VERSION [1.0]

DECEMBER 6, 2017

ONTARIO CYBER SECURITY FRAMEWORK

CONTENTS

INTRODUCTION

The risk of security breaches and exposure to cyber-attacks within the electrical energy sector has grown substantially with the implementation of Smart Grids, Smart Metering and Self-Generation. Increased use of automation, different communication networks, and the use of wireless networks, data flows, hand-held electronic devices and the internet of things (IoT) have created attack vectors that have not been considered in the past. As well, the growing demand for real-time data exchange between entities within the province, to support business units have resulted in increased cyber security risks to Ontario's energy sector.

In the absence of a recognized electricity transmission/distribution standard or framework for cyber security, the OEB facilitated a consultation to establish a cyber security policy and the development of a Framework to be used as the common basis for assessing and reporting capability to the OEB.

In 2016, a Cyber Security Working Group (CSWG), was struck, including a transmitter, a significant number of Local Distribution Company (LDC) participants and other stakeholders. The primary focus of this consultation was to develop an industry cyber security Framework for Ontario's non-bulk power sector. It leveraging recognized industry standards, policy guidelines and auditing requirements by applying a distribution context to provide oversight and validation of the adequacy of measures taken by distributors and transmitters for Ontario's non-bulk system assets.

To assist in developing the Framework, two industry consultative bodies were formed. A Steering Committee of senior industry executives to help define and guide the scope of the Framework, and a Working Group of operational experts were tasked with the development of the Framework at a more detailed level. Industry experts (AESI, Richter and DLA Piper) were engaged to work with these two consultative bodies to develop the Ontario Cyber Security Framework.

The Working Group met from June 2016- Nov 2017. It was composed of local distribution companies (LDCs) including Toronto Hydro, Hydro One, Energy+, Burlington Hydro, Oakville Hydro, London Hydro, Enersource, Veridian Connections, PowerStream and Horizon, with service areas in different planning regions across Ontario. Representatives of the Ontario Ministry of Energy, the OEB, IESO, Electrical Safety Ontario, and the natural gas utilities participated as stakeholders. The result of their cumulative efforts is the Ontario Cyber Security Framework.

CONCEPT

Using both qualitative and quantitative research methods, the Cyber Security Working Group developed an Ontario distributor and non-bulk transmitter Cyber Security Framework (Framework), based on the NIST Cybersecurity Framework, with influences from the DOE-C2M2, Privacy by Design and input from a wide variety of stakeholders.

The CSWG determined that the following criteria for the Cyber Security Framework should be incorporated into the design:

- Needs to reflect different risk profiles to scale requirements;
- Needs to be prescriptive with criteria, not subjective, but allow for operational;
- Needs to be quantitative and defensible;
- Provide process guidance and tools to support LDCs;
- Guidance resources and shared resources to be provided; and
- Needs to describe a phased-in approach that provides a map of incremental improvements over time.

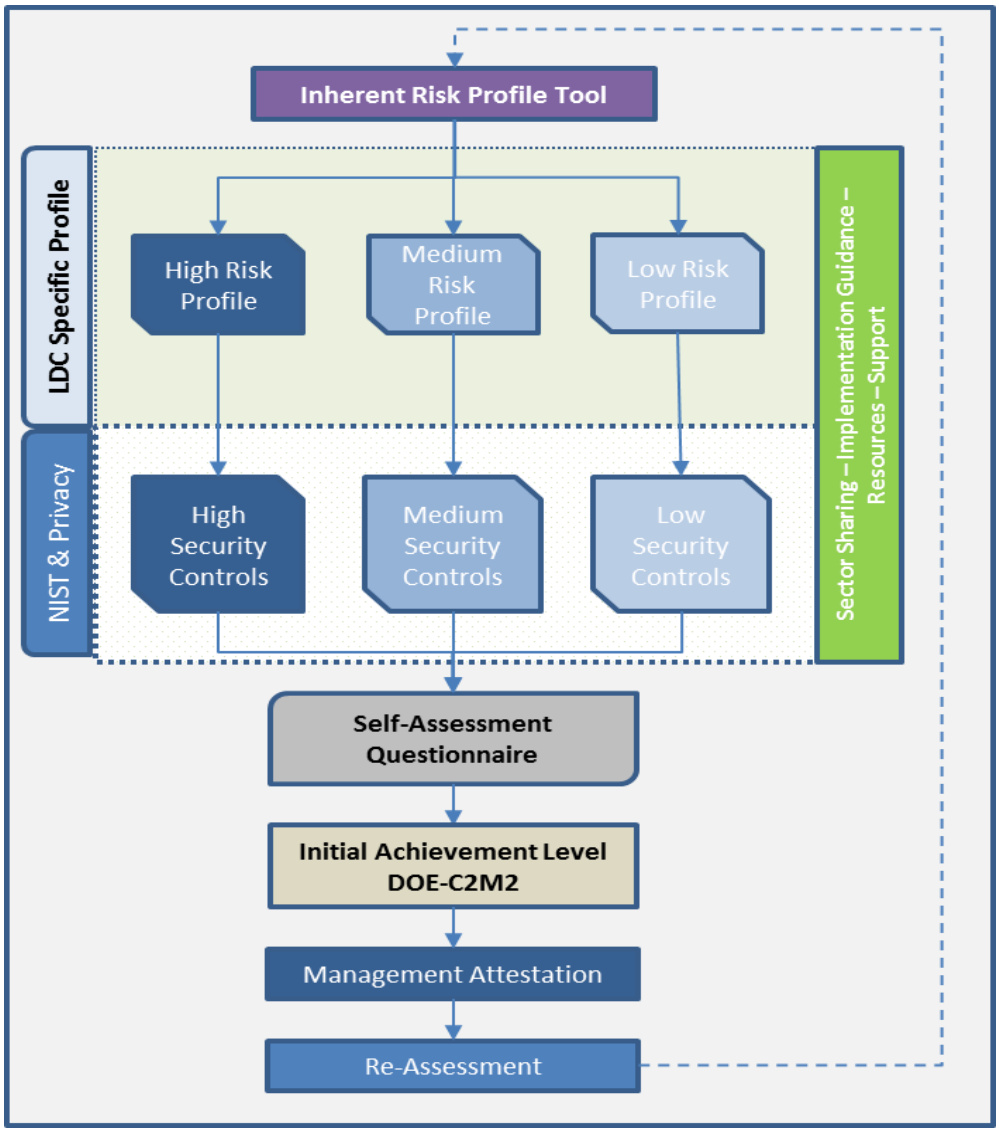
The developed Framework incorporates a process and methodology for transmitters and distributors to assess their level of risk (Inherent Risk Profile Tool) which is mapped to a set of suggested controls (NIST Controls and Privacy Requirements). A self-assessment tool (Self-Assessment Questionnaire) has been designed for the transmitter or distributor to be able to identify their capability relative to the suggested controls. These three instruments form the basis of supporting the reporting requirements outlined by the OEB.

The CSWG also believes that this approach can be used by the transmitter and distributor to inform their enterprise risk management strategies.

The CSWG has designed the Framework in such a manner as to support continuous improvement. This can be achieved in the short term, by adding additional controls to suit the specific risk tolerance of the company. The CSWG is recommending that the long term strategy for the Framework evolution consider the adoption of increasing maturity levels, as described in the US DOE Maturity Model (C2M2).

Conceptually, the Framework can be visualized as follows:

Figure 1 – Ontario Cyber Security Framework



INHERENT RISK PROFILE TOOL

The Cyber Security Framework begins with an Inherent Risk Profile Tool, developed with input from the CSWG and specifically tailored to the inherent cyber security risks in Ontario's LDC community. The Tool allows each Ontario LDC to be categorized objectively. Based on size, maturity and capability, each Ontario LDC will have different inherent risk profiles which will require a varying degree of security controls to be applied to ensure an adequate level of confidence in their cybersecurity posture can be attained. Once an Inherent Risk Profile for the LDC is established using the Tool, the Security Controls (based on NIST with the injection of Privacy by Design and Fair Information Principles) are defined for High, Medium and Low (baseline) entities.

The Inherent Risk Profile Tool utilizes a set of questions shown in Appendix D, with weighed scoring to produce a Risk Profile number. The Risk profile number enables the LDC to be categorized as having High, Medium or Low (baseline) inherent risk.

Ranged thresholds exist to transition between Low to Medium Risk and Medium to High-Risk Profiles. A threshold range provides more flexibility for LDCs to choose the risk profile that best matches their unique situation, rather than defining their risk profile to a single number, helping to recognize that risk is a spectrum, rather than a single specific number.

If an LDC's risk rating score lies within these transition ranges, then the LDC could choose to align to either risk profile or a combination of both. For example, if an LDC's risk rating was 70, they could choose to implement the Low-Risk or Medium-Risk controls. If they implement the Low-Risk controls, it is then recommended that the LDC consider implementing the highest priority controls in the Medium Risk group after they have implemented the controls in the Low Risk / Baseline group.

Figure 2 - Inherent Risk Profile Range

Type	Range
Max Resultant Risk Factor	200
Min Resultant Risk Factor	5
Low Risk Profile Range	0 - 70
Transition Range: Low to Medium	63 - 77
Medium Risk Profile Range	71 - 120
Transition Range: Medium to High	108 - 132
High Risk Profile Range	121 - 200

NIST CONTROLS AND PRIVACY PRINCIPLES

Regardless of whether an entity has a High, Medium or Low-Risk Profile, privacy compliance is mandatory. Accordingly, the CSWG has provided for all entities, regardless of Risk Profile, to be pointed to privacy best practices for implementation.

The NIST Cybersecurity Framework does not address privacy in any detail. It has one (1) Subcategory that speaks to privacy as follows:

> *"ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed".*

While the NIST controls are weak with respect to Fair Information Principles, the NIST controls are entirely compatible with the Fair Information Principles. Indeed, all of the NIST security controls can be seen together as an articulation of a chief Fair Information Principle, "Safeguards". Safeguarding information is key to privacy best practices and is the raison d'être of the NIST Framework. Applying Privacy by Design, 11 privacy controls that express the other nine (9) Fair Information Principles have been integrated amongst the cybersecurity or "Safeguard" controls already present in the NIST Framework. The goal is for such privacy controls to become integral to LDC business processes, functions and technology, as recommended by Privacy by Design. Each of the privacy controls created relates to one or more Fair Information Principles contained in PIPEDA.

The 11 privacy controls are specifically placed at appropriate points among the NIST controls and, together with the NIST controls, address all of the Fair Information Principles. The privacy controls are summarized in the table below.

Figure 3 - Privacy Controls

#	Category	Subcategory	Informative References
1	Asset Management	ID.AM-P1 - The organization is able to identify: the personal information or customer proprietary information in its custody or control, its authority for the collection, use and disclosure of such information, and the sensitivity of such information.	PIPEDA, Sch1, s.4.1, 4.2, 4.3 GAPP, 1.2.3, 8.2.1
2	Asset Management	ID.AM-P2 - Responsibility for the privacy management program has been established	PIPEDA, Sch1, s.4.1 GAPP, 1.1.2, 1.2.6
3	Business Environment	D.BE-P1 - Senior management is committed to a privacy respectful culture	PIPEDA, Sch1, s.4.1 GAPP, 1.1.2, 1.2.1
4	Governance	ID.GV-P1: A policy is established for collection, use and disclosure of customer personal and proprietary information, including requirements for consent and notification	PIPEDA, Sch1, s.4.1.4, 4.3, 4.4· GAPP, 1.1.0, 3.0, 5.0
5	Governance	ID.GV-P2: A policy is established for retention and disposal of customer personal or proprietary information	PIPEDA, Sch1, s.4.5.2, 4.5.3 GAPP, 1.1.0, 5.0
6	Governance	ID.GV-P3: Governance and risk management processes address privacy risks	PIPEDA, Sch1, s.4.1 GAPP, 1.1.2, 1.2.4
7	Risk Assessment	ID. RA-P1: Activities and processes which involve the collection, use or disclosure of personal or customer proprietary information are identified	PIPEDA, Sch1, s.4.1, 4.3 GAPP, 1.2.3, 1.2.4, 1.2.11

#	Category	Subcategory	Informative References
8	Risk Management Strategy	ID.RM-P1: Privacy impacts are considered when a new process, technology or activity is contemplated	PIPEDA, s.5(3), Sch1, s.4.4, 4.5 GAPP, 1.2.4, 1.2.6, 1.2.11
9	Awareness and Training	PR.AT-P1: Documentation is developed to explain the organization's personal information policies and procedures to staff and customers	PIPEDA, Sch1, s.4.1.4, 4.8, 4.9, 4.10 GAPP, 2.0
10	Information Protection Processes and Procedures	PR.IP-P1: Privacy is included in human resources practices (e.g. privacy training)	PIPEDA, Sch1, s4.1.4 GAPP, 1.2.9, 1.2.10
11	Anomalies and Events	DE.AE-P1 - Policies for receiving and responding to privacy complaints or inquiries are established and such policies are communicated to customers	PIPEDA, Sch1, s.4.1.4, 4.6, 4.8, 4.9, 4.10 GAPP, 6.0, 10.0

As with the NIST controls, each of the privacy controls provides informative references. In particular, the privacy controls reference PIPEDA, and specifically, the Fair Information Principles set out in Schedule 1 to PIPEDA. Further, they reference the American Institute of Certified Public Accountants and the Canadian Institute of Accountants (now CPA Canada) Generally Accepted Privacy Principles (GAPP) Guide. GAPP is ten (10) principles that are worded slightly differently from the FIPs, but can be mapped directly to PIPEDA and the FIPs. The GAPP Guide includes a chart that contains useful illustrative controls and procedures that a business might consider as part of its privacy program.

