there a process in place to identify staff and schedule required training?	OPTIONAL: For staff members that require additional, security-specific training (beyond IM 117 and IM 118), is there a process in place to identify staff and schedule required training?	OPTIONAL: Do you require additional, security-specific training (beyond IM 117 and IM 118) in your job? Is there a process in place to identify staff and schedule required training?		documented process to identify staff, training stats	
Info Prot	1.4	External Parties - Assessment of risks from external party access to government information, information systems or information processing facilities are performed and appropriate security controls implemented prior to granting access	Are risk assessments conducted before granting access to external parties to government information?				Defensible Security	
Info Prot	1.5	Asset Management - An inventory of information assets and	Does the Ministry/area maintain an	OPTIONAL: Does the Ministry/area			Defensible Security	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
		systems exists and is maintained. Ownership of assets is assigned and accountabilities associated with ownership are defined.	inventory of information systems and assets?	maintain an inventory of information systems and assets?				
Info Prot	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.	How does the ministry document Information protection roles and accountabilities for employees? How do you confirm that staff understand their responsibilities?	OPTIONAL: How does the ministry document Information protection roles and accountabilities for employees? How do you confirm that staff understand their responsibilities?			Defensible Security	
Info Prot	1.7	Physical and Environmental Protection - Equipment containing personal or sensitive information must be protected throughout its lifecycle, including secure disposal, to	Are there any ministry specific policies or procedures about reducing the risk to information due to unauthorized access or loss?	OPTIONAL: Do you have any policies or procedures to guide staff in protecting government information or devices? How	OPTIONAL: How does the ministry communicate requirements to protect government information and devices?		Defensible Security	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
		reduce the risks from unauthorized access or loss.	How does the ministry communicate to staff about security issues?	do you communicate to staff about the need to protect information and devices in their care?				
Info Prot	1.8	Protection Against Malicious Code - There is an established process in place to prevent, detect, and resolve malicious code infections on information systems and infrastructure.	Does the ministry have a documented process or procedure advising 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?)	OPTIONAL: Does the ministry have a documented process or procedure advising 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?)	OPTIONAL: How does the ministry communicate to you about how to protect yourself from malicious code or malware? Government information and devices? (e.g.' Don't click on that attachment' posters or reminder emails?)		Defensible Security	
Info Prot	1.9	Security Classification - Records are organized so that security classifications can be applied to protect	Does the ministry have a policy and procedures to classify records by security	OPTIONAL: Does the ministry have a policy and procedures to	OPTIONAL: How does the ministry communicate to you about		Defensible Security	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
		different classes of information based on their sensitivity.	classification? What percentage/proportion of ministry records have the been classified?	classify records by security classification? What percentage/ proportion of ministry records have been classified?	using security classifications for government information?			
Info Prot	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.	Does the ministry have a policy and procedures regarding the use of portable storage devices? Is there a defined procedure to assist business areas in setting up and managing an inventory for portable media? How do business areas ensure that information is encrypted, and transferred to government record keeping systems as appropriate? How is the	OPTIONAL: Are portable storage devices used in your area? Do you or your staff maintain an inventory of portable storage devices? How do you ensure that information is encrypted and transferred to government record keeping systems as appropriate? How is the process documented	OPTIONAL: Are portable storage devices used in your area? How does the ministry communicate to you about the use of portable storage devices? E.g., USB sticks, etc.		Defensible Security	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
			process documented and communicated to staff?	and communicated to staff?				
Info Prot	1.11	User Access and Responsibilities - Users must only access information permitted by their assigned roles and responsibilities -Users must ensure unattended equipment has appropriate protection. -Users must ensure the safety of sensitive information from unauthorized access, loss or damage.	How does the ministry communicate user responsibilities for the protection of government assets?	OPTIONAL: What steps do you take to prevent unauthorized access or theft of government computing equipment and information? How are user responsibilities for the protection of government assets communicated to staff?	OPTIONAL: What steps do you take to prevent unauthorized access or theft of government computing equipment and information? How does the ministry communicate to you about your responsibilities for protecting government information and assets?		Defensible Security	
Info Prot	1.12	Access Control - Logical access to personal information is restricted by procedures that address the following matters: - Authorizing and	Does the ministry have access management procedures that apply to all users (e.g., staff and contractors?) Is the access to	OPTIONAL: Is the access to systems periodically (at least annually) monitored to ensure that only	N/A: Access Control		Defensible Security	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
		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.	systems periodically (at least annually) monitored to ensure that only authorized and appropriate personnel have access to information systems? Does the ministry have an on-boarding and off-boarding process to confirm that access is granted, changed or revoked in a timely manner?	authorized and appropriate personnel have access to information systems? Does the business area have an on-boarding and off-boarding process to confirm that access is granted, changed or revoked in a timely manner?				
Info Prot	1.13	Security requirements for information systems - Security controls are identified as part of the business requirements for new information systems or enhancements to	Are security controls identified for new or changes to the existing information systems? (e.g. risk assessment	N/A: Security requirements for information systems not applicable for most managers	N/A: Security requirements for information systems not applicable for most staff		Defensible Security	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
		existing information systems through the information security risk assessment (the former STRA) process, and controls are implemented and reviewed prior to implementation.	conducted?) Does the ministry have a process to ensure that security risk and controls are identified prior to implementation or modification of new or existing systems?					
Info Prot	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	Are regular assessment conducted to evaluate risks associated with information system vulnerabilities? What is the process that the ministry undertakes to remediate vulnerabilities?	N/A: Technical Vulnerability Management not applicable to manager	N/A: Technical Vulnerability Management not applicable to staff		Defensible Security	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
		mitigated or remediated.						
Info Prot	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.	Is there a ministry policy requiring applications to be monitored, reviewed and audit logs retained for exceptions and investigation of information security events like tempering and unauthorized access?	OPTIONAL: Do applications in your business area require monitoring, review and audit logs retention for exceptions and investigation of information security events like tempering and unauthorized access?	N/A; Logging and Monitoring not applicable to staff		Defensible Security	
Info Prot	1.16	Business Continuity Management - Business continuity management processes and plans have been developed tested, maintained, updated and they include provisions to maintain security and information protection in the case of an incident.	Do you have a documented, up-to-date Business Continuity Plan in your Ministry? When was the Disaster Recovery Plan last tested?	OPTIONAL: Do you have a documented, up-to-date Business Continuity Plan for your business area? When was the Disaster Recovery Plan last tested?			Defensible Security	

Domain	#	Statement	Specialist Questions	Manager Questions	Staff Questions	Doc Provided (Y/N)	Potential Documents	Responses
Info Prot	1.17	Monitoring Service Provider Compliance with Information Protection requirements - The Ministry has a process to monitor service provider compliance for information protection requirements.	Does the ministry have a process to monitor and track service provider compliance to information protection requirements? Is there a process to define how the service provider should address instances of non-compliance?	OPTIONAL: If the staff person manages service providers - Do you have a process to monitor service provider compliance with information protection requirements? Is there a process to define how the service provider should address instances of non-compliance?	OPTIONAL: If the staff person manages service providers - Do you have a process to monitor service provider compliance with information protection requirements? Is there a process to define how the service provider should address instances of non-compliance?		Defensible Security	

Legend

Domains – Privacy, Records Mgmt, Info Access, Info Protection

Doc? – indicates that potentially a document exists to substantiate verbal responses. There are 51 potential documents that may exist.

Document Provided – was the document provided as part of the initial document request from the Ministry.

Specialist Questions – Questions specific to the MPO (Privacy), RO (Rec. Mgmt), Minister's Office (Info. Access) or MISO (Info. Protection)
General Questions – used at the start of an interview to identify if managers/staff have relevant experience necessary to respond to select questions.
Manager Questions – as described. N/A – not applicable to most Managers. OPTIONAL: potential questions depending on work area.
Staff Questions – as described. N/A – not applicable to most Staff. OPTIONAL: potential questions depending on work area.

