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 managemen 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 Awarenes						
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 rol 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 Schedule						
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 fo 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 digit 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 transfe 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 ter retention or systematic monitoring of formats and record repositories to help ensure long term usability.
5. Records Retention, Maintenance and Dispositio						
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 awar 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 record 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 Inventorie						

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 enabl easy classification across disparate systems and platforms; and/or * mechanisms and strategies to continuously refine recordkeeping systems adopted for documenting government decisions; ensuring its alignment with Directive CRO 01-2019 and section 6 of the Information Management Act.
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.