Integrating privacy with the NIST controls is an innovative approach that provides a complete perspective on cyber security and privacy.

INITIAL ACHIEVEMENT LEVEL

Given that all LDCs / non-bulk system operators are at various starting points, based on their experience, the CSWG selected an initial level for each of the risk profiles. The group wanted to align with levels of progress that map to maturity, with the requirement to increase maturity levels over time to be able to effectively address the changing threat landscape.

In one of the CSWG meetings, a breakout session was conducted to test the applicability of various maturity models. The working group provided feedback that the US Department of Energy Cybersecurity Capabilities Maturity Model (DOE C2M2) model was extremely difficult to use on its own, but contained excellent reference material in terms of how to implement security controls.

Further, US DOE provided a mapping document that mapped the C2M2 maturity levels into the NIST Framework providing an integrated approach. The following are the Maturity Indicator Levels (MIL) in the C2M2 model:

Figure 4 - Initial Achievement Level

Initial Achievement Level
MIL0: Not Performed
MIL1: Initiated
MIL2: Repeatable
MIL3: Managed/Adaptive

For the initial achievement levels for the three (3) risk profiles the CSWG have selected MIL1 as the starting point. Although there is no specified period of time allocated for the LDCs to attain the initial achievement levels, identified gaps will inform the report that is provided to the OEB, and LDC's are expected to take the appropriate steps to address these weaknesses.

Using this approach authoritative references from multiple sources, providing specific guidance for LDCs, and providing a phased-in implementation period to achieve higher levels of maturity. Appendix E maps the Initial Achievement Level to each NIST security control as well as establishing the baseline for each risk profile.

METRICS AND REPORTING

An LDC's control environment and principles of reporting form an integral part of the compliance and assurance regime. The Framework begins to articulate the key reporting elements which should be considered. In addition, the Framework will be implemented in a phased approach and reporting will be part of this approach, which will ensure that a strong baseline for reporting is created and that key learnings are integrated into the Framework in future phases of implementation. The Reporting elements outlined under this evolving Framework should be considered as a progression along a staged continuum. This staged approach allows for the development of a baseline reporting strategy and the adoption of an evolving and maturing approach to capability and compliance.

The initial reporting activities LDCs will employ during **"Stage 1"**, would include the completion of a self-assessment questionnaire (SAQ). The Self-Assessment Questionnaire could be used by an organization to validate compliance with the NIST and privacy subcategory elements. In addition, some organizations with very specific business models may find that some NIST subcategory requirements do not apply. As responses will be linked to NIST subcategories, an additional level of integration with the overall Framework will occur and provide the LDC with a roadmap for areas in which the organization is strong, in need to improvement or void of a current reasonable control.

The roadmap will be directly linked to the individual results of the LDC's SAQ responses and test results, potentially allowing for greater integration between areas such as weaknesses, improvements and when an LDC would progress to the next rollout phase of the Framework. Further work regarding the roadmap and key learnings from the process which could be shared broadly between LDC's will need to be explored as the Framework develops and the phased implementation occurs.

COMPLETING THE SELF-ASSESSMENT QUESTIONNAIRE

The Self-Assessment Questionnaire (SAQ), forms the basis for the LDC's understanding of its maturity and capability. Used by the LDC, for internal use, it forms the foundation support for reporting to the OEB.

For each question, there will be a choice of responses to indicate the LDC's status regarding that requirement. A potential description of the meaning of each response is provided in the table below:

Figure 5 - SAQ Definitions

Response	Definition
Yes	The expected testing has been performed and all elements of the requirement have been met
Yes with CCW[1]	The expected testing has been performed and the requirement has been met with the assistance of a compensating control.
Work In Process	Some or all elements of the requirement are in the process of being implemented.
No	Some or all of elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be know if they are in place
N/A	The requirement does not apply to the organization's environment.
Not Tested	The requirement was not included for consideration in the assessment and was not tested in any way

The sample below illustrates the subcategory used related to NIST and the response requirements of the LDC (the reporting entity). It should also be noted that the LDCs will be responsible for responding to the NIST subcategories attributable to them based on their risk profile (i.e., low-risk profile LDC's will have only fifty-six (56) NIST subcategory criteria to self-assess against).

All LDCs, regardless of risk profile, will be directed to each of the privacy controls.

Function	Subcategory	Expected Testing Response	Self-Assessment
IDENTIFY (ID)	**ID.AM-1**: Physical devices and systems within the organization are inventoried	Review written policy and procedures Review asset management inventory files	Select Status
	ID.AM-3: Organizational communication and data flows are mapped	Review written policy and procedures Interview personnel	Select Status
PROTECT (PR)	**PR.AC-3:** Remote access is managed	Review written policy and procedures Examine privileged and general user IDs and associated authorizations	Select Status
	PR.AT-1: All users are informed and trained	Review training material Review list of staff training programs and associated completion checklists	Select Status

[1] CCW compensating control worksheet – this is a document that has additional controls outlined that were required to ensure compliance with the tests performed.

MANAGEMENT CERTIFICATION

The SAQ results support the "Management Certification" such as outlined below. This certification should be provided by the LDC CEO to the OEB, ensuring that appropriate attention and focus is undertaken to address both determining current compliance and the potential follow-up remediation activities required.

Option		Description
	Compliant:	- All sections of the NIST subcategory SAQ are complete. All questions were answered affirmatively, resulting in an overall **COMPLIANT** rating; illustrating overall compliance.
	Non-Compliant	- Not all sections of the NIST subcategory SAQ are complete, or not all question are answered with positive affirmation, resulting in an overall **NON-COMPLIANT** rating - Target Date for Compliance will be set and remediation activities outlined.

IMPLEMENTATION SUPPORT

Surrounding the implementation of these security controls are dual resources for the LDC community. Recognizing that resources, both financial and human, are constrained in the Ontario market, a Cyber Security Exchange is proposed to provide the technical resources and information such as implementation guidance and support, awareness training, threat remediation advice as well as opportunities to liaise with other organizations in North America undergoing similar initiatives to shore-up the cybersecurity posture of their constituents (APPA, NRECA among others).

This is a key factor for the implementation of the security controls so that the duplication of efforts is not cascaded across the industry and that the culture of sharing already inherent in the Ontario LDC community is encouraged and nurtured.

EVOLUTION – COINCIDENT WITH MATURITY LEVELS

The CSWG expects that as the sector matures, that the Framework will evolve to build on the initial Achievement level, by increasing the maturity expectations of the security objectives, from an 'initiated' requirements to 'repeatable' or 'managed', as described in the DOE's C2M2 (i.e. MIL1 to MIL2/3).

Stage 1 - The implementation plan outlines the overall evolution of the implementation of the Framework and its elements. At some point, Stage 1 will be complete. The LDCs will have adopted a baseline of security controls in accordance with their inherent risk profile with maturity implementation level of 1 (MIL1) in accordance with C2M2's implementation levels. The following table from C2M2 describes the maturity implementation levels.

Figure 6 - C2M2 Maturity Implementation Levels

C2M2 Implementation Levels	Characteristics
MIL0	Practices are not performed
MIL 1	Initial practices are performed but may be ad hoc
MIL2	Institutionalization characteristics: - Practices are documented - Stakeholders are identified and involved - Adequate resources are provided to support the process - Standards or guidelines are used to guide practice implementation Approach characteristic: - Practices are complete or more advanced than at MIL1
MIL3	Institutionalization characteristics: - Activities are guided by policy (or other directives) and governance - Policies include compliance requirements for specified standards or guidelines - Activities are periodically reviewed for conformance to policy - Responsibility and authority for practices are assigned to personnel - Personnel performing the practice have adequate skills and knowledge Approach characteristic: - Practices are complete or more advanced than at MIL2

Stage 2 - To evolve to a higher level of maturity, the LDCs will need to begin having their security controls evaluated. The resulting reports to the OEB will no longer be on the status of the LDCs for implementing the baseline. Rather, the reports will indicate the status of the LDCs in reducing their residual risk through the maturation of their security controls. An example of a level of control expected in Stage 2 can be illustrated as follows:

Figure 7 - Stage 2 Controls

Subcategory	High Risk	Med. Risk	Low Risk (Baseline)	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)
ID.AM-1: Physical devices and systems within the organization are inventoried	☑	☑	☑	C2M2 ACM-1a a. There is an inventory of OT and IT assets that are important to the delivery of the function.

MIL2 → C2M2 ACM-1c, d

c. Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards).

d. Inventoried assets are prioritized based on their importance to the delivery of the function.

INCORPORATION OF KEY RISK INDICATORS

As the sector improves its overall cyber security posture, the CSWG is recommending the development of "Key Risk Indicators" **(KRI).**

The **self-assessment** process will enable the LDC to provide reporting in a flexible and meaningful way and will include a possible combination of the SAQ discussed above, along with a set of mutually developed and agreed upon "Key Risk Indicators" (KRI), that would support information sharing and peer learning, and reporting to the OEB.

Risk indicators are metrics capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite.[2] Identifying key risk indicators as a standard reporting and measurement metric across the LDCs will assist the sector in identifying areas of risk across the industry, as well areas of risk within each individual LDC. These key risk indicators must be linked to a risk profile. This will ensure that the measurement of the indicator is effective, efficient, and relevant to the organization. Identifying key risk indicators should include the following steps at a minimum:

- Ensuring LDC involvement when establishing the risk indicator to be reported on. This will ensure that greater buy-in and ownership is achieved by the LDCs. This will also ensure that any KRI's are measurable and feasible to implement and report on.
- Make a balanced selection of risk indicators, including preventative, detective and corrective indicators.
- Ensure that the selected indicators are useful and address the root cause of potential / reported events. Indicators should be linked to high-risk areas.

Ensure that the KRI is highly relevant and possesses a high probability of predicting or indicating an important risk and would have a high business impact.[3]

- Ensure that the KRI can be consistently measured by each LDC. If the KRI cannot be consistently measured across the industry, it will be difficult to aggregate in order to determine the performance of the industry.

The measurement of KRIs will show the following benefits, provided that the most relevant KRIs are identified and measurement guidelines for LDCs are established:

- Provide a warning that a high risk is emerging or exists. This will help guide the OEB's audit/assurance activities
- Identify areas for improvement by analysis of trends
- Assist in continuously improving the governance, risk and compliance environment

[2] ISACA, The Risk IT Framework Excerpt, 2009, www.isaca.org
[3] ISACA, The Risk IT Framework Excerpt, 2009, www.isaca.org

The CSWG expressed interest in seeing examples of cyber security KRIs as a useful tool to help in determining their cyber security posture.

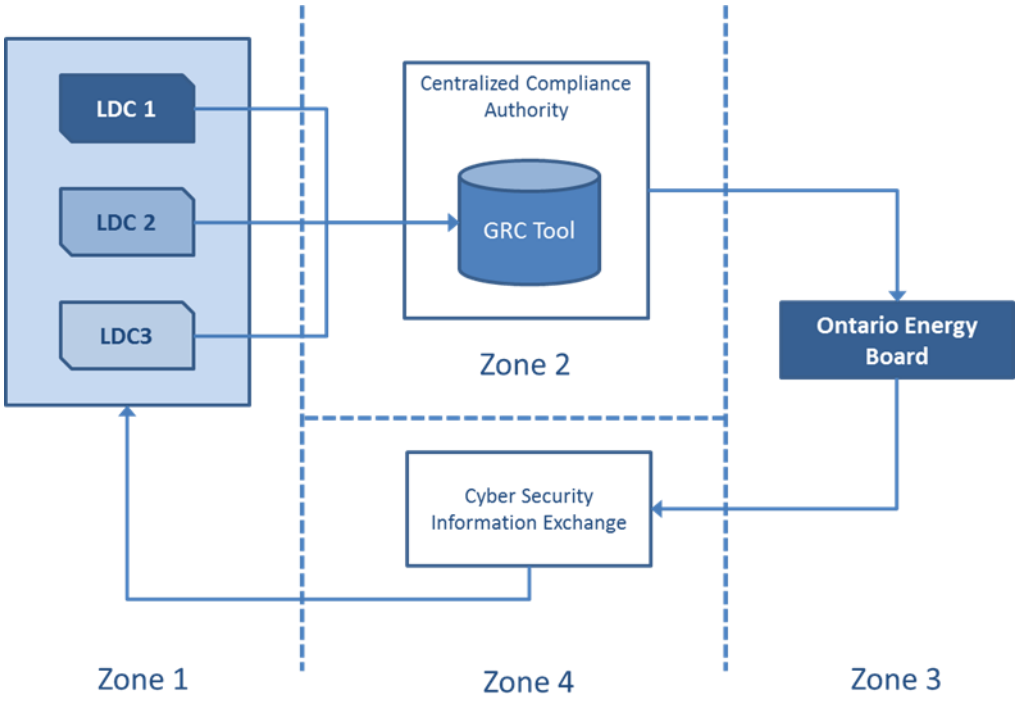
ESTABLISHMENT OF A CENTRALIZED COMPLIANCE AUTHORITY (CCA)

POTENTIAL FUTURE INFORMATION FLOW AND ZONES

The electricity sector in Ontario is interconnected, and cyber security threats should be coordinated in a manner that identifies common and interdependent elements. As a result, the CSWG believes that there is significant value for the sector to establish an independent oversight body to receive additional information based on the LDC SAQ reports, and potentially perform a level of independent auditing. The recommendation includes the establishment of "Central Compliance Authority" (CCA), in order for industry trends and overall progress be understood. The CSWG has recommended that either the sector itself or the OEB establish the CCA.