Consolidated Responses - Interview Questions

Do Not Print – Display Only

Case Number	
Ministry	
Division	

CONSOLIDATION OF INTERVIEW QUESTIONS BY DIVISION

Privacy								
v# Criteria	**Summary Response 1**	**Summary Response 2**	**Summary Response 3**	**Summary Response 4**	**Summary Response 5**	**Summary Response 6**	**Summary Response 7**	**Summary Response 8**
1. Accountability for Privacy Management								
1.1 **Designated Ministry Privacy Officer** The Deputy Minister has named a Ministry Privacy Officer and roles and responsibilities related to privacy in the ministry have been defined.								
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.								
1.3 **MPO Delegation of Duties** If the MPO has delegated any duties, powers or functions (such as MPO delegating to an Analyst the review and sign off of PIAs), a formal PMAP delegation instrument is documented, in place, and current. Delegation instruments are maintained and communicated to								

Privacy								
v# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
CIRMO.								
1.4 **Privacy Policies/Procedures** Ministry-specific privacy policies and procedures, incorporating Ministry-specific privacy requirements, have been developed and deployed, where appropriate.								
2. Education and Awareness								
2.1 **Mandatory Employee Training** Employees have completed mandatory training related to privacy (IM117 or equivalent) within an appropriate amount of time and updated periodically.								
2.2 **Role Based Privacy Training** A process is in place to develop and deliver additional privacy training (beyond IM117) to employees.								
3. Privacy Impact Assessments								
3.1 **Process for PIAs** The MPO has developed and communicated Ministry processes for the completion of PIAs within their Ministry, and these are easily accessible by all employees.								
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.								
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								

Privacy								
v# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
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).								
4. Agreements								
4.1 **Completion and updating of ISAs, RAs, CPAs and IPAs** The MPO has a process to identify when ISAs, RAs, CPAs, and IPAs need to be developed and/or updated. This process includes engagement by the MPO as part of the development or updating of the agreement to ensure the agreements are completed as required.								
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.								
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.								
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								

Privacy								
v# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
agreements.								
5. Service Provider Management								
5.1 **Privacy Protection Schedules** Privacy Protection Schedules are included for contracts containing personal information, and the MPO is made aware of all such contracts.								
5.2 **Inventory of Access to Personal Information** The MPO maintains an up to date inventory of service providers or volunteers with access to personal information within the Ministry's custody and control.								
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.								
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).								
6. Personal Information Inventories and Directory								

Privacy								
v# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
6.1 **Create and Maintain Personal Information Inventory** A procedure exists to create and maintain a Personal Information Inventory, and to create it within one year of the Personal Information Inventory Policy being published.								
6.2 **Reporting to CIRMO** A procedure exists for the creation and reporting to CIRMO of Personal Information Banks as required.								
6.3 **Health Information Banks** *For the Ministry of Health:* A procedure exists for the creation and reporting (to CIRMO) of Health Information Banks.								
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.								
7. Foreign Demands for Disclosure								
Reporting Foreign Demands A procedure is in place for reporting foreign demands for disclosure to CIRMO.								
8. Information Incident Management								
8.1 **Information Incident Management** If an information incident occurred in the past 12 months, the incident was reported immediately, all CIRMO instructions were followed and all recommendations were								

Privacy								
v# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
implemented.								

Records Management								
# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
1. Governance and Accountability								
1.1 **Records Management Accountabilities** The Ministry has articulated employees' responsibilities for records management and business areas have clearly assigned accountabilities to employees with additional role specific records management duties, as appropriate. There is a clear understanding of respective roles and responsibilities and the names of such person(s) or group(s) and their responsibilities are communicated to internal personnel.								
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.								
2. Education and Awareness								

Records Management								
# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
2.1 **Mandatory Employee Training** Employees have completed mandatory training related to records management (IM117).								
2.2 **Role Specific Training** Individuals have received additional, role-specific records management training where appropriate.								
3. Classification								
3.1 **Record Classification** The ministry has procedures in place to classify and/or organize records so that the records can be managed according to the function of the information and the approved retention schedules.								
4. Digitization / Documentary Evidence								
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. Retention, Holds and Disposition								
5.1 **Information Schedule Development and Maintenance** The ministry has a process to support and enable the development and implementation of information schedules. The ministry collaborates with GRS to maintain the currency of existing schedules and to develop a procedure to								

Records Management								
# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
identify records that are not covered by approved schedules.								
5.2 **Records Retention, Holds and Disposition** The ministry has procedures to dispose of, transfer, or archive government information based on official policies, specifications, schedules, guidelines, and procedures published by the Government Records Service. In the case of a legal hold or FOI request, the ministry has processes in place to ensure that such records are not destroyed. Where records are scheduled, retention is limited to the scheduled time period and no longer. Unscheduled records are retained.								
6. Archiving / Preservation / Record Transfers								
6.1 **Identify and Protect Digital Records Scheduled for Archiving** The ministry has documented procedures for identifying, protecting, and maintaining the usability and integrity of digital records scheduled for transfer to archives.								
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								

Records Management								
# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
includes procedures to monitor such transfers.								
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.								
7. Records Maintenance and Storage								
7.1 **Manage Information in Recordkeeping Systems** The ministry manages government information through its lifecycle using recordkeeping system(s) as appropriate. Systems are used to meet records management requirements, including schedules as mandated in the IMA.								
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.								
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.								

Information Access								
# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
1. Accountability								
1.1 **Information Access Procedures and the Duty to Assist** Information Access and Duty to Assist procedures have been clearly defined and have been communicated to all staff. Ministry staff are informed and aware of the appropriate response to FOI requests (e.g., how to conduct a comprehensive and timely search for responsive records, seeking clarification, and execute these steps in accordance to defined procedures).								
1.2 **Information Access Accountability** Accountabilities for FOI requests are assigned, and roles and responsibilities are clearly defined.								
2. Education and Awareness								
2.1 **Employee Training** Employees have completed mandatory (IM117) training related to FOI/ Information Access.								
2.2 **Role Specific Training** Individuals have received additional, role-specific FOI/Information Access training where appropriate (e.g. ministerial staff, FOI co-ordinators).								
3. Minister's Offices & Ministerial Staff								

Information Access								
# Criteria	**Summary Response 1**	**Summary Response 2**	**Summary Response 3**	**Summary Response 4**	**Summary Response 5**	**Summary Response 6**	**Summary Response 7**	**Summary Response 8**
3.1 **Dedicated Public Servant** A dedicated Public Servant is designated as the person in charge of all requests involving a Minister's office. This person is accountable for contacting all staff directly, in writing, with the details of the request and directing that staff search for responsive records and respond within a set time period. This individual must also retain a current list of all Ministerial staff that is shared on an ongoing basis with IAO.								
4. Monitoring								
4.1 **Monitoring of FOI Requests** A documented process is in place to track and monitor all active FOI requests. This includes regular reporting to Ministry leadership and escalation processes to ensure compliance with timeliness and/or "duty to assist" requirements.								
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.								

Information Protection								
# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
1. Information Protection								
1.1 **Security Program** An Information Security Program has been developed, documented, approved, and implemented based on the Information Security Policy (ISP) developed by the Office of the Government Chief Information Officer (OCIO) and Corporate Information and Records Management Office (CIRMO) with respect to security of personal information. Responsibilities for the Information Security Program are documented and assigned.								
1.2 **Employee Training** Employees have completed training related to the protection of government information (IM117 and IM118).								
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 access to government information, information systems or information processing facilities are performed and appropriate security controls implemented prior to granting access.								
1.5 **Asset Management** An inventory of information assets and systems exists and is maintained. Ownership of assets is assigned and accountabilities associated with ownership are defined.								

Information Protection								
# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
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.								
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.								
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.								
1.9 **Security Classification** Records are organized so that security classifications can be applied to protect different classes of information based on their sensitivity								
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.								

Information Protection								
# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
1.11 User Access and Responsibilities - Users must only access information permitted by their assigned roles and responsibilities -Users must ensure unattended equipment has appropriate protection. -Users must ensure the safety of sensitive information from unauthorized access, loss or damage.								
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.								
1.13 **Security requirements for information systems** Security controls are identified as part of the business requirements for new information systems or enhancements to existing information systems through the information security risk assessment (the former STRA) process, and controls are implemented								

Information Protection								
# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
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.								
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.								
1.16 **Business Continuity Management** Business continuity management processes and plans have been developed tested, maintained, updated and they include provisions to maintain security and information protection in the case of an incident	.				.			

Information Protection								
# Criteria	Summary Response 1	Summary Response 2	Summary Response 3	Summary Response 4	Summary Response 5	Summary Response 6	Summary Response 7	Summary Response 8
1.17 **Monitoring Service Provider Compliance with Information Protection requirements** The Ministry has a process to monitor service provider compliance for information protection requirements								

Ministry Coordinator - Planning Topics
Discuss IMPR approach (i.e. Review phases, sampling methodology, ministry resource/time commitments, etc.)
Provide newest version of Practice Review Framework
Request ministry org charts
Ask if there are Ministry timing concerns or constraints (i.e. other audits, reviews, ministry initiatives)
Discuss high-level overview of ministry processes and/or ministry risks for each IM domain (i.e. privacy, records, FOI and security)
Obtain ministry-level contact information (i.e. MPO, MISO, FOI Coordinator [i.e. IAO single-point-of-contact] and RO/DGD Champion)

PRIVACY			RECORDS MANAGEMENT	ACCESS TO INFORMATION	INFORMATION PROTECTION		
PCT - Privacy Policy and Training	**PCT - Privacy Operations**	**PCT - Investigation Unit**	**Government Records Services (GRS)**	**Information Access Operations (IAO)**	**Information Security Branch (ISB)**	**IM/IT Policy and Legislation**	
Contact: - First: Rhianna (meet with to collect ministry reports and ask interview questions)	**Contact:** - First: Quinn (meet with to collect ministry reports and ask interview questions)	**Contact:** - First: Quinn (meet with to collect ministry reports and ask interview questions)	**Contact:** - First: Elizabeth Vander Beesen, Director of Information Solutions and Transformation (advise of upcoming review) - Second: ministry GRS RO (meet with to collect ministry reports and ask interview questions)	**Contact:** - First: Kris Ghag, Senior Director (advise of upcoming review) - Second: ministry IAO Manager (meet with to collect ministry reports and ask interview questions)	**Contact:** - First: Don Costello, Director (advise of upcoming review) - Second: AISR lead (Brian Horncastle) and DefSec Lead (Dan Lethigee) (meet with to collect ministry reports and ask interview questions)	**Contact:**	
Meeting Introduction: Provide high-level overview of the IMPR program and what stage the review is in Provide meeting context: collect information to determine which branches will benefit from review, which branches will demonstrate best practices for ministry to leverage, and collect contextual information to review before interviewing employees (i.e. if office completes several PIAs, if office uses TRIM, etc.) Advise that the Ministry Coordinator is aware that IMPR is collecting information to plan review If ministry executive have not yet been briefed, advise contact to not share this interaction with others State we are not looking to evaluate an individual's performance, but rather to gain an understanding of the ministry practices to inform sampling decisions and prepare for interviews Ask that the requested reports be sent to directly to you							
Reports: First, discuss framework criteria and describe the type of information IMPR would find useful Mention previous reports we have received that we found useful: - Privacy policies reviewed by PCT - Role-based privacy training provided by PCT Ask contact if their area can provide any reports or statistics relevant to framework criteria	**Reports:** First, discuss framework criteria and describe the type of information IMPR would find useful Mention previous reports we have received that we found useful: - PIAs completed by ministry - Review PID (completed by IMPR) Ask contact if their area can provide any reports or statistics relevant to framework criteria	**Reports:** First, discuss framework criteria and describe the type of information IMPR would find useful Mention previous reports we have received that we found useful: - Summary of past information incidents Ask contact if their area can provide any reports or statistics relevant to framework criteria	**Reports:** First, discuss framework criteria and describe the type of information IMPR would find useful Mention previous reports we have received that we found useful: - Reports indicating how many boxes are in offsite storage - EDRMS Content Manager report indicating how often electronic records are "offsited" or destroyed (by program area/branch) - EDRMS Content Manager usage report (by program area/branch) over the last two years - Report indicating all approved ORCS schedules, draft schedules, requested schedules/schedules updates, and schedules currently being worked on by GRS Ask contact if their area can provide any reports or statistics relevant to framework criteria	**Reports:** First, discuss framework criteria and describe the type of information IMPR would find useful Mention previous reports we have received that we found useful: - Reports demonstrating how often IAO has provided FOI training to the ministry over the last two years - Stephen Question: can we get some stats to compare ministries or divisions within CITZ? % of process time met? Darlene response: the Weekly Executive Report shows the timeliness for all ministries. Ask contact if their area can provide any reports or statistics relevant to framework criteria	**Reports:** First, discuss framework criteria and describe the type of information IMPR would find useful Mention previous reports we have received that we found useful: - - Ask contact if their area can provide any reports or statistics relevant to framework criteria	**Reports:** First, discuss framework criteria and describe the type of information IMPR would find useful Mention previous reports we have received that we found useful: - - Ask contact if their area can provide any reports or statistics relevant to framework criteria	
Interview Questions (for Review): Instead of asking "what are the positives and negatives" for the ministry, ask contact to describe their interactions with the ministry and their awarness of current projects and initiatives - Are there any large policy initatives being worked on within the ministry? "	**Interview Questions (for Review):** Instead of asking "what are the positives and negatives" for the ministry, ask contact to describe their interactions with the ministry and their awarness of current projects and initiatives - Are any divisions/branches in the midst of completing large PIAs? - -	**Interview Questions (for Review):** Instead of asking "what are the positives and negatives" for the ministry, ask contact to describe their interactions with the ministry and their awarness of current projects and initiatives - - -	**Interview Questions (for Review):** Instead of asking "what are the positives and negatives" for the ministry, ask contact to describe their interactions with the ministry and their awarness of current projects and initiatives - If the ministry is not using EDRMS Content Manager, are you aware of any other system they're using to manage their information? - Have you been involved in any digitization projects within the ministry? - Do you have any records management contacts within the ministry (e.g. DGD champion, ministry RO, divisional RM coordinators, branch records assistants, etc.)	**Interview Questions (for Review):** Instead of asking "what are the positives and negatives" for the ministry, ask contact to describe their interactions with the ministry and their awarness of current projects and initiatives - Which divisions or branches have mature FOI practices? - Any divisions that would regularly need assistance with FOI? - Are there certain FOI processes (e.g., gathering records, approval process, etc.) that IAO often has to prompt or remind the ministry of in order that the ministry's responsibilities are met? - Is there an effective escalation process with the ministry to ensure compliance with timelines, and what does this look like? - In reviewing the current FOI Year to Date Report, what factors do you think contribute to the ministry's on-time percentage?	**Interview Questions (for Review):** Instead of asking "what are the positives and negatives" for the ministry, ask contact to describe their interactions with the ministry and their awarness of current projects and initiatives - Are any branches implementing new systems? - -	**Interview Questions (for Review):** Instead of asking "what are the positives and negatives" for the ministry, ask contact to describe their interactions with the ministry and their awarness of current projects and initiatives - Are there any large policy initatives being worked on within the ministry? - -	

Framework Questions (Develop IMPR Understanding of Criteria): How would IMPR discern if a privacy policy is needed but has not yet been developed? Is there a way for IMPR to review PIAs and previous incident recommendations to determine if a privacy policy is required? When ministrys completed the risk mitigation table in PIAs, are the activities confirmed in any way or followed up on (i.e. if future-state)?	**Framework Questions (Develop IMPR Understanding of Criteria):** When ministrys completed the risk mitigation table in PIAs, are the activities confirmed in any way or followed up on (i.e. if future-state)? How would IMPR know if a PIA was needed but missed (e.g. Holly mentioned she found out about a new initiative via @Work that had not completed necessary PIA)? Retro-active PIAs - how do they typically get identified? If a PIA is retroactive, are these one flagged in any way (i.e. ministrys that commonly miss completing PIAs)? Are there any types of initiatives where PIAs typically get missed? RFL checklist notes PIAs/STRAs as requirements... are there other lists/triggers for ministrys to complete PIA/STRAs? Are there other checklists that it would make sense to get PIA added to? If yes, how can this occur?						

PRIVACY	RECORDS MANAGEMENT	ACCESS TO INFORMATION	INFORMATION PROTECTION	
MPO	**Ministry RO and DGD Champion**	**Ministry FOI Coordinator**	**MISO**	
Meeting Introduction: Provide high-level overview of the IMPR program and what stage the review is in Provide meeting context: collect information to determine which branches will benefit from review, which branches will demonstrate best practices for ministry to leverage, and collect contextual information to review before interviewing employees (i.e. if office completes several PIAs, if office uses TRIM, etc.) Advise that the Ministry Coordinator is aware that IMPR is collecting information to plan review If ministry executive have not yet been briefed, advise contact to not share this interaction with others State we are not looking to evaluate an individual's performance, but rather to gain an understanding of the ministry practices to inform sampling decisions and prepare for interviews Ask that the requested reports be sent to directly to you				
Reports: First, discuss framework criteria and describe the type of information IMPR would find useful Mention previous reports we have received that we found useful: - Privacy policies - Role-based privacy training provided - PIAs completed by ministry Ask contact if their area can provide any reports or statistics relevant to framework criteria	**Reports:** First, discuss framework criteria and describe the type of information IMPR would find useful Mention previous reports we have received that we found useful: - DGD champion: DGD GRS self-assessment results Ask contact if their area can provide any reports or statistics relevant to framework criteria	**Reports:** First, discuss framework criteria and describe the type of information IMPR would find useful Mention previous reports we have received that we found useful: - Ask contact if their area can provide any reports or statistics relevant to framework criteria	**Reports:** First, discuss framework criteria and describe the type of information IMPR would find useful Mention previous reports we have received that we found useful: - Ask contact if their area can provide any reports or statistics relevant to framework criteria	
Interview Questions (for Review): Instead of asking "what are the positives and negatives" for the ministry, ask contact to describe their interactions with the ministry and their awarness of current projects and initiatives - Are there any large policy initatives being worked on within the ministry? - Are any divisions/branches in the midst of completing large PIAs? - Large information incidents	**Interview Questions (for Review):** Instead of asking "what are the positives and negatives" for the ministry, ask contact to describe their interactions with the ministry and their awarness of current projects and initiatives - -	**Interview Questions (for Review):** Instead of asking "what are the positives and negatives" for the ministry, ask contact to describe their interactions with the ministry and their awarness of current projects and initiatives - Are there designated FOI contacts? - Is there a designated person in charge of all FOI requests involving the Minister's office?	**Interview Questions (for Review):** Instead of asking "what are the positives and negatives" for the ministry, ask contact to describe their interactions with the ministry and their awarness of current projects and initiatives -	

Executive Director Questions
Materials to Print for Meeting: - org chart of their area (helpful when selecting staff to interview… spelling names correctly, identifying supervisors and employees, etc.)
General: As you know, we are here to meet with members of your staff about IM practices. Do all your staff work here in this office? Do you have a current ORG chart? Do you have an office manager? Does this person manage the onboarding/offboarding? **Branch Strengths and Areas for Improvement:** Can you give me any examples of best practices within your branch? (i.e. privacy, records management, access to information and information protection)? Are there any areas within your branch that you have concerns with as it relates to IM? **Branch Timing Concerns:** Are there any branch constraints (e.g. other audits/reviews) or employee timing issues (e.g. upcoming vacation) that our team should be aware of?
Privacy and IP: Has your branch completed any PIAs and does your branch regularly connect with the Ministry Privacy Officer or the Privacy, Compliance and Training Branch? Do you have service providers and if you do, do you have someone who manages the contracts for you?
RM and IP: How are records managed in your area (i.e. how are records classified, offsited/destroyed, etc.)? What systems and repositories are utilized by the branch (i.e. paper-based, LAN, TRIM, case management systems, etc.)? Does the branch manage any of these systems (i.e. collect and review audit logs, provide access manually (outside of IDIR), etc.)?
FOI: Do you have an FOI co-ordinator in the branch?
Office Manager IP (Onboarding/Offboarding) Questions: How are employees onboarded/offboarded within the branch (e.g. does the office manager complete all tasks, do supervisors complete tasks, etc.)? How are access controls managed in the branch (e.g. access to/from LAN, branch-specific applications and systems, etc.)? How is asset management conducted for the branch (e.g. who is responsible for issuing and tracking laptops, cell phones, USBs, etc.)? *Our team would like to request branch onboarding/offboarding documentation*
Branch Contacts Please provide the names and roles of employees that our team can meet with (i.e. privacy/records/FOI/security SMEs, contract managers, supervisors and their direct reports [if possible, junior and senior employees]) If applicable, please provide names of employees from different offices and/or physical locations.