The following model serves as a reference for a discussion on the scope of a CCA, and potential information flows in the future between LDCs, information sharing and OEB. The purpose of this model is to allow the LDCs to report on the status of the implementation of the Cybersecurity Framework for their organization, without sharing specific control deficiency information with the OEB or other entities.

Figure 8 - GRC Model



LDCs – Gathers and compiles information with respect to their inherent risk through the risk profile tool and reports on the status of their implementation of the NIST Cyber Security Framework + Privacy baseline through a Self-Assessment Questionnaire (SAQ). The SAQ that is completed is commensurate with their inherent risk profile. The

completed SAQ is sent to the CCA where it is programmatically summarized for further use in summary and trending reports.

CENTRALIZED COMPLIANCE AUTHORITY (CCA)

The CCA acts as and completes the following:

Stage 1

- Could be a sector-created and managed entity or a separate division within OEB
- Uses a programmatic tool to collect and summarize the status of the LDCs
- Develops status and trending reports for the OEB to measure including the progress of the LDCs in reaching baseline controls:
    - Percentage of staff dedicated to cybersecurity
    - Percentage of employees with super user access
    - Percentage of endpoints with inactive/suspended end-point protection tools (i.e. virus and firewall)
    - Percentage of un-patched "known" vulnerabilities
    - Number of successful cybersecurity breaches within the year
    - Number of detected network attacks during the year
    - Average number of days between notification of job departure and elimination of corporate access (physical access and logical access)
    - Percentage

Stage 2

- Turns to reporting on the residual risk of the LDCs and the sector by collecting information on the status of the effectiveness of the security controls
- Establishes risk-based and rotational testing consisting of:
    - Self-assessment
    - Desktop audits
    - On-site tests, by CCA or independent 3rd party (SOC 2 plus)

OEB – Obtains summary and statistical information around how the sector is progressing against the NIST and Privacy controls.

Zone 1 - Information in this zone is highly protected and segregated. In Zone 1, certain information specific to the LDC, such as implementation status of a subcategory in NIST Cyber Security Framework, will stay logically separated to the LDC. The Centralized Compliance Authority (CCA), OEB and other LDCs will not have direct access to this information.

Zone 2 – Information in this zone is protected but shared. LDCs provide information into Zone 2 for summarization and anonymization by the CCA. This is done programmatically through a governance, Risk Management and Compliance (GRC) tool. Summary information is passed to the OEB in the form of reports and dashboards for use in policy and decision-making.

Zone 3 – Information in this zone is summarized for the sector for use by the OEB. OEB provides guidance and facilitates initiatives to the C based on the sector analysis.

Zone 4 – Is a shared zone for the LDCs. The Cyber Security Information Forum takes direction from the industry on the types of resources that should be allocated to cyber security (e.g., tools, funding, training, technology, etc.)

- Number (or percentage) of IT security incidents that are cybersecurity related. Even further, number (or percentage) of those that are still open over an "x" number of days
- Number of spam that has been blocked
- Number of employee training sessions on cybersecurity per year
- Percentage of employees that have completed cybersecurity related training

The **desktop audits** would be a more involved process which would require the LDC to provide specific information to allow for a more detailed compliance review. For example, this desk top audit process could involve the establishment of agreed upon specified procedures, outlined between the LDC and the OEB. This may potentially include items such as:

- Review policies and procedures including any significant changes within areas such as technology, security, etc.
- Review any significant changes to hardware/software/etc. and related resources (e.g., staffing, funding, etc.)
- Examine the preparation of the annual business plan and technology strategy to ensure:
    - Appropriate allocation of resources
    - Alignment on strategy across the LDC regarding cybersecurity and general security posture
    - Documentation provided for cyber program implementation appears reasonable and accurate
- Examine any breach occurrences and remediation actions taken
- Review and summarize the observations made through program reviews
- Provide recommendations regarding outcomes of procedures performed

It should be understood that the results of a desktop audit may require further on-site review/audit activity, or may highlight that the LDC is focused and maturing with regards to its cybersecurity posture and, therefore, requires no further review activities at this time. In addition, the desktop audit procedure is foundational in the evolution of the Framework, as outputs from this activity may provide data feedback into the broader LDC community for best practices and made available to the LDCs to assist with Framework baseline implementation strategies in Stage 1 and maturity in Stage 2.

Figure 9 - Zone Reporting Elements

Reporting element	Zone 1	Zone 2	Zone 3	Zone 4
Risk-based profile tool	Specific information stays here	Specific information is securely collected and programmatically summarized and anonymized	Summary information is collected and reviewed	Guidance and resources are provided back to the LDCs based on analysis
SAQ – controls information section	Specific information stays here	Specific information is securely collected and programmatically summarized and anonymized	Summary information is collected and reviewed	Guidance and resources are provided back to the LDCs based on analysis
SAQ – Management certification section	➔	➔ Collected and archived	Certification summary status provided	N/A

AUDITING

The on-site tests, by the CCA or accredited independent 3rd party, involves either the CCA or the use of an independent audit firm(s) that would provide an attestation of compliance for the LDC. This approach can be leveraged to support continuous improvement of LDC operations and provide independent validation regarding the LDC's control environment related to cybersecurity and the effectiveness of their implemented controls.

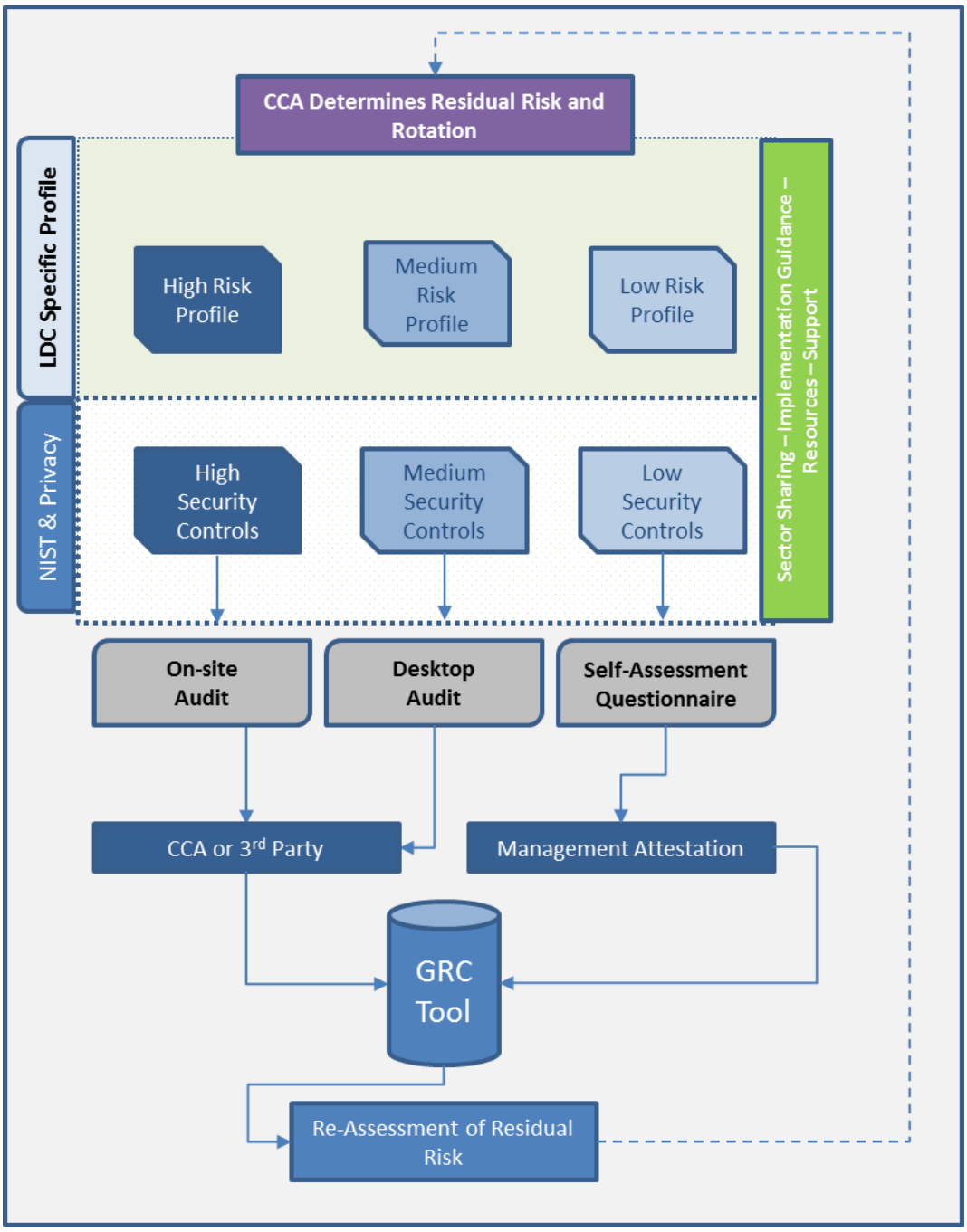
A risk-based approach should be leveraged that integrates leading industry practices and standards to efficiently evaluate the design and operating effectiveness of controls over key IT security and cybersecurity areas specifically. General audit approaches should follow standards such as the International Professional Practices Framework (IPPF) from the Institute of Internal Auditors (IIA). In addition, embedded in this approach should be continuous communication with the key executives and stakeholders, ensuring that collaborative communication facilitates a smooth and efficient audit and ensures that timelines are met.

Outlined below is an illustration of how the typical audit review activity would be executed and some key deliverables that an independent 3rd party would provide through the assurance reporting.

Figure 10 - Audit Review Activity

	Phase 1 Planning and Scoping of Work	Phase 2 Conducting the Audit	Phase 3 Communicating Results
Activities	- Kick-off meeting with key stakeholders - Review existing artifacts - Conduct discovery workshops to determine risk management maturity profile	- Testing of controls using various audit tools and techniques - Documentation of results in working paper files	- Audit report preparation - Communication of findings and recommendations - Exit meeting with Stakeholders
Deliverables	- Planning memo - Risk and control matrix (RCM) - Flowcharts and diagrams	- Completed audit programs	- Findings summary - Audit report

Figure 11 - Ontario Cybersecurity Framework, Stage 2 Concept



IMPLEMENTATION PLAN

The following is the CSWG's recommended implementation plan:

Framework Element	Stage 1 - Baseline	Stage 2 - Maturity
Risk Profile Tool	- Objective to establish baseline controls and security (the implementation of the Inherent Risk Profile Tool will result in articulated corresponding controls to be implement) - Determines inherent risk, makes recommendations for baseline controls - Leverage C2M2 Maturity Integration Levels (MIL) - MIL1 for baseline - Uses NIST Cyber Security Framework + Privacy controls - Initial practices are performed but may be ad hoc (designed)	- Objective is to move towards a more mature level of control and security - Determines residual risk, tracks Key Risk Indicators (KRI) - Leverage C2M2 Maturity Integration Levels (MIL) - MIL2+ - Uses NIST Cyber Security Framework + Privacy controls - Practices are documented and adequate resources are provided to support the process (early stage effectiveness)
Compliance and Reporting	- Basic reporting - Self-assessment questionnaire (SAQ) with management attestation - Follows similar model to PCI Self-Assessment Questionnaire – D (SAQ-D) - Report sent to centralized compliance authority (CCA)	- Next level reporting - Centralized compliance authority establishes risk-based and rotational testing consisting of: - Self-assessment - Desktop audits - On-site tests, by CCA or independent 3rd party (SOC 2 plus) - CCA tracks sector-wide risk by NIST Cyber Security Framework category, does not have access to individual LDC security report - LDCs are provided with anonymous / confidential peer security report - Governance, Risk management and Compliance (GRC) tools are used to collect, secure and disseminate data
Guidance / Support	- Provide guidance on use of risk profile tool - Provide guidance to LDCs on the implementation of controls	- Provide guidance on use of risk profile tool - Provide guidance on the CCA audit cycle - Provide guidance to LDCs on the maturation of controls
Other Approach Notes	- Centralized compliance authority will collect and track results for summarization which could trigger the sector to Stage 2 - Pilot test group should be chosen that can help fine tune the tools, report and guidance	- Early adopters may want to jump to Stage 2, could become pilot test group for tools, reports, KRIs and guidance in this Stage