Manager/Employee PreInterview Information
* Provide this information in a separate email to interview; do not include within the outlook meeting invite * Subject Line for Pre-Interview Email: *Division-Branch* Information Management Practice Review Meeting **Information to Copy into Email:** Hi xxxx, Our team, the Information Management Practice Review (IMPR) Program, is currently conducting an IM Practice Review for the Ministry of Citizens' Services (CITZ). We are meeting CITZ employees to determine the ministry's maturity with respect to its IM practices (i.e. privacy, records management, access to information and information protection). Your name has been provided to us by your executive director as you are a current xxxx within the branch. Our team would like to set up a meeting with you to ask a series of questions regarding your daily IM practices. In addition to asking questions, our team will request documentation that demonstrates how these practices are conducted. Documents do not need to be provided in the meeting; our team will request the documents via email after the meeting has concluded. To prepare for the meeting, please begin to think about your daily practices with respect to: * Privacy (e.g. do you complete PIAs? do you complete agreements? do you manage contracts? have you ever reported an information incident?) * Records Management (RM) (e.g. who is responsable for records management in your office? are there any branch-specific or corporate RM materials you reference? have you recieved any specialized RM training (e.g. TRIM)? do you classify records? what systems are used to maintain your records (e.g. LAN, TRIM, case management system, etc.)? * Access to Information (e.g. have you ever been involved in an FOI request?) * Information Protection (e.g. do you download applications or software to your work desktop or phone? how do you protect sensitive data in your workplace (e.g. passwords, locked cabinets, etc.)? do you use portable media?) Our team would like to meet with you during the week of: xxxx xx to xxxx xx. Please book an available room for one hour in your building for this meeting. Two IMPR team members will attend the meeting. Please also advise our team of any special security arrangements for your builing (e.g. sign in at reception on first level, security desk on second level, etc.). If you have any questions about the meeting or are not available during the requested week, please let me know and we can determine a new meeting time. Thanks!

Hi **[name]**,

As you may know, we are starting the first Ministry wide review of IM practices. As the **[Role]** for **[Division]**, we'd like to meet with you. There is a deck attached for your information, but the intention of this brief meeting (45 mins at most) is to introduce our team and ask you some questions specific to your role.

We have clear calendars and would be happy to meet with you at your office and at your convenience.

Can I ask you to send a meeting request to us at whatever time/date suits you best? Later this week or early next would be great.

Cheers and thanks,

Manager/Employee PreInterview Information
* Subject Line for Post-Interview Email: Information Management Practice Review Meeting - *Division-Branch* Document Request **<u>Information to Copy into Email:</u>** Hi xxxx, Thank you for taking the time to meet with our team. Included below is list of documents our team requested during the meeting: 1) 2) 3) 4) 5) Please feel free to provide any additional documents or materials that were not discussed during the meeting. If you are able to, please provide the documents by XXXX XX. If you have any additional information you would like to provide or have remaining questions you would like to ask, please feel free to respond to this email, call one of our IMPR team members, or organize another meeting.

Privacy							
#	Criteria	3 - Defined	4 - Managed	MPO Questions	Manager Questions	Staff Questions	IMPR Notes
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.	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.	Have your responsibilities as MPO been documented? Is the performance of your MPO duties monitored in any way (e.g. DM, supervisor)?	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	
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.	The MPO maintains and monitors all Ministry FOIPPA Delegation Instruments.	Has the Deputy Minister delegated any privacy duties, powers, or functions to you or other roles within the ministry? If yes, was a FOIPPA Delegation Instrument been used and was it communicated to CIRMO?	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	
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.	The MPO monitors all delegated duties, powers and functions.	Have you, as an MPO, delegated any duties to others, and if so, has it been documented? How do you monitor the duties and functions of the powers that you have delegated?	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	
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.	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).	Has the ministry developed or updated any ministry-specific privacy policies or procedures (beyond PMAP)? (E.g. CITZ - IDIM Identity Program, s.13: s.13: s.15 ENV - Use of Drones) If yes, have the policy/procedures or changes been reviewed by CIRMO (i.e. PCT)? If yes, how are the policies and procedures communicated to your staff?	Does your division/branch have its own privacy policy or procedures (beyond PMAP)? (E.g. CITZ - IDIM Identity Program, s.13: s.13: s.15 ENV - Use of Drones) If yes, have the policy or procedures been communicated to the appropriate staff?	Are you aware of any ministry-specific privacy policies or procedures (beyond PMAP)? (E.g. CITZ - IDIM Identity Program, s.13: s.13: s.15 ENV - Use of Drones)	
2. Education and Awareness							

Privacy							
#	Criteria	3 - Defined	4 - Managed	MPO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability							
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.	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.	Do you track IM 117 completion when new versions of the training are developed/offered by CIRMO? Are there any types of privacy awareness activities (e.g., emails, posters, presentations, etc.) conducted for the ministry? If yes, does a privacy awareness and training program exist for the ministry?	How do you ensure new employees receive IM 117 training when they are hired? Are there any types of privacy awareness activities (e.g., emails, posters, presentations, etc.) conducted for the ministry or your division/branch? Does a privacy awareness and training program exist for your division/branch?	When you were onboarded to your current branch, were you required to take the IM 117 course? Have you taken the most recent version of IM 117 (requirement announced April 2019, deadline is July 15, 2019)? Are there any types of privacy awareness activities (e.g., emails, posters, presentations, etc.) conducted for your ministry or your division/branch?	
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.	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.	How do you identify employees who require additional privacy training (beyond IM117)? E.g. privacy training to support employees using information systems and programs that involve the handling of high-risk or sensitive personal information within their Ministry. Have you developed any ministry role-based privacy training in consultation with CIRMO? Is training delivered in a timely manner (i.e. 6 months) and are results tracked?	How do you identify employees who require additional privacy training (beyond IM117)? E.g. privacy training to support employees using information systems and programs that involve the handling of high-risk or sensitive personal information within their Ministry. What type of additional training is provided? How often is the training provided?	Have you received additional information privacy training (beyond IM117)? E.g. privacy training to support employees using information systems and programs that involve the handling of high-risk or sensitive personal information within their Ministry.	
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.	The MPO monitors the compliance with internal processes to ensure the completion of PIAs.	What is your process for tracking PIA completion? How do you keep track of outstanding items that require follow-up?	Have you ever done a Privacy Impact Assessment? Are you familiar with the PIA process?	Have you ever done a Privacy Impact Assessment? Are you familiar with the PIA process?	

Privacy							
#	Criteria	3 - Defined	4 - Managed	MPO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability							
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.	The MPO monitors the compliance with policies and procedures to ensure the completion of PIAs in a timely manner.	What processes or procedures do you have in place to ensure that the ministry's PIAs are conducted in a timely manner? How do you support ministry employees in the development and completion of PIAs? What kind of guidance do you provide to employees who complete PIAs to ensure that the completed and signed PIAs are submitted to CIRMO? Do you monitor this process?	Has your branch conducted PIAs? Do you know when a PIA is to be conducted? Is there a PIA process you follow, which includes providing the PIA to your MPO before it's submitted to CIRMO? Once the PIA is reviewed by CIRMO, did you ensure that their input was incorporated into the PIA and is signed by all required parties and the PID is updated?	Have you conducted Privacy Impact Assessments (PIAs)? Do you know when you should conduct PIAs? Is there a PIA process you follow, which includes providing the PIA to your MPO before it's submitted to CIRMO? Once the PIA is reviewed by CIRMO, did you ensure that their input was incorporated into the PIA and is signed by all required parties and the PID is updated?	
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.	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.	Do you have a process to identify when ISAs, RAs, CPAs and IPAs are required? Are you consulted during the development and/or updating of these agreements? Are there templates for the development of these agreements? Are you actively involved with Ministry staff to keep them informed about the process relating to agreements?	Have your area ever created ISAs, RAs, CPAs and IPAs? Do you consult with the MPO when an agreement is required?	Have your area ever created ISAs, RAs, CPAs and IPAs? Do you consult with the MPO when an agreement is required?	
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.	The MPO monitors the process to ensure the ISAs are reported to CIRMO.	Do you have a process to ensure all the ISAs are reported to CIRMO for entry into the PID?	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	
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.	The MPO monitors the RAs tracking process and ensures outstanding items are followed up in a timely manner.	Do you have an inventory of all research agreements entered into by the ministry? How do you follow up on outstanding items?	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	
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.	Through review of prior agreements, the MPO assess the effectiveness of the monitoring process.	Do you monitor counterparty compliance within agreements and how do you address issues of non-compliance?	If you have an agreement, is there a process for monitoring counterparty compliance with privacy requirements? Is there a path for escalation or corrective measures built into the agreement?	NA This question does not need to be asked of ministry employees. The MPO and manager response is adequate.	
5. Service Provider Management							