APPENDIX A - GLOSSARY OF TERMS AND ABBREVIATIONS

American Gas Association (AGA): Represents more than 200 local energy companies that deliver clean natural gas throughout the United States. (www.aga.org)

American Public Power Association (APPA): The service organisation for the more than 2,000 U.S. community-owned electric utilities that serve more than 47 million Americans. APPA was created in September 1940 to represent the common interests of these utilities. Today, APPA's purpose is to advance the public policy interests of its members and their consumers and provide member services to ensure adequate, reliable electricity at a reasonable price with the proper protection of the environment. Regular APPA membership is open to U.S. public power utilities, joint action agencies (state and regional consortia of public power utilities), rural electric cooperatives, Canadian municipal/provincial utilities, public power systems within U.S. territories and possessions, and state, regional, and local associations in the United States and Canada that have purposes similar to APPA. (www.publicpower.org)

Bulk Electric System (BES): Unless modified by the lists shown in the NERC Glossary of Terms, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy. See NERC Glossary of Terms[4] for a list of Inclusions and Exclusions. (NERC)

Bulk Power System (BPS): The interconnected electrical systems within northeastern North America comprised of system elements on which faults or disturbances can have a significant adverse impact outside of the local area. (NPCC)

Canadian Energy Pipeline Association (CEPA): Represents Canada's transmission pipeline companies who operate approximately 119,000 kilometres of pipeline in Canada and 15,000 kilometres in the United States. (www.cepa.com)

Control Objectives for Information and Related Technologies (COBIT): An information technology and control good practice framework created by the Information Systems Audit and Control Association (ISACA) for information technology (IT) management and IT governance.

Cyber Assets (CAs): Programmable electronic devices, including the hardware, software, and data in those devices. (NERC)

Distributed Energy Resources (DERs) are smaller power sources that can be aggregated to provide the power necessary to meet regular demand. As the electricity grid continues to modernise, DER such as storage and advanced renewable technologies can help facilitate the transition to a smarter grid.

Distributed Network Protocol (DNP3): A set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

Electricity Sector Information Sharing and Analysis Center (E-ISAC): Gathers and analyses security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the Electricity Subsector, across interdependent sectors, and with government partners. The E-ISAC, in collaboration with the Department of Energy and the Electricity Subsector Coordinating Council (ESCC), serves as the primary security communications channel for the Electricity Subsector and enhances the subsector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents. The E-ISAC is operated on behalf of the Electricity Subsector by the North American Electric Reliability Corporation. (www.eisac.com)

[4] NERC - Glossary of Terms.pdf

Fair Information Practices Principles (FIPP): These principles are usually referred to as "fair information principles". They are included in the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's private-sector privacy law.

Federal Energy Regulatory Commission (FERC): An independent agency that regulates the interstate transmission of natural gas, oil, and electricity. FERC also regulates natural gas and hydropower projects. (www.ferc.gov)

Federal Financial Institutions Examination Council's (FFIEC): A formal U.S. government interagency body that includes five (5) banking regulators—the Federal Reserve Board of Governors (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). (www.ffiec.gov)

Framework: Provide guidelines without being too detailed or rigid. Frameworks give the organisation the liberty of customizing the structure based on their business needs. Frameworks can be represented with diagrams with little documentation.

Freedom of Information Protection of Privacy Act (FIPPA): The purposes of this Act are to provide a right of access to information under the control of provincial institutions in accordance with the principles that information should be available to the public, necessary exemptions from the right of access should be limited and specific, and decisions on the disclosure of government information should be reviewed independently of government. FIPPA takes into account privacy in determining whether information should be provided. FIPPA also provides individuals with a right of access to their personal information.

Governance, Risk Management and Compliance (GRC): GRC is three pillars that work together for the purpose of assuring that an organisation meets its objectives. Governance is the combination of processes established and executed by the board of directors that are reflected in the organisation's structure and how it is managed and led toward achieving goals. Risk management is predicting and managing risks that could hinder the organisation to achieve its objectives. Compliance with the company's policies and procedures, laws and regulations, strong and efficient governance is considered key to an organisation's success. GRC is a discipline that aims to synchronise information and activity across governance, risk management and compliance in order to operate more efficiently, enable effective information sharing, more effectively report activities and avoid wasteful overlaps.

Independent Electricity System Operator (IESO): The IESO is a not-for-profit corporate entity established in 1998 by the Electricity Act of Ontario. It is governed by an independent Board whose Chair and Directors are appointed by the Government of Ontario. Its fees and licences to operate are set by the Ontario Energy Board and it operates independently of all other participants in the electricity market. (www.ieso.ca)

Independent System Operators (ISOs): Operates a region's electricity grid, administers the region's wholesale electricity markets, and provides reliability planning for the region's bulk electricity system.

Industrial Control Systems (ICyber Security): Encompasses several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCyber Security), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures.

Information Technology (IT): Refers to the corporate business systems and applications.

Intelligent Electronic Device (IED): Microprocessor-based controllers of power system equipment, such as circuit breakers, transformers and capacitor banks

Inter-Control Center Communications Protocol (ICCP): Allows the exchange of real-time and historical power system information including status and control data, measured values, scheduling data, energy accounting data and operator messages.

International Electrotechnical Commission (IEC): Prepares and publishes International Standards for all electrical, electronic and related technologies. (www.iec.ch)

International Organization for Standardization (ISO): ISO is an independent, non-governmental international organisation with a membership of 163 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant international standards that support innovation and provide solutions to global challenges. (www.iso.org)

Internet Protocol Security (IPsec): A protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session.

Intrusion Detection System (IDS): A device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a SIEM system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

Intrusion Prevention System (IPS): A network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine.

Joint Action Agencies (JAAs): A body consisting of utility companies, municipalities who own public utilities, and/or municipalities who purchase energy from private utilities, which acts as a committee for making decisions regarding the acquisition and delivery of energy resources or related services.

Local Distribution Company (LDC): Refers to the companies that make up Ontario's electrical distribution network including small, medium and large utilities. Local distribution companies are responsible for delivering electricity, transformed from the high-voltage transmission system to the low-voltage distribution system, to more than four million Ontario homes, businesses and public institutions. Local distribution companies deal directly with residents and small businesses, create and implement conservation programs and maintain local distribution wires. There are about 80 local distribution companies in the province. They are both publicly and privately owned with the majority being owned by municipalities. Local distribution companies are regulated monopolies in their respective communities and service areas. Their rates are regulated by the Ontario Energy Board. (http://microfit.powerauthority.on.ca/local-distribution-companies)

Low Impact BES Cyber System Electronic Access Point (LEAP): A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems. (NERC)

Low Impact External Routable Connectivity (LERC): Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols). (NERC)

Market Assessment and Compliance Division (MACD): The IESO's Market Assessment and Compliance Division (MACD) monitor the operation of Ontario's electricity market and foster compliance with the Ontario market rules and North American reliability standards. It does this through its prevention, monitoring, auditing, investigation, and enforcement activities. www.ieso.ca/sector-participants/market-oversight

Methodology: Methodology uses a repeatable approach with a defined set of rules, methods, deliverables, and processes for organisations to follow.

Multiprotocol Label Switching (MPLS): A type of data-carrying technique for high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA): Requires municipal institutions to protect the privacy of an individual's personal information existing in government records. The Act creates a privacy protection scheme, which the government must follow to protect an individual's right to privacy. The scheme includes rules regarding the collection, use, disclosure and disposal of personal information in the custody and control of a municipal institution. The Act also gave individuals the right to access municipal government information, including most general records and records containing their own personal information, subject to very specific and limited exemptions

National Institute of Standards and Technology (NIST): A measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. (www.nist.gov)

National Rural Electric Cooperative Association (NRECA): Represents the interests of over 900 electric cooperatives in the United States, to various legislatures. Independent electric utilities are not-for-profit and are owned by their members. (www.electric.coop)

NERC Critical Infrastructure Protection (CIP): Mandatory Reliability Standards include CIP standards 002 through 014, which address the security of Cyber Assets essential to the reliable operation of the electric grid. (NERC)

NIST Internal or Interagency Reports (NISTIR): Describe research of a technical nature of interest to a specialised audience. The series includes interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment). NISTIRs may also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in more comprehensive form.

North American Electric Reliability Corporation (NERC): A not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organisation (ERO) in North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves more than 334 million people. NERC is the US Federal Energy Regulatory Commission (FERC) certified Electric Reliability Organization (ERO) for the United States and confirmed by Ontario Ministry of Energy on November 28, 2006, as the ERO for Ontario and as the successor to the former North American Electric Reliability Council. NERC is a "*Standards Authority*" within the meaning of the Electricity Act, 1998 (Ontario) and the Ontario Market Rules, having the purpose of enhancing the reliability of the international, interconnected bulk power systems in northeastern North America through the development of continent-wide Reliability Standards. (www.nerc.com)

Office of the Information and Privacy Commissioner of Ontario (IPC): The function of the office is to uphold and promote open government and the protection of personal privacy in Ontario, established as an officer of the Legislature by Ontario's Freedom of Information and Protection of Privacy Act (FIPPA). The IPC also has responsibility for the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the Personal Health Information Protection Act (PHIPA). Together, these three Acts establish rules about how the institutions covered may collect, use, and disclose personal data. They also establish a right of access that enables individuals to request their own personal information and have it corrected if necessary. (www.ipc.on.ca)

Open Web Application Security Project (OWASP): an Online community which creates freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security. (www.owasp.org)

OpenSSL: A software library to be used in applications that need to secure communications against eavesdropping or need to ascertain the identity of the party at the other end. It has found wide use in internet web servers, serving a majority of all websites.

Operational Technology (OT): Refers to the systems and applications that are related to grid operations.

Payment Card Industry (Data Security Standard) (PCI DSS): The PCI Security Standards is a global open body formed to develop, enhance, disseminate and assist with the understanding of security standards for payment account security. (www.pcisecuritystandards.org)

Personal Information Protection Electronic Documents Act (PIPEDA): Governs how private sector organisations collect, use and disclose personal information in the course of commercial business. In addition, the Act contains various provisions to facilitate the use of electronic documents.

Policy: High-level management directives and is mandatory.

Privacy by Design (PbD): Developed by the then Information and Privacy Commissioner of Ontario, Canada, Dr Ann Cavoukian, back in the '90s. Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must become an organisation's default mode of operation.

Procedure: Low level and provide step-by-step process to be followed to achieve a specific task. Procedures are mandatory.

Processes: They are well-defined steps and decisions for individuals to follow in order to execute a specific task.

Public Key Infrastructure (PKI): A Public Key Infrastructure incorporates hardware as well as software components, which are in turn managed by security policies. The main components include Public Key Cryptography, a Certificate Authority (CA), a Registration Authority (RA), a Certificate Distribution System, Security Policies, and a PKI-enabled application.

Regional Transmission Operator (RTO): An entity that is independent of all generation and power marketing interests and has exclusive responsibility for grid operations, short-term reliability, and transmission service within a region.

Remote Terminal Unit (RTU): A microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.

Risk Indicator: Is a metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite.

Security Information and Event Management (SIEM): Software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by network hardware and applications.

Standard: Standards are mandatory and define processes or rules to follow the specific use of technology and are often applied to hardware and software.

Supervisory Control and Data Acquisition (SCADA): A system for remote monitoring and control that operates with coded signals over communication channels (using typically one communication channel per remote station). The control system may be combined with a data acquisition system by adding the use of coded signals over communication channels to acquire information about the status of the remote equipment for display or for recording functions. It is a type of industrial control system (ICyber Security). Industrial control systems are computer-based systems that monitor and control industrial processes that exist in the physical world. SCADA systems historically distinguish themselves from other ICyber Security systems by being large-scale processes that can include multiple sites and large distances.

Technical Interconnection Requirements (TIR): The TIR provides Hydro One's technical interconnection requirements for Distributed Generation interconnections at voltages 50kV and below.

US Department of Energy (DOE): a Cabinet-level department of the United States Government concerned with the United States' policies regarding energy and safety in handling nuclear material. Its responsibilities include the nation's nuclear weapons program, nuclear reactor production for the United States Navy, energy conservation, energy-related research, radioactive waste disposal, and domestic energy production. (www.energy.gov)

US Department of Homeland Security (DHS): is a cabinet department of the United States federal government with responsibilities in public security, roughly comparable to the interior or home ministries of other countries. Its stated missions involve antiterrorism, border security, immigration and customs, cybersecurity, and disaster prevention and management. It was created in response to the September 11 attacks. (https://www.dhs.gov/our-mission).

Virtual Private Network (VPN): a private network that extends across a public network or the internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. VPNs can provide functionality, security and/or network management benefits to the user. But they can also lead to new issues, and some VPN services, especially "free" ones, can actually violate their users' privacy by logging their usage and making it available without their consent or make money by selling the user's bandwidth to other users.

APPENDIX B - TABLE OF FIGURES

APPENDIX C - INFORMATIVE REFERENCES

1. AMI System Security Requirements: Security requirements for advanced metering infrastructure.
2. IEEE (Institute of Electrical and Electronics Engineers) 1686-2007, Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities (this document must be purchased).
3. ISO (International Organization for Standardization) 27001, Information Security Management Systems: Guidance on establishing governance and control over security activities (this document must be purchased).
4. NERC CIP Standards 002–009:2 NERC critical infrastructure protection (CIP) standards for entities responsible for the availability and reliability of the bulk electric system.
5. NIST IR 7628:3 Smart grid cyber security strategy and requirements.
6. NIST SP800-39, DRAFT Integrated Enterprise-Wide Risk Management: Organization, mission, and information system view.
7. NIST SP800-53, Recommended Security Controls for Federal Information Systems and Organizations: Catalog of security controls in 18 categories, along with profiles for low-, moderate-, and high-impact systems.
8. NIST SP800-82, DRAFT Guide to Industrial Control Systems (ICS) Security.
9. NIST's Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 2014.
10. U.S. Department of Energy, Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.0, May 2012

APPENDIX D - INHERENT RISK PROFILE TOOL

#	Question	Response				Risk Factor				Additional Context
1	How many customers does your entity serve?	<20K	20K-100K	>100K		1	5	10		Total number of residential and Commercial & Industrial customers
2	How many employees / subcontractors in total does your entity have on staff?	<50	50-200	>200		1	5	10		Total employees and the average number of subcontractors at any time
3	How many employees / subcontractors in total work remotely?	<50	50-200	>200		1	3	5		This includes anyone working from home or remote offices, and accesses utility networks remotely (e.g. using a VPN or similar connection)
4	Does your entity have a contiguous service territory?	Yes	No			0	5			Answer 'no' If the LDCs service territory is geographically diverse and contains remote locations away from major city centers
5	Is your entity connected physically or logically to your municipal network?	Yes	No			3	0			This refers to computer connections to your municipal networks / offices
6	Are your IT and Operational Technology (OT) environments directly connected?	Yes	No			3	0			Directly connected refers to some path of connectivity between the two environments
7	Is your entity connected physically or logically to one of more of your Affiliates?	Yes	No			3	0			This refers to any form of computer connections with the LDC's Affiliates
8	Does your entity process credit card transactions or pre-authorized bank payments?	Yes – On Site Client Data	Yes – No On Site Data	No		3	0	0		This refers to accepting any method of account payment that is not by cheque or cash
9	Does your entity collect driver's license, passport or social insurance number information from customers?	Yes	No			3	0			Answer 'yes' if any of these types of information is taken at account opening or at any other time
10	Does your entity provide your customers' data to any third party vendor?	Yes	No			3	0			This could include AMI data, energy usage data, etc.

#	Question	Response				Risk Factor				Additional Context
11	Do your employees use their own devices (mobile phones, tablets, PCs) for work purposes?	Yes	No			3	0			This refers to connecting with LDC applications from employee's own devices
12	Do your subcontractors use their own devices (mobile phones, tablets, PCs) for work purposes connected to your networks / applications?	Yes	No			3	0			This refers to connecting with LDC applications from subcontractor's own devices
13	Does your entity allow USBs to be inserted into computing devices?	Yes	No			3	0			This refers to computing devices of any type
14	How many third parties have access to your systems?	<10	10 to 50	>50		1	3	5		Third parties include third party vendors, service providers, etc.
15	Does your entity outsource any IT or OT services, including cloud computing?	Yes	No			5	0			This refers to any application that is outsourced
16	Does your entity have a SCADA System/ Distribution Management System?	Yes	No			5	0			This refers to the head end control systems
17	Does your entity have one or more SCADA HMI systems?	Yes	No			5	0			This refers to the distributed control systems (e.g. in substations)
18	Does your entity have any SCADA points that are shared with another entity?	Yes	No			5	0			This would include any shared points between the transmission provider, generators, and LDCs
19	Does your entity have a smart meter / AMI system?	Yes	No			3	0			This refers to automated meter systems
20	Does your entity provide metering connections separate from your AMI system for Commercial & Industrial customers?	Yes	No			3	0			This refers to separate wholesale metering arrangements
21	Does your entity have Distribution Automation technology?	Yes	No			3	0			This refers to automated technology (e.g. re-closers / breaker control) deployed within the service territory

#	Question	Response				Risk Factor				Additional Context
22	Does your entity provide smart energy technology for your customers?	Yes	No			3	0			This refers to devices at customer sites that communicate usage information to the utility such as smart thermostats, Home Area Networks, etc.
23	Does your entity host any applications for another party?	Yes	No			3	0			This includes any form of hosting that you provide for other parties
24	Does your entity provide any computing-based services for another party? (e.g. billing, SCADA, MDM)	Yes	No			3	0			This refers to cloud based / virtual services that you provide for other entities
25	How many Distribution Substations does your entity have?	0	1 to 10	10 to 50	>50	0	3	5	10	The total number of Distribution Substations that you own and operate
26	Does your entity have Substation Automation technology?	Yes	No			3	0			This refers to advanced automation in the substation
27	How many Transformer Stations does your entity own?	0	1-3	4-7	>8	0	3	5	10	The total number of Transformer Stations that you own and operate
28	Does your entity have an Outage Management System?	Yes	No			3	0			This is any form of automated outage management
29	Does your entity have a Geographical Information System?	Yes	No			3	0			This is any form of automated geographical information systems
30	Are your operational field devices administered remotely?	Yes	No			3	0			This includes substation equipment, breakers, relays, etc.
31	Does your entity have ICCP connections with the IESO or your transmission provider?	Yes	No			5	0			This refers to ICCP connections between any other entity and your entity
32	Does your entity have RTU connections with the IESO or your transmission provider?	Yes	No			5	0			This refers to any RTUs that you own that other entities have access to
33	Does your entity have field personnel that use mobile computing devices?	Yes	No			3	0			This includes field technicians with smart meter tools, diagnostic tools, etc.

#	Question	Response				Risk Factor				Additional Context
34	Does your entity use wireless communications for networks or SCADA?	Yes	No			3	0			Wireless includes all forms of wireless including proprietary, WiMAX, microwave, etc. Any wireless access is a potential external access point to systems.
35	Does your entity have Distributed Energy Resources / Micro Grids connected to your systems?	Yes	No			3	0			This refers to any solar / wind / renewable systems and / or full Micro Grid implementations in your service territory that you own and operate
36	What is your generation capacity as a % of load?	0%	<25%	25%-50%	>50%	0	3	5	10	This is your total generation sources that you own and operate as a % of your total load
37	Are you currently involved in any publicly disclosed merger & acquisition discussions?	Yes	No			5	0			This refers to any M&A activity that has been disclosed
38	Are you currently in the process of implementing a merger & acquisition?	Yes	No			10	0			This refers to the implementation / integration period after the M&A transaction closes
39	Do you allow sensitive data to be stored offsite?	Yes	No			3	0			This includes any form of IT or OT data, and refers to any storage of data off-premises, including in the cloud
40	Is your entity connected physically or logically to another LDC?	Yes	No			3	0			This refers to any computer connections with another LDC
41	Does your entity have any shared OT environments?	Yes	No			3	0			This includes connectivity / sharing with other OT environments such as water, ISP, etc.
42	Does your entity serve any critical infrastructure installations?	Yes	No			3	0			This includes any sensitive cortical infrastructure such as military bases, any major medical facilities, major federal government offices, Embassies, etc.

#	Question	Response				Risk Factor				Additional Context
43	Does your entity provide any public facing applications that require authentication?	Yes	No			3	0			This includes any applications that you provide for consumers / businesses, such as for viewing their data usage or account information on-line
44	Is your entity involved in any publicly contentious energy projects?	Yes	No			3	0			This would include any contentious wind, solar, hydro projects
45	Does your entity provide any Demand Response programs?	Yes	No			3	0			This includes any demand response, peak shaving, load management programs that you provide and manage
46	Does your entity share any operating data with other entities?	Yes	No			3	0			This includes sharing with fire departments, police, emergency response, etc.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	· **CCS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8	X	X	1	C2M2 ACM-1a: There is an inventory of OT and IT assets that are important to the delivery of the function	This could be as simple as a spreadsheet containing a list of OT and IT p**hysical devices and systems** with some indication of their importance to the delivery functions. It could be as sophisticated as an automated asset management and tracking tool. Often this information can be collected from various IT systems scanning and detection tools. This inventory may be collected during business impact analysis exercises in preparation of a disaster recovery plan (DRP). This inventory may be collected in preparation for vulnerability assessments. It may be collected as part of a software licensing audit.
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CCS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8	X	X	1	C2M2 ACM-1a: There is an inventory of OT and IT assets that are important to the delivery of the function	As with ID.AM-1, this could be as simple as a spreadsheet containing a list of OT and IT **software platforms and applications** with some indication of their importance to the delivery functions. It could be as sophisticated as an automated asset management and tracking tool. Often this information can be collected from various IT systems scanning and detection tools. This inventory may be collected during business impact analysis exercises in preparation of a disaster recovery plan (DRP). This inventory may be collected in preparation for vulnerability assessments. It may be collected as part of a software licensing audit.
		ID.AM-3: Organizational communication and data flows are mapped	· **CCS CSC** 1 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8	X	X	3	The entity has created a communications and data flow map for the OT and IT assets that are important to the delivery of the function.	These communications and data flow maps may include a number of different artefacts, including data flow diagrams, network diagrams, interface maps and business process flow documentation. Data flow diagrams may have been created as part of a data classification exercise. Network diagrams may have been created as part of the network architecture planning and ongoing support. Business process flow documentation may have been created as part of the development and integration of new IT and OT systems. It is important as this control matures that this documentation is updated regularly and hangs together to provide management with the information it requires to make decisions concerning critical IT and OT systems.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
		ID.AM-P1 - The organization is able to identify: the personal information or customer proprietary information in its custody or control, its authority for the collection, use and disclosure of such information, and the sensitivity of such information.	· **PIPEDA**, Sch 1, s.4.1, 4.2, 4.3 · **GAAP**, 1.2.3, 8.2.1	X	X	1	The entity has created an inventory of customer information categories and has identified the purpose for the collection of each category of information.	"Personal information" means information about an identifiable individual. PIPEDA provides that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. PIPEDA further requires that the organization document the purposes for which personal information is collected. This inventory could include, for example, a spreadsheet, with one column listing the information sought when a new account is opened and other customer information collected from-time-to time and marked in the customer's file (such as a customer complaint or disconnection), and a second column answering the question "why is this information needed?". This inventory should include categories such as name, address, primary contact number, secondary contact number, individuals authorized to seek account information, driver's license, etc. Reasons may include: for billing purposes, to notify in case of emergency, for collections purpose, OEB requirement, etc.
		ID.AM-4: External information systems are catalogued	· **COBIT 5** APO02.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9	X	X	1	C2M2 EDM-1a: "Important IT and OT supplier dependencies are identified (i.e., external parties on which the delivery of the function depend, including operating partners)"	The organization should have a set of operational procedures, contracts and service level agreements in place with important suppliers for which the entity is dependent on their services. The operational procedures should clearly define the tasks and interactions between the entity and the supplier, including escalation procedures. The contract and service level agreement should clearly identify the tasks and responsibilities of the supplier, including tasks and responsibilities with respect to maintaining security controls. Where a significant amount of security and control is dependent on the supplier, the entity should obtain on an annual basis, a report on controls, such as a service organization control (SOC) report, completed by an accredited and independent accounting firm (i.e. Chartered Professional Accountants (CPA) Canada or American Institute of Certified Professional Accountants (AICPA)).
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· **COBIT 5** APO03.03, APO03.04, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14	X	3		C2M2 ACM-1a: "There is an inventory of OT and IT assets that are important to the delivery of the function" C2M2 ACM-1b: "There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data)"	This could be as simple as a spreadsheet containing a list of OT and IT assets with some indication of their importance to the delivery functions. It could be as sophisticated as an automated asset management and tracking tool. Often this information can be collected from various IT systems scanning and detection tools. This inventory may be collected during business impact analysis exercises in preparation of a disaster recovery plan (DRP). This inventory may be collected in preparation for vulnerability assessments. It may be collected as part of a software licensing audit. The inventory listing should identify the criticality of the asset in relation to delivery as well as the exposure of the asset in the attack surface (i.e. inherent security risk profile). For example, a web server in a DMZ would normally be considered high risk due to high visibility to the public. "
		ID.AM-P2 - Responsibility for the privacy management program has been established	· **PIPEDA**, Sch 1, s.4.1 · **GAPP**, 1.1.2, 1.2.6	X	X	1	Senior management has designated a representative of the entity (privacy officer) to oversee all activities related to the development and implementation of and adherence to the entity's privacy policies and procedures.	PIPEDA requires that the organization designate an individual(s) who is accountable for compliance with PIPEDA. This does not necessarily have to be a full-time person, nor does it have to be someone who works exclusively on privacy issues.
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce	· **COBIT 5** APO01.02, DSS06.03	X	X	1	C2M2 WM-1a: "Cybersecurity responsibilities for the function are identified"	Cybersecurity roles and responsibilities are often identified and established within the organizations' information security policies, procedures, standards and guidelines. A well-written information security policy, procedure, standard