Privacy							
#	Criteria	3 - Defined	4 - Managed	MPO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability							
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.	There is a monitoring process for contracts that involve personal information to ensure that Privacy Protection Schedules are included and accurate.	NA This question does not need to be asked of the MPO. Manager responses are adequate.	Does your branch manage contracts that involve personal information? Is the General Service Agreement (GSA) template used to ensure that a PPS is included and completed? If no, how do you ensure PPSs are included in each contract? What is the process if the PPS needs to be amended? Is there a process to monitor your contracts to ensure that PPSs are included and accurate?	NA This question does not need to be asked of ministry employees. Manager responses are adequate.	
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.	There is a monitoring of the process for informing the MPO of service providers and volunteers who have access to personal information.	Do you have an inventory of your service providers and/or volunteers with access to personal information? How do you keep the inventory up to date?	Do you inform the MPO of any service provider or volunteer that has access to personal information? Do you regularly review and update the list of service providers and volunteers with access to PI?	NA This question does not need to be asked of ministry employees. The MPO and manager response is adequate.	
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.	Training for service providers and volunteers is documented, scheduled, timely, consistent and is augmented by regular awareness activities (e.g. emails, posters, presentations, etc.).	Do you have a process to confirm that service providers and volunteers have received the appropriate training prior to providing services? Do you provide any additional privacy awareness activities for service providers (e.g. regular emails, etc.)?	If you have service providers who have access to PI, how do you ensure they receive the appropriate training before providing services? Do you provide any additional privacy awareness activities for service providers (e.g. regular emails, etc.)?	NA This question does not need to be asked of ministry employees. The MPO and manager response is adequate.	
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.	There is a monitoring process for ensuring service provider compliance with Privacy Protection Schedules.	NA This question does not need to be asked of the MPO. The manager responses is adequate.	Do you have a role in managing service provider contracts? If yes, is there a process in place to monitor service provider compliance with the contract's privacy requirements (e.g. ensure appropriate collection, storage, protection, retention, use and disclosure of personal information)? If yes, is there a process in place to manage issues of non-compliance?	NA This question does not need to be asked of ministry employees. The manager response is adequate.	
6. Personal Information Inventories and Directory							

Privacy							
#	Criteria	3 - Defined	4 - Managed	MPO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability							
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.	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.	NA The PII does not yet exist.	NA The PII does not yet exist.	NA The PII does not yet exist.	
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.	The MPO monitors the process for creating and reporting PIBs to CIRMO.	What process do you have in place for reporting all ministry PIBs to CIRMO? Is this process monitored?	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	
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.	The MPO monitors the process for creating and reporting HIBs to CIRMO.	Health MPO Only: Is there a process in place on how to create and report all HIBs to CIRMO?	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	
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.	Through review of PID, the MPO assesses the effectiveness of the monitoring process.	Is there a process to monitor the Personal Information Directory to ensure that PIAs, ISAs, PIBs and, where applicable, HIBs are entered correctly? Do you monitor the PID for currency of the entries?	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	
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.	A Ministry-wide awareness and training program exists for reporting all foreign demands for disclosure to CIRMO.	Have you ever received a foreign demand (i.e. an order, demand or request from an authority outside of Canada for the unauthorized disclosure of personal information)? If yes, what process did you follow to report the foreign demand?	Have you ever received a foreign demand (i.e. an order, demand or request from an authority outside of Canada for the unauthorized disclosure of personal information)? If yes, what process did you follow to report the foreign demand?	Have you ever received a foreign demand (i.e. an order, demand or request from an authority outside of Canada for the unauthorized disclosure of personal information)? If yes, what process did you follow to report the foreign demand?	
8. Information Incident Management							

Privacy							
#	Criteria	3 - Defined	4 - Managed	MPO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability							
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.	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.	What is your process for tracking and following up on information incidents that you have been involved in? How does the ministry train and generate awareness on how to recognize and report information incidents? If employees are involved in incident response processes, how are they trained? Is the training monitored?	Can you please describe what an information incident is? How would you report this type of incident? How does the ministry train and generate awareness on how to recognize and report information incidents? Do you have employees that are involved in incident response processes? If yes, how are they trained? Is the training monitored?	Can you please describe what an information incident is? How would you report this type of incident? What types of training and awareness activities have you been provided for recognizing and reporting information incidents?	
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.	The Ministry tracks key information about information incidents and has developed incident response plans specific to their business context. The Ministry monitors its incident reporting and processes, analyzes trends and root causes, and identifies remediation steps as required.	How do you track information incidents and their resolution? Has the ministry developed incident response plans? Does the ministry monitor its information incidents in order to analyze trends and root causes to then identify remediation steps?	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	NA This question does not need to be asked of ministry employees. The MPO response is adequate.	

Records Management								
#	Criteria	3 - Defined	4 - Managed	DGD Champion Questions	Ministry RO Questions	Manager Questions	Staff Questions	IMPR Notes
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.	Management regularly reviews the ministry's records management program, seeks ways to improve the program's performance, including appropriate and adequate resources.	What are your responsibilities in regards to DGD? Have you delegated any of your DGD responsibilities or know of divisional RM contacts? If yes, what are the contact names? How are DGD responsibilities communicated to staff? Do you work on any projects with GRS? How do you ensure that decisions in your area are documented appropriately?	What are your responsibilities in regards to records within the ministry? Have you delegated any of your RO responsibilities or know of divisional RM contacts? If yes, what are the contact names? How are records responsibilities communicated to staff? Do you work on any projects with GRS? How do you ensure that decisions in your area are documented appropriately?	What are your responsibilities in regards to records for the branch? Have you delegated any RM responsibilities to branch staff? If yes, who? How are records responsibilities communicated to staff? Do you work on any projects with GRS? Do you think all of the important decisions in your office are documented? Please explain. How do you ensure that decisions in your area are documented appropriately?	What are your responsibilities in regards to records management? If you have any questions about RM, who do you ask – is there a dedicated RM person? If yes, who? How are records responsibilities communicated to you? Do you work on any projects with GRS? How do you ensure that decisions in your area are documented appropriately?	
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 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.	Have the DGD guideline and directive been formally shared with the ministry? Have the requirements of DGD been communicated across the ministry? Are there plans in place for future communications and/or projects related to DGD for the ministry?	Do you know of, or have you utilized, Government Records Services? Does the ministry have any Ministry-specific RM policies or procedures? Have you received any communications about DGD? What is your understanding of DGD?	Do you know of, or have you utilized, Government Records Services? Does your branch have any branch-specific RM policies or procedures? Have you received any communications about DGD? What is your understanding of DGD?	Do you know of, or have you utilized, Government Records Services? Does your branch have any branch-specific RM policies or procedures? Have you received any communications about DGD? What is your understanding of DGD?	
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.	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.	NA This question is addressed by privacy criteria 2.1 IM 117 training and statistics are monitored by the MPO The maturity value provided in privacy for IM 117 will be carried over into the RM, Access and IP domains	NA This question is addressed by privacy criteria 2.1 IM 117 training and statistics are monitored by the MPO The maturity value provided in privacy for IM 117 will be carried over into the RM, Access and IP domains	NA This question is addressed by privacy criteria 2.1 IM 117 training and statistics are monitored by the MPO The maturity value provided in privacy for IM 117 will be carried over into the RM, Access and IP domains	NA This question is addressed by privacy criteria 2.1 IM 117 training and statistics are monitored by the MPO The maturity value provided in privacy for IM 117 will be carried over into the RM, Access and IP domains	

Records Management								
#	Criteria	3 - Defined	4 - Managed	DGD Champion Questions	Ministry RO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability								
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 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.	What training on DGD has been provided to the ministry? Is there a ministry-wide records management training and awareness program?	How are employees who require additional records management training (beyond IM117) identified? Has the ministry developed any role-based records management training? What is the process to identify the need for and development of ministry role-based records management training? Have you received any training on DGD? Is there a ministry-wide records management training and awareness program?	How are employees who require additional records management training (beyond IM117) identified? What type of additional training is provided? How often is the training provided? Have you received any training on DGD?	Have you received additional records management training (beyond IM117)? Have you received any training on DGD?	
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.	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.	NA This question does not need to be asked of DGD champion The ministry RO, manager and employee responses are adequate.	What is your role in supporting the classification efforts within the ministry? How are the ministry's records organized and managed? Are the majority of records classified (i.e. ARCS and ORCS)? What kinds of communication regarding records classification are provided to the ministry? Do you monitor compliance with records classification requirements?	Are the records in your office classified (i.e. ARCS and ORCS)? If yes, have you documented the process used to classify records? Who is responsible for classifying the records? If records are not classified, how do you file them? If no appropriate classifications exist, what is the current process for maintaining those records? Do you monitor compliance with records classification requirements?	Are the records in your office classified (i.e. ARCS and ORCS? Who is responsible for classifying the records? If records are classified, are the procedures for classifying the records documented? If records are not classified, what are the possible reasons for no classification? If no appropriate classifications exist, what is the current process for maintaining those records?	TW note: Potentially change staff question to read: How are your records organized and managed? Are the records in your office classified (i.e. ARCS and ORCS?) Who is responsible for classifying the records and are procedures documented? If records are not classified, why is that?