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
		and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11				C2M2 WM-1b: "Cybersecurity responsibilities are assigned to specific people"	or guideline will identify the roles and responsibilities of individuals, department, business units including different levels of management, employees and contractors. The roles and responsibilities may be described with respect to particular areas of information security. Cybersecurity roles and responsibilities are commonly found in acceptable use policies and/or code of conduct policies. Cybersecurity roles and responsibilities can sometimes be found in job descriptions for jobs that have a specific task that involves information security. Contracts with 3rd parties should clearly identify cybersecurity roles and responsibilities.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	· **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** CP-2, SA-12	X	X	2	C2M2 EDM-1b: "Important customer dependencies are identified (i.e., external parties that are dependent on the delivery of the function including operating partners)"	Artefacts and documentation related to the organization's role in the supply chain may appear in several areas, including but not limited to: Operations manuals should clearly identify the dependencies on external parties for the delivery of services. Contract management systems should have a listing of external parties, identifying those that are critical to services. A business impact assessment, disaster recovery plan and/or a business continuity plan might identify important customer dependencies.
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	· **COBIT 5** APO02.06, APO03.01 · **NIST SP 800-53 Rev. 4** PM-8	X	X	2	C2M2 EDM-1b: "Important customer dependencies are identified (i.e., external parties that are dependent on the delivery of the function including operating partners)"	Artefacts and documentation related to the organization's role in the supply chain (place in critical infrastructure) may appear in several areas, including but not limited to: The organization's annual plan, financial statements and key reports to stakeholders and the executive board may include mission statements and business objectives that describe the organization's role in critical infrastructure. Operations manuals should clearly identify the dependencies on external parties for the delivery of services. Contract management systems should have a listing of external parties, identifying those that are critical to services. A business impact assessment, disaster recovery plan and/or a business continuity plan might identify important customer dependencies.
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	· **COBIT 5** APO02.01, APO02.06, APO03.01 · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 · **NIST SP 800-53 Rev. 4** PM-11, SA-14	X	X	3	A mission statement has been developed and communicated it to all employees.	The organization's annual plan, financial statements and key reports to stakeholders and the executive board may include mission statements and business objectives that describe the organization's role in critical infrastructure. This should be communicated to all new employees through on-boarding material. It should be available via the organization's website and/or intranet.
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14	X	X	1	C2M2 ACM-1a: "There is an inventory of OT and IT assets that are important to the delivery of the function" C2M2 ACM-1b: "There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data)" C2M2 EDM-1a: "Important IT and OT supplier dependencies are identified (i.e., external parties on which the delivery of the function	This could be as simple as a spreadsheet containing a list of OT and IT assets with some indication of their importance to the delivery functions. It could be as sophisticated as an automated asset management and tracking tool. Often this information can be collected from various IT systems scanning and detection tools. This inventory may be collected during business impact analysis exercises in preparation of a disaster recovery plan (DRP). This inventory may be collected in preparation for vulnerability assessments. It may be collected as part of a software licensing audit. The inventory listing should identify the criticality of the asset in relation to delivery as well as the exposure of the asset in the attack surface (i.e. inherent security risk profile). For example, a web server in a DMZ would normally be considered high risk due to high visibility to the public. "

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
							depend, including operating partners)"	
		ID.BE-P1 - Senior management is committed to a privacy respectful culture	· **PIPEDA**, Sch 1, s.4.1 · **GAPP**, 1.1.2, 1.2.1	X	X	1	Senior management promotes staff privacy awareness through the allocation of specific resources (ex. Training, orientation, educational programs, information bulletins)	Management should show staff that customer privacy is important to them. This could include written directives from management reminding all employees to be mindful of customer privacy issues, posters in the lunchroom with privacy tips and best practices, the distribution of a mandatory online training video, etc.
		ID.BE-5: Resilience requirements to support delivery of critical services are established	· **COBIT 5** DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14	X	2		C2M2 IR-4a: "The activities necessary to sustain minimum operations of the function are identified" C2M2 IR-4b: "The sequence of activities necessary to return the function to normal operation is identified" C2M2 IR-4c: "Continuity plans are developed to sustain and restore operation of the function"	A business impact assessment should identify the key activities that are required to sustain minimum operations. Disaster recovery and business continuity plans should identify a sequence activities to recover IT and business operations. Critical assets may have operational guides that list the sequence of activities to recover the asset in the case of outage or malfunction. Critical business capabilities when driven through information technology should be architected for resiliency using fail-over capabilities. Concepts to be found in the artefacts listed above include: Hot site - A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. Warm site - A warm site is a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Cold site - A cold site is the least expensive type of backup site for an organization to operate. It does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up. Recovery Point Objective (RPO) - Is the maximum targeted period in which data might be lost from an IT service due to a major incident. Recovery Time Objective (RTO) - is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and	**ID.GV-1:** Organizational information security policy is established	· **COBIT 5** APO01.03, EDM01.01, EDM01.02 · **ISA 62443-2-1:2009** 4.3.2.6	X	X	1	A security policy has been developed and communicated to all employees.	An information security policy s a set or rules enacted by an organization to ensure that all users or networks of the IT structure within the organization's domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organization stretches its authority. Typically it will contain the following elements: - Purpose - Scope - Objectives

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
	inform the management of cybersecurity risk.		· **ISO/IEC 27001:2013** A.5.1.1 · **NIST SP 800-53 Rev. 4** -1 controls from all families · **PIPEDA**, Sch1, s.4.7 · **GAPP**, 1.2.7					- Roles and responsibilities - Reference to relevant legislation An information security policy may be supported by an information security policy framework that divides the policy into different areas of information security concern, each being a separate artifact with an overarching policy. For example, there may be a specific policy concerning the classification, labelling and handling of data. However, the organization chooses to document the information security policy it is important that it is communicated to all employees. Communication can occur in a number of ways, including but not limited to: - Company intranet - New hire onboarding - Security awareness training - Annual sign-off
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	· **COBIT 5** APO13.12 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 · **NIST SP 800-53 Rev. 4** PM-1, PS-7	X	X	1	C2M2 WM-1a: "Cybersecurity responsibilities for the function are identified" C2M2 WM-1b: "Cybersecurity responsibilities are assigned to specific people"	Cybersecurity roles and responsibilities are often identified and established within the organizations' information security policies, procedures, standards and guidelines. A well-written information security policy, procedure, standard or guideline will identify the roles and responsibilities of individuals, department, business units including different levels of management, employees and contractors. The roles and responsibilities may be described with respect to a particular areas of information security. Cybersecurity roles and responsibilities are commonly found in acceptable use policies and/or code of conduct policies. Cybersecurity roles and responsibilities can sometimes be found in job descriptions for jobs that have a specific task that involves information security. Contracts with 3rd parties should clearly identify cybersecurity roles and responsibilities.
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· **COBIT 5** MEA03.01, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.7 · **ISO/IEC 27001:2013** A.18.1 · **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)	X	X	1	Legal and regulatory requirements have been reviewed and understood.	The electricity subsector has created several guidelines, standards, and programs based on cybersecurity practices and controls. Any utility that opts to use the Framework should leverage these existing materials, rather than create new—and perhaps duplicative—efforts. - Complies with the latest applicable version of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards; - Is aware of other security standards and relies on the informative references used in the Framework Core; - Has performed a Department of Energy (DOE) Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) self-evaluation and is knowledgeable in the relevant domains and practices; and - Is familiar with risk management processes, such as those contained in both the NERC CIP standards and DOE Risk Management Process.
		ID.GV-P1: A policy is established for collection, use and disclosure of customer	· **PIPEDA**, Sch1, s.4.1.4, 4.3, 4.4	X	X	1	A policy requires reasonable efforts to ensure that customers are notified of the purposes for which their	PIPEDA provides that entities shall implement policies and practices to give effect to privacy principles, including implementing procedures to protect personal information, establishing procedures to receive and respond to complaints and inquiries, training staff and communicating to staff information

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
		personal and proprietary information, including requirements for consent and notification	· GAPP, 1.1.0, 3.0, 5.0				information is collected, how it is used and when and how it will be disclosed.	about the organization's policies and practices, and developing information to explain the organization's policies and procedures. The policy could include, for example, a requirement that a script be used during an intake phone call, that employees comply with a questions and answer sheet, that the website specify what personal information is collected, why it is collected, and what it is used for, that customers with questions about their personal information are directed to a specific employee who can answer their questions, that customer information only be disclosed to third parties under particular circumstances, etc.
		ID.GV-P2: A policy is established for retention and disposal of customer personal or proprietary information	· **PIPEDA**, Sch1, s.4.5.2, 4.5.3 · **GAPP**, 1.1.0, 5.0	X	X	1	General guidelines have been established for preventing the retention of customer information, and its safe disposal, after its identified purposes have been fulfilled.	PIPEDA requires that personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Employees should be told what to do with customer information when an account is closed and the information is no longer needed to perform services.
		ID.GV-P3: Governance and risk management processes address privacy risks	· **PIPEDA**, Sch1, s.4.1 · **GAPP**, 1.1.2, 1.2.4	X	X	1	Privacy policies and procedures are reviewed and approved by senior management. The board of directors (or a committee thereof) includes privacy periodically in its regular review of overall corporate governance. A process is in place to periodically identify the risks of unauthorized use or disclosure of the entity's customer information.	PIPEDA provides that an organization is responsible for personal information under its control. Privacy compliance should be discussed in a formal manner among senior management and among the directors, and discussions should include how to evaluate the policies referred to in ID.GV-P1, ID.GV-P2 and DE.AE-P1.
		ID.GV-4: Governance and risk management processes address cybersecurity risks	· **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **NIST SP 800-53 Rev. 4** PM-9, PM-11	X	X	1	C2M2 RM-2a: "Cybersecurity risks are identified" C2M2 RM-2b: "Identified risks are mitigated, accepted, tolerated, or transferred" The Executive Team and Board are actively involved and supportive of the Cyber Security Program.	As part of the organization's risk assessment processes, cybersecurity related risks are identified, registered and a risk mitigation plan is in place. Indicators that an organization does this include: - Risk strategy - Threat risk assessments - Risk register - Enterprise risk management program If artefacts similar to the above exist, they should also be addressing cybersecurity related risks.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	· **CCS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	X	1		C2M2 TVM-2a: "Information sources to support cybersecurity vulnerability discovery are identified (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings, internal assessments)" C2M2 TVM-2b: "Cybersecurity vulnerability information is gathered and interpreted for the function"	A vulnerability management program is in place that tracks vulnerabilities that are specific to the IT assets. Information concerning vulnerabilities to the organization's assets can come from multiple sources including, ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings, internal assessments. Typically organizations deploy an automated vulnerability scanning tool to identify vulnerabilities to their assets.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
		ID. RA-P1: Activities and processes which involve the collection, use or disclosure of personal or customer proprietary information are identified	· PIPEDA, Sch1, s.4.1, 4.3 · **GAPP**, 1.2.3, 1.2.4, 1.2.11	X	X	1	When a new activity or process is being considered, or an activity or process is being changed, the entity considers whether customer information is flowing and, if so, considers where it flows from, to whom it flows, and under what conditions.	"Personal information" means information about an identifiable individual. PIPEDA provides that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.PIPEDA further provides that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5	X	3		C2M2 TVM-1a: "Information sources to support threat management activities are identified (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associates, vendors, federal briefings)" C2M2 TVM-1b: "Cybersecurity threat information is gathered and interpreted for the function" C2M2 TVM-2a: "Information sources to support cybersecurity vulnerability discovery are identified (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings, internal assessments)" C2M2 TVM-2b: "Cybersecurity vulnerability information is gathered and interpreted for the function"	Information concerning vulnerabilities to the organization's assets can come from multiple sources including, ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings, internal assessments. This information may come in the form of email lists, web-based databases or internally from automated vulnerability scanners.This information is collected and reviewed against the organization's IT assets to determine if mitigating controls need to be deployed.
		ID.RA-3: Threats, both internal and external, are identified and documented	· **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16	1			C2M2 TVM-1a: "Information sources to support threat management activities are identified (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associates, vendors, federal briefings)" C2M2 TVM-1b: "Cybersecurity threat information is gathered and interpreted for the function"	Information concerning vulnerabilities to the organization's assets can come from multiple sources including, ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings, internal assessments. This information may come in the form of email lists, web-based databases or internally from automated vulnerability scanners. This information is collected and reviewed against the organization's IT assets to determine if mitigating controls need to be deployed.
		ID.RA-4: Potential business impacts and likelihoods are identified	· **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14	1			C2M2 TVM-1d (MIL2): "A threat profile for the function is established that includes characterization of likely intent, capability, and target of threats to the function" C2M2 TVM-1f (MIL2): "Identified threats are analyzed and prioritized"	The organization conducts threat risk assessments on a regular basis to determine the impact that threats may have on the organizations assets and processes. The threats are documented in a risk register. The organization assesses the threat in the risk register based on known vulnerabilities, the likelihood and impact to determine the risk treatment or set of controls that reduce the risk of the threat manifesting itself.
		ID.RA-5: Threats, vulnerabilities, likelihoods,	· **COBIT 5** APO12.02	1			C2M2 RM-1c (MIL3): "Organizational risk criteria	The organization conducts threat risk assessments on a regular basis to determine the impact that threats may have on the organizations assets and

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
		and impacts are used to determine risk	· **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16				(objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available" C2M2 RM-2j (MIL3): "A risk register (a structured repository of identified risks) is used to support risk management activities" C2M2 TVM-2m (MIL3): "Cybersecurity vulnerability information is added to the risk register (RM-2j)"	processes. The threats are documented in a risk register. The organization assesses the threat in the risk register based on known vulnerabilities, the likelihood and impact to determine the risk treatment or set of controls that reduce the risk of the threat manifesting itself.
		ID.RA-6: Risk responses are identified and prioritized	· **COBIT 5** APO12.05, APO13.02 · **NIST SP 800-53 Rev. 4** PM-4, PM-9	1			C2M2 RM-2e (MIL2): "Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy" C2M2 TVM-1d (MIL2): "Cybersecurity vulnerability information sources that address all assets important to the function are monitored"	The organization conducts threat risk assessments on a regular basis to determine the impact that threats may have on the organizations assets and processes. The threats are documented in a risk register. The organization assesses the threat in the risk register based on known vulnerabilities, the likelihood and impact to determine the risk treatment or set of controls that reduce the risk of the threat manifesting itself.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	· **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **NIST SP 800-53 Rev. 4** PM-9	X	X	1	C2M2 RM-2a: "Cybersecurity risks are identified" C2M2 RM-2b: "Identified risks are mitigated, accepted, tolerated, or transferred"	As part of the organizations risk assessment processes, cybersecurity related risks are identified, registered and a risk mitigation plan is in place. Indicators that an organization does this include artefacts such as: - Risk strategy - Threat risk assessments - Risk register - Enterprise risk management program If artefacts similar to the above exist, they should also be addressing cybersecurity related risks. The processes documented in artefacts listed above include an appropriate set of stakeholders for the organization including asset owners, information owners and executives. This should include executive committees and/or board of directors.
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.2.6.5 · **NIST SP 800-53 Rev. 4** PM-9	X	1		C2M2 RM-1c (MIL3): "Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available" C2M2 RM-1e (MIL3): "An	As part of the organization's risk management processes, a set of criteria exist that enable the organization to consistently evaluate risks. The organization has gone through a risk harmonization process to ensure risks can be broadly discussed across different business units or functions. The executive committee or the board of directors have established the organization's risk appetite/tolerance.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
							organization-specific risk taxonomy is documented and is used in risk management activities"	
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	· **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14	X	1		C2M2 RM-1b (MIL2): "The strategy provides an approach for risk prioritization, including consideration of impact"	The executive committee or the board of directors have established the organization's risk appetite/tolerance. This risk tolerance is created in the context of the organization's role in the sector. Sector-specific language is understood and used in the risk tolerance statements.
		ID.RM-P1: Privacy impacts are considered when a new process, technology or activity is contemplated	· **PIPEDA**, s.5(3), Sch1, s.4.4, 4.5 · **GAPP**, 1.2.4, 1.2.6, 1.2.11	X	X	1	The entity's privacy officer is consulted before a new process, technology or activity is implemented to provide advice with respect to potential privacy impacts and mitigation strategies.	PIPEDA provides that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances. PIPEDA further provides that collection of personal information shall be limited to that which is necessary for the purposes identified by the organization, that information be collected by fair and lawful means, and that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Any new process, technology or activity should be examined to attempt to minimize the amount of personal information collected/used/disclosed.
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	· **CCS CSC** 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 4** AC-2, IA Family · **GAPP**, 8.2.2	X	X	1	C2M2 IAM-1a: "Identities are provisioned for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities)" C2M2 IAM-1b: "Credentials are issued for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys)" C2M2 IAM-1c: "Identities are deprovisioned when no longer required." - Deprovisioning is the act of removing access from and freeing up resources reserved by end users and their file transfer workflows. Rapid removal of access upon termination or end of contract is key to any organization."	An access control policy is in place and is followed for provisioning, changing or terminating access for employees and services to the organization's assets. It should include controls addressing: - Authentication - Authorization - Roles - Delegation This may be further augmented by more sophisticated identity access management (IAM) processes and capabilities such as: - Access certification - automating the review of access - Automated access provisioning - allowing users to get access through an automated process - Password self-reset - automating the password reset process if a password is forgotten - Single Sign-On - allows users to sign-on once an get access to multiple assets that would normally require a separate log-on process
		PR.AC-2: Physical access to assets is managed and protected	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3	X	X	1	C2M2 IAM-2a: "Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of	Access to physical assets, although using a different set of technologies, such as biometrics, electronic cards/badges, should be managed similarly to logical access. Employees and contractors should only be given access to facilities that they need to access to complete their job function. Access to operationally sensitive areas such as computer rooms/data centres should be highly restricted. Typical controls include: - Visitor sign-in sheets

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
			· **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 · **GAPP**, 8.2.3				entities are allowed to access the asset, the limits of allowed access, and authentication parameters)" C2M2 IAM-2b: "Access is granted to identities based on requirements" C2M2 IAM-2c: "Access is revoked when no longer required"	- Card access controls - Video monitoring (CCTV) - Review of access - Review of access logs - Bio-metric readers
		PR.AC-3: Remote access is managed	· **COBIT 5** APO13.01, DSS01.04, DSS05.03 · **ISA 62443-2-1:2009** 4.3.3.6.6 · **ISA 62443-3-3:2013** SR 1.13, SR 2.6 · **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20 · **GAPP**, 8.2.2	X	X	1	C2M2 IAM-2a: "Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters)" C2M2 IAM-2b: "Access is granted to identities based on requirements" C2M2 IAM-2c: "Access is revoked when no longer required"	Following the core access control policy for access management, the provisioning of remote access typically includes providing users with remote access via a secure channel such as VPN. Users gaining access remotely are typically required to used enhanced/dual factor authentication such as hardware tokens/fobs.
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	· **CCS CSC** 12, 15 · **ISA 62443-2-1:2009** 4.3.3.7.3 · **ISA 62443-3-3:2013** SR 2.1 · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 · **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16	X	X	1	C2M2 IAM-2d (MIL2): "Access requirements incorporate least privilege and separation of duties principles"	The access control policy should incorporate the principle of least privilege, which requires that the computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	· **ISA 62443-2-1:2009** 4.3.3.4 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8 · **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, SC-7	X	1		C2M2 CPM-3a: "A strategy to architecturally isolate the organization's IT systems from OT systems is implemented"	Isolation of networks to allow the minimal set of channels and services that are required is built into the network architecture. Network segregation is typically achieved by a combination of firewalls and VLANs (Virtual Local Area Networks).
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities	**PR.AT-1:** All users are informed and trained	· **CCS CSC** 9 · **COBIT 5** APO07.03, BAI05.07 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.7.2.2	X	X	1	C2M2 WM-3a: "Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities" C2M2 WM-4a: "Cybersecurity awareness activities occur" Awareness sessions are conducted on a quarterly basis.	Cybersecurity training is provided to all personnel who have cybersecurity responsibilities. Training can consist of: - on-line training - in class training - security awareness campaigns that combine social events with a message concerning - posters, emails newsletter and other media to communicate simple security concepts - phishing campaigns in which the organization is tested to see how many employees fall victim to a simulated phishing attack

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
	consistent with related policies, procedures, and agreements.		· **NIST SP 800-53 Rev. 4** AT-2, PM-13 · **GAPP**, 1.2.10, 5.1.1, 10.2.5					Training should occur periodically. Many suggest quarterly in some form. Training should be conducted as part of the onboarding process of new personnel. A security awareness training policy should exist. HR should be engaged with this process.
		PR.AT-P1: Documentation is developed to explain the organization's personal information policies and procedures to staff and customers	· PIPEDA, Sch1, s.4.1.4, 4.8, 4.9, 4.10 · **GAPP**, 2.0	X	X	3	Internal privacy policies and procedures are documented and displayed (ex. on an intranet, posters), and the consequences of non-compliance with such policies and procedures are communicated to staff. A customer-facing privacy policy is published (ex. website, bill insert, available at office) which addresses the choices available to the individual with respect to their information and provides notice with respect to the consent, collection, use, and disclosure of their customer information.	PIPEDA requires that the organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
		PR.AT-2: Privileged users understand roles & responsibilities	· **CCS CSC** 9 · **COBIT 5** APO07.02, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13 · **GAPP**, 1.2.9	X	X	1	C2M2 WM-1a: "Cybersecurity responsibilities for the function are identified" C2M2 WM-1b: "Cybersecurity responsibilities are assigned to specific people"	"Privileged users are users who are set up as administrators on systems and have a large degree of access to make changes to the system. Privileged use should be managed through a clear set of roles and responsibilities, ensuring that key control processes such as change management adhere too. Some companies restrict privileged access through "fire call" ids. These highly privileged IDs can be used, however only when certain business or system circumstances exist. Privileged use activities, such as adding/deleting or changing users on systems, making configurations changes, turning services on or off are activities that should have significant monitoring. "
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	· **CCS CSC** 9 · **COBIT 5** APO07.03, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** PS-7, SA-9 · **GAPP**, 7.0, 7.2.2, 7.2.4	X	X	1	C2M2 WM-1a: "Cybersecurity responsibilities for the function are identified" C2M2 WM-1b: "Cybersecurity responsibilities are assigned to specific people"	Typically third-party stakeholder will have their responsibilities outlined very clearly in the contractual arrangements that are in place. Third-party stakeholders may sign non-disclosure agreements and acceptable use agreements.
		PR.AT-4: Senior executives understand roles & responsibilities	· **CCS CSC** 9 · **COBIT 5** APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2,	X	X	1	C2M2 WM-1a: "Cybersecurity responsibilities for the function are identified" C2M2 WM-1b: "Cybersecurity responsibilities are assigned to specific people"	The executive committee or the board of directors should be sufficiently aware that cybersecurity is not an "IT issue", that it is a business issue. This should be reflected in board meeting minutes and be a part of board meeting agendas.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
			· **NIST SP 800-53 Rev. 4** AT-3, PM-13 · **PIPEDA**, Sch1, s.4.1 · **GAAP**, 1.1.2					
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	· **CCS CSC** 9 · **COBIT 5** APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, · **NIST SP 800-53 Rev. 4** AT-3, PM-13 · **PIPEDA**, Sch1, s.4.1, 4.7 · **GAPP**, 1.1.2	X	X	1	C2M2 WM-1a: "Cybersecurity responsibilities for the function are identified" C2M2 WM-1b: "Cybersecurity responsibilities are assigned to specific people"	Personnel that deal with physical and information security on a day to day business should have their responsibilities clearly outlined in security operation manuals. Their role and responsibilities may be written in their job description or as part of the letter of employment.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	· **CCS CSC** 17 · **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06 · **ISA 62443-3-3:2013** SR 3.4, SR 4.1 · **ISO/IEC 27001:2013** A.8.2.3 · **NIST SP 800-53 Rev. 4** SC-28 · **PIPEDA**, Sch1, s.4.7 · **GAPP**, 8.2.1	X	X	1	C2M2 TVM-1c: "Threats that are considered important to the function are addressed (e.g., implement mitigating controls, monitor threat status)" C2M2 TVM-2c: "Cybersecurity vulnerabilities that are considered important to the function are addressed (e.g., implement mitigating controls, apply cybersecurity patches)"	Depending on the sensitivity of the data as well as where it resides, data-at-rest should be protected by a number of controls, including: - disk/data encryption - data masking - access permissions
		PR.DS-2: Data-in-transit is protected	· **CCS CSC** 17 · **COBIT 5** APO01.06, DSS06.06 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** SC-8 · **PIPEDA**, Sch1, s.4.7 · **GAPP**, 8.2.1	X	X	1	C2M2 TVM-1c: "Threats that are considered important to the function are addressed (e.g., implement mitigating controls, monitor threat status)" C2M2 TVM-2c: "Cybersecurity vulnerabilities that are considered important to the function are addressed (e.g., implement mitigating controls, apply cybersecurity patches)"	Depending on the sensitivity of the data as well as what networks/channels it is travelling over, it should be protected by a number of controls, including: - secure tunnel encryption - data encryption
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 · **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16 · **PIPEDA**, Sch1, s.4.7	X	2		C2M2 ACM-3a: "Changes to inventoried assets are evaluated before being implemented" C2M2 ACM-3b: "Changes to inventoried assets are logged"	The asset inventory should have sufficient IT and business process to ensure that when assets are formally removed, transferred and disposed of, that the inventory is updated accordingly. A policy or procedure should exist to ensure assets are managed through a formal change management process.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
			· **GAPP**, 8.2.1					
		PR.DS-4: Adequate capacity to ensure availability is maintained	· **COBIT 5** APO13.01 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.12.3.1 · **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5	X	2		C2M2 TVM-1c: "Threats that are considered important to the function are addressed (e.g., implement mitigating controls, monitor threat status)" C2M2 TVM-2c: "Cybersecurity vulnerabilities that are considered important to the function are addressed (e.g., implement mitigating controls, apply cybersecurity patches)"	Typically organizations collect metrics from systems, such as the use of memory, disk space and network speed and throughput. These metrics are trended over time to provide management with a view as for whether sufficient capacity is being met. Capacity is reviewed on a regular basis and sometimes in real-time. As system performance metrics reach their threshold, management will plan to increase capacity through budgeting and planning.
		PR.DS-5: Protections against data leaks are implemented	· **CCS CSC** 17 · **COBIT 5** APO01.06 · **ISA 62443-3-3:2013** SR 5.2 · **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 · **PIPEDA**, Sch1, s.4.7 · **GAPP**, 1.2.7, 8.2.1	X	1		C2M2 TVM-1c: "Threats that are considered important to the function are addressed (e.g., implement mitigating controls, monitor threat status)" C2M2 TVM-2c: "Cybersecurity vulnerabilities that are considered important to the function are addressed (e.g., implement mitigating controls, apply cybersecurity patches)"	Typically organizations use a combination of: - Access policy - Data classification, labelling and handling procedures - Access permissions - Data loss prevention (DLP) tools In order to protect data, management should have a good understanding of where data resides in the organizations. Documentation such as network diagrams and data flow diagrams can assist with this.
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	· **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 · **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** SI-7 · **PIPEDA**, Sch1, s.4.7 · **GAAP**, 8.2.1	2			C2M2 SA-2e (MIL2): "Indicators of anomalous activity have been defined and are monitored across the operational environment"	Typically organisations will have a standard set configurations, often hardened for their systems. Tools can be deployed to identify if those configurations have inadvertently been changed.
		PR.DS-7: The development and testing environment(s) are separate from the production environment	· **COBIT 5** BAI07.04 · **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 4** CM-2	2			C2M2 ACM-3c (MIL2): "Changes to assets are tested prior to being deployed, whenever possible"	These environments are kept separate to ensure that changes to systems made during the development process do not affect the integrity and availability of systems in production. Organizations typically have a change management process that documents these different environments. As part of the change management process, management will have documented a code migration process. Not only should these environments be logically separated through the network architecture, access to the production environment should not be available to developers.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	· **CCS CSC** 3, 10 · **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6	1			C2M2 ACM-2a: "Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly" C2M2 ACM-2b:	Typically organisations will have a standard set configuration, often hardened for their systems. Tools can be deployed to identify if those configurations have inadvertently been changed. Typically organizations have: - Build books - Hardening standards