Records Management								
#	Criteria	3 - Defined	4 - Managed	DGD Champion Questions	Ministry RO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability								
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.	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.	NA This question does not need to be asked of DGD champion The ministry RO, manager and employee responses are adequate.	What is your role in information schedule development and maintenance for the ministry? Does the ministry have up-to-date ORCS schedules? If yes, has the ORCS schedule been applied to all records in offsite storage, onsite physical and electronic records? If yes, is there a process in place to review and update the existing schedules? If no, is there a process in place to obtain schedules? How do you identify records that do not have schedules? How does the Ministry monitor the information schedule development and maintenance process? When required, are changes and improvements made in a timely manner?	Does your office have an up-to-date ORCS schedule? If yes, has the ORCS schedule been applied to all records in offsite storage, onsite physical and electronic records? If yes, is there a process in place to review and update the existing schedule? If no, is there a process in place to obtain a schedule? TW Note: delete next question - this criterion is about schedules, not classification. We asked it above. How do you store records that do not have an appropriate classifications? TW Note: Do schedules change? Also, I think this could be combined with question 4 above. When required, are changes and improvements made in a timely manner?	APPLICABILITY OF THESE QUESTIONS IS DETERMINED BY THE RESPONSES FOR RM CRITERIA 3.2 - JN Note - should this read 3.1? If you classify records, how do you store records that do not have an appropriate classification TW Note - change to: How do you store records that do not have an appropriate classification? If your office requires a new classification, what is the process to obtain one?	
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 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.	Are you aware of any previous or current digitization projects in the ministry? If yes, do you have a role in the project?	Are you aware of any previous or current digitization projects in the ministry? If yes, do you have a role in the project?	Are you aware of any previous or current digitization projects in the ministry? If yes, do you have a role in the project? Do you manage your records physically, electronically or a combination of the two?+G13:G16	Are you aware of any previous or current digitization projects in the ministry? If yes, do you have a role in the project? Do you manage your records physically, electronically or a combination of the two?	JN Note: The “digitization” requirements in section 9 of the IMA are not yet in force. When they are in force, they will be prospective only, meaning that they will apply only to records created after that future date.

Records Management								
#	Criteria	3 - Defined	4 - Managed	DGD Champion Questions	Ministry RO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability								
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.	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.	NA This question does not need to be asked of DGD champion The ministry RO, manager and employee responses are adequate.	Are you aware of the major systems used to store digital records within the ministry? Have the records within these systems been classified using ARCS or ORCS (i.e. assigned a retention which indicated the records are being sent to archives or destroyed)? Can records eligible for archiving be exported from the systems?	What systems are used to store digital records within the branch? Have the records within these systems been classified using ARCS or ORCS (i.e. assigned a retention which indicated the records are being sent to archives or destroyed)? TW Note: All the records must be scheduled for archiving, correct? If scheduled for destruction, would they still go to archives first? Can records eligible for archiving be exported from the systems?	What systems are used to store digital records within the branch? Have the records within these systems been classified using ARCS or ORCS (i.e. assigned a retention which indicated the records are being sent to archives or destroyed)? Can records eligible for archiving be exported from the systems?	
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.	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.	NA This question does not need to be asked of DGD champion The ministry RO, manager and employee responses are adequate.	What is your role in regards to offsiting/destruction processes within the ministry? For your scheduled records, do you retain, archive, transfer and/or destroy them according to the schedules assigned by GRS? Do you have records that are not scheduled and if so have you requested schedules? Are you aware that all unscheduled records must be retained? What processes are in place to ensure that records subject to a legal hold or FOI request are not destroyed? Assuming your records are properly scheduled, do you monitor your schedules for accuracy?	What is your role in regards to offsiting/destruction processes within the branch? For your scheduled records, do you retain, archive, transfer and/or destroy them according to the schedules assigned by GRS? Do you have records that are not scheduled and if so have you requested schedules? Are you aware that all unscheduled records must be retained? What processes are in place to ensure that records subject to a legal hold or FOI request are not destroyed? Assuming your records are properly scheduled, do you monitor your schedules for accuracy?	What is your role in regards to offsiting/destruction processes within the branch?	Does your office have an up-to-date ORCS schedule? If yes, has the ORCS schedule been applied to all records in offsite storage, onsite physical and electronic records? If yes, is there a process in place to review and update the existing schedule? If no, is there a process in place to obtain a schedule? How do you store records that do not have an appropriate classifications? When required, are changes and improvements made in a timely manner? +I16

Records Management								
#	Criteria	3 - Defined	4 - Managed	DGD Champion Questions	Ministry RO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability								
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.	Monitoring of all transfers has been implemented, and where issues are encountered they are remediated.	NA This question does not need to be asked of DGD champion. The ministry RO and manager and responses are adequate.	Are you aware of instances in the ministry where offices (program areas) or records are transferred to another ministry (e.g. re-organization)? If so, what processes are followed with respect to records? If yes, who is responsible for contacting GRS to request that records in these program areas, both offsite and electronic (e.g. TRIM, CRMS), are updated to reflect the new ministry name that now has responsibility? Do you monitor the transfers (e.g. via requested reports from GRS or other methods) to ensure these records are associated with the ministry to which they belong?	Are you aware of instances in the ministry where offices (program areas) or records are transferred to another ministry (e.g. re-organization)? If so, what processes are followed with respect to records? If yes, who is responsible for contacting GRS to request that records in these program areas, both offsite and electronic (e.g. TRIM, CRMS), are updated to reflect the new ministry name that now has responsibility? Do you monitor the transfers (e.g. via requested reports from GRS or other methods) to ensure these records are associated with the ministry to which they belong?	Are you aware of instances in the ministry where offices (program areas) or records are transferred to another ministry (e.g. re-organization)? If so, what processes are followed with respect to records? If yes, who is responsible for contacting GRS to request that records in these program areas, both offsite and electronic (e.g. TRIM, CRMS), are updated to reflect the new ministry name that now has responsibility? Do you monitor the transfers (e.g. via requested reports from GRS or other methods) to ensure these records are associated with the ministry to which they belong?	
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.	There is a process in place to monitor transfers to non-IMA bodies and any incidents of non-compliance are remediated.	NA This question does not need to be asked of DGD champion The ministry RO, manager and employee responses are adequate.	Are you aware of instances in the ministry where offices or records are transferred from government to an outside agency? If yes, what processes are in place to update records when offices or records are transferred outside of Government? NOTE: legal instrument includes a contract, records schedule or legislation If yes, who is responsible for connecting with GRS to ensure all offsite and appropriate electronic (e.g. TRIM, CRMS) records are updated?	Are you aware of instances in the ministry where offices or records are transferred from government to an outside agency? If yes, what processes are in place to update records when offices or records are transferred outside of Government? NOTE: legal instrument includes a contract, records schedule or legislation If yes, who is responsible for connecting with GRS to ensure all offsite and appropriate electronic (e.g. TRIM, CRMS) records are updated?	Are you aware of instances in the ministry where offices or records are transferred from government to an outside agency? If yes, what processes are in place to update records when offices or records are transferred outside of Government? NOTE: legal instrument includes a contract, records schedule or legislation If yes, who is responsible for connecting with GRS to ensure all offsite and appropriate electronic (e.g. TRIM, CRMS) records are updated?	

Records Management								
#	Criteria	3 - Defined	4 - Managed	DGD Champion Questions	Ministry RO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability								
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.	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.	NA This question does not need to be asked of DGD champion The ministry RO, manager and employee responses are adequate.	How are physical records managed in the ministry? Are you aware of any issues the ministry has had with storage facilities (e.g. lost boxes, breaches, etc.)? Who is responsible for managing the offsite records (e.g. ensuring access lists are up-to-date)?	Who is responsible for protecting the onsite physical records (e.g. securing sensitive files)? Are you aware of any issues the ministry has had with storage facilities (e.g. lost boxes, breaches, etc.)? Who is responsible for managing the offsite records (e.g. ensuring access lists are up-to-date)?	APPLICABILITY OF THESE QUESTIONS IS DETERMINED BY THE RESPONSES FOR RM CRITERIA 5.1 If the office has onsite/offsite physical records... Who is responsible for protecting the onsite physical records (e.g. securing sensitive files)? Who is responsible for managing the offsite records (e.g. ensuring access lists are up-to-date)? Are you aware of any issues the ministry has had with storage facilities (e.g. lost boxes, breaches, etc.)?	
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.	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.	What is your role in establishing and/or communicating procedures for managing information appropriately in recordkeeping systems to the ministry? Are you aware of any projects to review Ministry alignment with the appropriate recordkeeping system requirement? Are you aware of any projects to review Ministry alignment with the documenting government decisions requirement?	Can you describe your current knowledge of the recordkeeping systems in place for the ministry (e.g. TRIM, CRMS, classified LANs, case management systems, etc.)? What is your role in establishing and/or communicating procedures for managing information appropriately in recordkeeping systems to the ministry? Are you aware of any projects to review Ministry alignment with the appropriate recordkeeping system requirement? Are you aware of any projects to review Ministry alignment with the documenting government decisions requirement?	Can you describe your current knowledge of the recordkeeping systems in place for the branch (e.g. TRIM, CRMS, classified LANs, case management systems, etc.)? What is your role in establishing and/or communicating procedures for managing information appropriately in recordkeeping systems to the division/branch? Are there any projects to review branch alignment with the appropriate recordkeeping system requirement? Are there any projects to review branch alignment with the documenting government decisions requirement?	Can you describe your current knowledge of the recordkeeping systems in place for the branch (e.g. TRIM, CRMS, classified LANs, case management systems, etc.)? Have you received any direction regarding the requirement to manage information appropriately in recordkeeping systems? Are there any projects to review branch alignment with the appropriate recordkeeping system requirement? Are there any projects to review branch alignment with the documenting government decisions requirement?	

Records Management								
#	Criteria	3 - Defined	4 - Managed	DGD Champion Questions	Ministry RO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability								
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.	The inventory process is regularly monitored and exceptions are identified and updated in the inventory on an ongoing basis, where required.	Are you aware of any ministry efforts to establish and maintain an inventory of ministry systems and repositories that manage and/or store government information?	Are you aware of any ministry efforts to establish and maintain an inventory of ministry systems and repositories that manage and/or store government information? Do you monitor the inventory for accuracy and make changes as required?	Are you aware of any branch efforts to establish and maintain an inventory of branch systems and repositories that manage and/or store government information?	NA This question does not need to be asked of ministry employees The ministry DGD champion, ministry RO, and manager responses are adequate.	THIS QUESTION SHOULD ALSO BE ASKED OF MISO OCIO? MCIO? Who would maintain this? CPPM 12.3.6.3 - Information and technology assets must be classified, inventoried and recorded with an identified officer who is responsible for achieving and maintaining appropriate protection of those assets. CPPM 12.3.5.d.1 - Ministries, in conjunction with Workplace Technology Services, must establish and maintain inventories of computer hardware, software and related communications equipment.

Access to Information								
#	Criteria	3 - Defined	4 - Managed	Ministry FOI Coordinator Questions	Manager Questions	Staff Questions	IMPR Notes
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.	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.	What is your role within the ministry with respect to processing FOI requests? Are there documented processes for employees to follow with regard to responding adequately and in a timely manner to FOI requests? If yes, how often do you review these processes and procedures and update them as required? Do you monitor the compliance with these processes and procedures? Are FOI accountabilities within the ministry regularly reviewed or updated?	How are FOI requests handled in your branch? Are there documented processes to follow when conducting searches for FOI requests? How do you ensure you've conducted an adequate search for responsive records? Do you monitor the compliance of these processes and procedures?	How are FOI requests handled in your branch? Are there documented processes to follow when conducting searches for FOI requests? How do you ensure you've conducted an adequate search for responsive records?	
1.2	**Information Access Accountability** Accountabilities for FOI requests are assigned, and roles and responsibilities are clearly defined.	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.	NA This criteria is addressed by FOI criteria 1.1	NA This criteria is addressed by FOI criteria 1.1	NA This criteria is addressed by FOI criteria 1.1	
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.	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.	NA This question is addressed by privacy criteria 2.1 IM 117 training and statistics are monitored by the MPO The maturity value provided in privacy for IM 117 will be carried over into the RM, Access and IP domains	NA This question is addressed by privacy criteria 2.1 IM 117 training and statistics are monitored by the MPO The maturity value provided in privacy for IM 117 will be carried over into the RM, Access and IP domains	NA This question is addressed by privacy criteria 2.1 IM 117 training and statistics are monitored by the MPO The maturity value provided in privacy for IM 117 will be carried over into the RM, Access and IP domains	

Access to Information							
#	Criteria	3 - Defined	4 - Managed	Ministry FOI Coordinator Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability							
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.	A Ministry-wide FOI awareness and training program, including any additional or role-based training, exists and is monitored.	How are employees who require additional FOI training (beyond IM117) identified (e.g. ministerial employees, FOI co-ordinators)? Have you developed any ministry role-based FOI training? What is the process to identify the need for and development of ministry role-based FOI training? Is there a ministry-wide FOI training and awareness program?	How are employees who require additional FOI training (beyond IM117) identified (e.g. FOI co-ordinators)? What type of additional training is provided? How often is the training provided?	Have you received additional FOI training (beyond IM117)?	
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.	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.	Which ministry role has been designated as the central contact for all FOI requests involving a Minister's office? Have the responsibilities for this role been formally defined and documented? Are accountabilities for this role reviewed on a regular basis and updated as required?	NA if the employee is not the ministry's designated employee. The FOI coordinator and manager response is adequate. If the employee is the ministry's designated employee. ask manager questions.	NA if the employee is not the ministry's designated employee. The FOI coordinator and manager response is adequate. If the employee is the ministry's designated employee. ask manager questions.	
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".	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.	What processes are in place to track and regularly monitor all active FOI requests for the ministry and their service providers? What is the escalation process if there is a risk of non-compliance with timeliness and/or duty to assist? Is there regular reporting on FOI requests to Ministry leadership? How are ministry and service provider issues identified and addressed proactively to support completion of requests within the allotted timeframe?	What processes are in place to track and regularly monitor all active FOI requests for the branch and their service providers? What is the escalation process if there is a risk of non-compliance with timeliness and/or duty to assist? Is there regular reporting on FOI requests to Ministry leadership? How are ministry and service provider issues identified and addressed proactively to support completion of requests within the allotted timeframe?	NA if the employee is not involved in the monitoring of FOI requests. The FOI coordinator and manager response is adequate. If the employee is responsible for managing FOI requests, ask manager questions.	

Access to Information							
#	Criteria	3 - Defined	4 - Managed	Ministry FOI Coordinator Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability							

Information Protection							
#	Criteria	3 - Defined	4 - Managed	MISO Questions	Manager Questions	Staff Questions	IMPR Notes
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.	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.	Does the ministry have a documented Information Security Program? If yes, are responsibilities for the program documented and assigned? (Relationship between OCIO and IMB) If yes, how often do you monitor the effectiveness of your Information Security Program?	NA This question does not need to be asked of managers. The MISO response is adequate.	NA This question does not need to be asked of ministry employees. The MISO response is adequate.	
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.	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.	NA This question does not need to be asked of the MISO. Manager response is adequate.	How do you inform employees of their responsibilities as users to protect sensitive information (e.g. clean desk policy, protecting unattended equipment, access to government information, etc.)? Is there a process to verify that employees acknowledge their information security responsibilities? Do you regularly review information security accountabilities and update them with program changes?	How are you informed of your responsibilities to protect sensitive information (e.g. clean desk policy, protecting unattended equipment, access to government information, etc.)?	Manager question suggestion from Stephen: do you have policy on travelling outside the country with laptop or phone? OCIO has policy; special laptop required for travel s.13
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.	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.	NA This question is addressed by privacy criteria 2.1 IM 117 training and statistics are monitored by the MPO The maturity value provided in privacy for IM 117 will be carried over into the RM, Access and IP domains	NA This question is addressed by privacy criteria 2.1 IM 117 training and statistics are monitored by the MPO The maturity value provided in privacy for IM 117 will be carried over into the RM, Access and IP domains	NA This question is addressed by privacy criteria 2.1 IM 117 training and statistics are monitored by the MPO The maturity value provided in privacy for IM 117 will be carried over into the RM, Access and IP domains	

Information Protection							
#	Criteria	3 - Defined	4 - Managed	MISO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability							
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.	A Ministry-wide information security awareness and training program, including any additional or role-based training, exists and is monitored.	How are employees who require additional information security training (beyond IM117 and IM 118) identified? Have you developed any ministry role-based security training (e.g. security training to support employees using information systems and programs that involve the handling of high-risk or sensitive information within their Ministry)? What is the process to identify the need for and development of ministry role-based security training? Is there a ministry-wide information security training and awareness program?	How are employees who require additional information security training (beyond IM117 and IM 118) identified? What type of additional training is provided? How often is the training provided?	Have you received additional information security training (beyond IM117 and IM 118)?	
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 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.	Risks associated with third-party access are monitored and reported on regularly. Controls are updated to reflect changes to risks on an ongoing basis.	What is the ministry's process for providing external party access? How does the ministry ensure that security controls are implemented consistently and in all cases prior to granting access? How are risks associated with third-party access monitored? Are controls updated to reflect changes to risks on an ongoing basis?	Do you manage contracts? If yes, does the branch currently have contractors who have access to your information systems? If yes, what is the risk assessment process for identifying, assessing, mitigating and managing the risks of external party access to information and information systems? (E.g. IDIR for contractor, HR background checks, procurement clauses (employee requirements for system use, appropriate/timely training), etc.) How are risks associated with third-party access monitored? Are controls updated to reflect changes to risks on an ongoing basis?	NA if the employee is not a contract manager. The manager response is adequate. If the employee is a contract manager, ask manager questions.	It is a procurement process to assess external party risk There is no single assessment tool government uses to grant access; system owner (DM, ADM, or ED; typically ED) grants access EDs should have risk assessment process (e.g. IDIR for contractor, HR background checks, procurement clauses (employee requirements for system use, appropriate/timely training), etc.)

Information Protection							
#	Criteria	3 - Defined	4 - Managed	MISO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability							
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.	The ministry monitors service provider compliance with information security requirements. Corrective actions are addressed with service providers and remediated.	Do you have a role in monitoring service provider compliance with information security requirements within contracts? If yes, are there provisions to deal with compliance to the requirements? How does the ministry address corrective actions with service providers?	If yes to 3.1 (contract manager): What is the branch's process for monitoring service provider compliance with information security requirements within contracts? Are there provisions to deal with compliance to the requirements? How does the branch address corrective actions with service providers?	NA if the employee is not a contract manager. The MISO and manager response is adequate. If the employee is a contract manager, ask manager questions.	
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.	Data security classification processes and ratings are regularly reviewed and updated.	Does the ministry have procedures to apply security classifications to information? If yes, how are the appropriate requirements applied? (i.e. it is MISO or branch-level responsibility)? If no, are there plans to apply security classifications in the future?	NA This question does not need to be asked of ministry employees The MISO response is adequate.	NA This question does not need to be asked of ministry employees The MISO response is adequate.	
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.	An inventory of ISRAs (complete and ongoing) is maintained and regularly reviewed. Outstanding items are tracked and monitored to confirm completion.	Is there a formal ISRA process in place for the ministry? How does the ministry ensure that ISRAs are completed for all new systems and system enhancements (i.e. new systems and older, critical systems)? Do you maintain and regularly review an inventory of all ministry ISRAs? Are outstanding items tracked and monitored to confirm completion?	NA This question does not need to be asked of ministry employees The MISO response is adequate.	NA This question does not need to be asked of ministry employees The MISO response is adequate.	

Information Protection							
#	Criteria	3 - Defined	4 - Managed	MISO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability							
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.	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.	Does the ministry have an awareness program advising employees about malicious code prevention (e.g. "don't click on that attachment" posters, emails, etc.)? Do you maintain a register of specific threat countermeasures (controls)?	How are employees informed of procedures regarding software and applications downloads and updates (i.e. requires supervisor approval)? How are incidents related to malicious code reported and followed up on?	Do you download and regularly update software or applications (outside of the software centre)? If yes, do you follow any approval process (i.e. obtain supervisor approval)?	
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 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.	How do you identify critical IT systems and ensure mitigation and remediation of vulnerabilities? Are assessments planned and conducted on a regular basis? Are vulnerabilities risk-ranked and remediated in priority order? Where remediation is not completed, is there a process to escalate?	NA MISO response is adequate	NA MISO response is adequate	
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.).	Access controls are regularly monitored, reported on and updated on a regular basis.	Do you have a role in supporting branches with access controls? Do you review IDIR accounts and access? Are employees removed from the system in a timely manner?	Do you have a documented access control procedure for both employees and contractors that covers; granting, reviewing, changing and removing access to information systems in a timely manner (e.g. onboarding/offboarding)? Is the access to systems periodically monitored to ensure that only authorized and appropriate personnel have access to information systems?	NA This question does not need to be asked of ministry employees The MISO and manager response is adequate.	

Information Protection							
#	Criteria	3 - Defined	4 - Managed	MISO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability							
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.	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.	Do you maintain audit logs on all ministry systems? For systems managed in the branches, did you provide guidance to the branches on how to determine whether audit logs were required? If yes, do the procedures include instructions for limiting access to the logs? How does the ministry ensure that log exceptions are reviewed and acted upon as necessary? Are the results of monitoring activities reported and used to enhance access and security controls on an ongoing basis?	Do you maintain audit logs on all ministry systems? For systems managed in the branches, how did you determine whether audit logs were required? How does the branch ensure that log exceptions are reviewed and acted upon as necessary? Are the results of monitoring activities reported and used to enhance access and security controls on an ongoing basis?	NA This question does not need to be asked of ministry employees The MISO and manager response is adequate.	
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 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.	How are employees informed of their responsibilities for the protection of government information assets? How are employees informed of the need for access restrictions regarding sensitive government information? How are branches advised to establish processes for user access and responsibilities? How does the ministry ensure that access and user controls are kept up to date and are regularly monitored for accuracy?	How are employees informed of their responsibilities for the protection of government information assets? How does your branch manage access restrictions regarding sensitive government information (e.g. role-based access to information assets)? How does the branch ensure that access and user controls are kept up to date and are regularly monitored for accuracy?	Can you describe any steps you take to prevent unauthorized access to government information (i.e. clean desk, do not leave equipment unattended, do not share password, lock screen, etc.)?	
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.	The business continuity plan is regularly reviewed and exercises are conducted on a periodic basis to test and improve the plan.	Within the ministry's BCP, does it include a risk assessment and information sensitivity component ? In addition to the BCP, do you have a DRP and if so, how frequently is it tested?	NA This question does not need to be asked of ministry employees The MISO and manager response is adequate.	NA This question does not need to be asked of ministry employees The MISO and manager response is adequate.	If manager response is required… why are there no manager questions? Brittany Note - 2019-10-07

Information Protection							
#	Criteria	3 - Defined	4 - Managed	MISO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability							
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.	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.	What is the ministry's asset management process? Is a formal inventory of information assets and systems maintained? Is the inventory actively monitored and updated? How often is ownership of assets reviewed? Are inventory accountabilities monitored?	What is the branch's asset management process? Is a formal inventory of information assets and systems maintained? Is the inventory actively monitored and updated? How often is ownership of assets reviewed? Are inventory accountabilities monitored?	NA This question does not need to be asked of ministry employees The MISO and manager response is adequate.	
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.	Controls related to physical/environmental protection are documented and monitored for effectiveness. They are reviewed and updated on a regular basis.	What is the process you follow to remove government information from devices that are no longer needed by government? How do you securely dispose of devices in a manner appropriate for the sensitivity of the information the device contained? Are these procedures and controls reviewed and updated regularly?	What is the process you follow to remove government information from devices that are no longer needed by government? How do you securely dispose of devices in a manner appropriate for the sensitivity of the information the device contained?	NA This question does not need to be asked of ministry employees The MISO and manager response is adequate.	Maybe not for MISO, TW to follow up
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.	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.	Does the ministry maintain an inventory of portable media? If yes, how often is the inventory of portable media reviewed and updated? Is there a ministry approval process in place for the use of portable media? Does the ministry have policies and procedures regarding the use of portable media? Is there a procedure to assist business areas in setting up and managing their inventory of portable media? How does the ministry ensure that portable media devices comply with applicable OCIO standards and that devices are managed with controls appropriate for the sensitivity of the data they contain?	Does the branch maintain an inventory of portable media? If yes, how often is the inventory of portable media reviewed and updated? Is there a branch approval process in place for the use of portable media? Does the branch have policies and procedures regarding the use of portable media? How does the branch ensure that portable media devices comply with applicable OCIO standards and that devices are managed with controls appropriate for the sensitivity of the data they contain?	Do you use portable media? If yes, have you been provided procedures regarding the use of portable media? If yes, do you store sensitive data on the portable media device? If yes, how do you protect the device appropriately with respect to the sensitivity of the data?	Do you keep list of all portable media devices, like phones or USB sticks with the names of their custodians? Is there a documented policy to inform employees of the appropriate use of these devices? How do you protect the information stored on these devices?

Information Protection							
#	Criteria	3 - Defined	4 - Managed	MISO Questions	Manager Questions	Staff Questions	IMPR Notes
1. Governance and Accountability							
RM 6.	**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.	The inventory process is regularly monitored and exceptions are identified and updated in the inventory on an ongoing basis, where required.	Are you aware of any ministry efforts to establish and maintain an inventory of ministry systems and repositories that manage and/or store government information?			This criteria exists in RM, but MISO may provide relevant information OCIO? MCIO? Who would maintain this? CPPM 12.3.6.3 - Information and technology assets must be classified, inventoried and recorded with an identified officer who is responsible for achieving and maintaining appropriate protection of those assets. CPPM 12.3.5.d.1 - Ministries, in conjunction with Workplace Technology Services, must establish and maintain inventories of computer hardware, software and related communications equipment.

[Type of Engagement]-[YY]-[Engagement #] Ministry acronym

Meeting Notes

[YYYY-MM-DD]

Attendees:

[List of interviewee]
Position, Ministry

[List of interviewer]
Senior Auditors
PCT (CITZ)

	Topic	Questions and Responses	ACTION ITEMS
1			
2			
3			

Meeting Summary:

1. Are there potential findings from this meeting? 2. Did you receive or request any documentation during this interview? 3. Are there any contradictory points that need to be clarified?	

BRITISH COLUMBIA

Page 101 of 107 to/à Page 107 of 107

Withheld pursuant to/removed as

s.13