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
	commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.		· **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10				"Configuration baselines are used to configure assets at deployment"	- Configuration Management database - Change management processes
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	· **COBIT 5** APO13.01 · **ISA 62443-2-1:2009** 4.3.4.3.3 · **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8	3			C2M2 ACM-3d (MIL2): "Change management practices address the full life-cycle of assets (i.e., acquisition, deployment, operation, retirement)"	Typically organizations have a formal system development lifecycle. Popular ones include "waterfall"; "spiral"; "Agile software development"; "rapid prototyping"; "incremental"; and "synchronize and stabilize". This should be formally documented. For cybersecurity organizations should consider: - Using secure coding techniques such as OWASP (Open Web Application Security Project - an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted) - Conducting code review and/or application vulnerability testing - Ensuring the software code repository is protected
		PR.IP-3: Configuration change control processes are in place	· **COBIT 5** BAI06.01, BAI01.06 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10	X	2		C2M2 ACM-3a: "Changes to inventoried assets are evaluated before being implemented" C2M2 ACM-3b: "Changes to inventoried assets are logged"	The objective of change management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service. A change is an event that is: - approved by management - implemented with a minimized and accepted risk to existing IT infrastructure results in a new status of one or more configuration items (CIs) - provides increased value to the business (Increased Revenue, Avoided Cost, or Improved Service) from the use of the new or enhanced IT systems. Typically organisations will have: - a formal change management process - a change approval board
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	· **COBIT 5** APO13.01 · **ISA 62443-2-1:2009** 4.3.4.3.9 · **ISA 62443-3-3:2013** SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 · **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9	X	X	1	C2M2 IR-4a: "The activities necessary to sustain minimum operations of the function are identified" C2M2 IR-4b: "The sequence of activities necessary to return the function to normal operation is identified"	Typically organizations will have: - Tape or electronic vaulting - off-site - a backup schedule indicating (full, differential or incremental backup) - periodic restoration tests
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18	X	X	1	C2M2 ACM-4f (MIL3): "Asset inventory, configuration, and change management policies include compliance requirements for specified standards and/or guidelines" C2M2 RM-3f (MIL3): "Changelogs include	An operations manual should exist to ensure the operating environment for physical assets meet the manufacturer's recommended requirements for operations. In data centres, this could include temperature and humidity control as well as consistent sources of electrical power. The organization may have commercial HVAC systems to maintain cooling. The organization may have UPS and back up generators to maintain consistent power.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
			· **PIPEDA**, Sch1, s.4.7 · **GAPP**, 8.2.1, 8.2.3				information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality)"	
		PR.IP-6: Data is destroyed according to policy	· **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · **NIST SP 800-53 Rev. 4** MP-6 · **PIPEDA**, Sch1, s.4.5.3 · **GAPP**, 5.2.3	X	X	1	C2M2 ACM-3d (MIL2): "Change management practices address the full life-cycle of assets (i.e., acquisition, deployment, operation, retirement)"	When data is no longer required, either for business purposes or compliance reasons, it should be destroyed. Organizations typically have a data archiving and destruction policy that accounts for this. Depending on the sensitivity of the data organizations may have a media handling policy that includes instructions for destroying the media that data once resided on. This might include physical destruction of media or logical overwrites sometime referred to as secure wiping.
		PR.IP-7: Protection processes are continuously improved	· **COBIT 5** APO11.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 · **GAPP**, 8.2.7, 10.2.3	X	3		C2M2 CPM-1g (MIL3): "The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile (TVM-1d)"	To do this, organizations will typically conduct vulnerability and system penetration tests. These can sometimes be done by an external consultant, or internally by their own personnel. Findings reported in the report should be tracked and managed to support a continuous improvement process.
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	· **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4	1			C2M2 ISC-1a: "Information is collected from and provided to selected individuals and/or organizations" C2M2 ISC-1b: "Responsibility for cybersecurity reporting obligations are assigned to personnel (e.g., internal reporting, DOE Form OE-417, ES-ISAC, ICS-CERT, law enforcement)"	As systems are tested and vulnerabilities are identified and reported, should an organization find a weakness that may affect the security of a 3rd parties data, that organization should notify the 3rd party about the vulnerability and what is being done to mitigate the vulnerability? If a breach occurs, the organization should enact breach notification to ensure the 3rd party can take appropriate measure to further secure its assets and data.
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	· **COBIT 5** DSS04.03 · **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 · **NIST SP 800-53 Rev. 4** CP-2, IR-8 · **PIPEDA**, Sch1, s.4.7 · **GAPP**, 1.2.7	X	X	1	C2M2 IR-4c: "Continuity plans are developed to sustain and restore operation of the function"	Typically organizations will have a BCP / DRP plan as well as an incident response plan. The two plans should integrate with an aim to created cyber resilience.
		PR.IP-10: Response and recovery plans are tested	· **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14	X	3		C2M2 IR-3e (MIL2): "Cybersecurity event and incident response plans are exercised at an organization-defined frequency" C2M2 IR-4f (MIL2): "Cybersecurity event and	Typically organizations will conduct disaster recovery exercises to test the availability of systems during a crisis. This should be conducted at least annually. Some organizations also test their security incident response plans through threat scenario and tabletop exercises. This is highly recommended.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
			· **PIPEDA**, Sch1, s.4.7 · **GAPP**, 1.2.7, 8.2.7				incident response plans address OT and IT assets important to the delivery of the function"	
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	· **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4 · **NIST SP 800-53 Rev. 4** PS Family · **PIPEDA**, Sch1 , s.4.7 · **GAPP**, 8.2.1	X	X	1	C2M2 WM-2a: "Personnel vetting (e.g., background checks, drug tests) is performed at hire for positions that have access to the assets required for delivery of the function" C2M2 WM-2b: "Personnel termination procedures address cybersecurity"	This typically includes: - security background checks for new employees - security awareness training as part of onboarding - sign-off on a code of conduct, acceptable use policy - during deprovisioning it includes a termination checklist in which the employee returns assets and is reminded of their obligations to keep information confidential
		PR.IP-P1: Privacy is included in human resources practices (e.g. privacy training)	· **PIPEDA**, Sch1, s.4.1.4 · **GAPP**, 1.2.9, 1.2.10	X	X	1	The onboarding procedure includes privacy training and the privacy policies and procedures are provided as part of the employee handbook or welcome package.	PIPEDA requires that staff be trained about the organization's privacy policies and practices.
		PR.IP-12: A vulnerability management plan is developed and implemented	· **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 · **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2 · **GAPP**, 8.0, 8.2.7	X	3		C2M2 TVM-3a (MIL2): "Documented practices are followed for threat and vulnerability management activities"	A vulnerability management program is in place that tracks vulnerabilities that are specific to the IT assets. Information concerning vulnerabilities to the organizations assets can come from multiple sources including, ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings, internal assessments. Typically organizations deploy an automated vulnerability scanning tool to identify vulnerabilities to their assets.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	· **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4.3.3.3.7 · **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5 · **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5	3			C2M2 ACM-3b: "Changes to inventoried assets are logged"	As part of the organizations asset inventory, a specific maintenance schedule is documented and maintained. This could include specific maintenance instructions from the vendor of the technology asset.
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	· **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 · **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 · **NIST SP 800-53 Rev. 4** MA-4 · **PIPEDA**, Sch1, s.4.7 · **GAPP**, 8.0	2			C2M2 SA-1a: "Logging is occurring for assets important to the function where possible" C2M2 IR-1c: "Cybersecurity events are logged and tracked" C2M2 IAM-2a: "Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and	Activity logs of actions are completed by users from remote locations are reviewed. This could include review of VPN logs and associated event on internal systems that were accessed.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
							authentication parameters)" C2M2 IAM-2b: "Access is granted to identities based on requirements" C2M2 IAM-2c: "Access is revoked when no longer required"	
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· **CCS CSC** 14 · **COBIT 5** APO11.04 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · **NIST SP 800-53 Rev. 4** AU Family	2			C2M2 SA-1a: "Logging is occurring for assets important to the function where possible" C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)"	Activity logs of actions taken on a system are review for malicious behaviour. This could include the misuse of privileged access, failed login attempt and other system events that could be indicative of an attack. The sophisticated organization will automate much of this through the centralized log management solutions combined with security information event monitoring (SIEM). The SIEM will have specific use cases that trigger an alert when certain suspicious behaviour occurs on or across the entities systems.
		PR.PT-2: Removable media is protected and its use restricted according to policy	· **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 2.3 · **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7 · **PIPEDA**, Sch1, s.4.7 · **GAPP**, 8.0	X	X	1	C2M2 IAM-2a: "Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters)" C2M2 IAM-2b: "Access is granted to identities based on requirements" C2M2 IAM-2c: "Access is revoked when no longer required"	Use of USB memory sticks and other removable media such as CD / DVD is restricted. If allowed encryption is used. If the organization uses tape to backup data. The data on the tape is encrypted and stored in a secure off-site facility.
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	· **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** AC-3, CM-7 · **PIPEDA**, Sch1, s.4.7	X	X	1	C2M2 IAM-2a: "Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters)" C2M2 IAM-2b: "Access is granted to identities based on requirements" C2M2 IAM-2c: "Access is revoked when no longer required"	The access control policy should incorporate the principle of least privilege, which requires that the computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
			· **GAPP**, 8.0					
		PR.PT-4: Communications and control networks are protected	· **CCS CSC** 7 · **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7 · **PIPEDA**, Sch1, s.4.7 · **GAPP**, 8.0	X	X	1	C2M2 CPM-3a: "A strategy to architecturally isolate the organization's IT systems from OT systems is implemented"	Isolation of networks to allow the minimal set of channels and services that are required is built into the network architecture. Network segregation is typically achieved by a combination of firewalls and VLANs (Virtual Local Area Networks).
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	· **COBIT 5** DSS03.01 · **ISA 62443-2-1:2009** 4.4.3.3 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4	X	1		C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)"	Monitoring of critical systems is performed and logs are reviewed within 90 days.
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4	1			C2M2 IR-1f (MIL3): "Event information is correlated to support incident analysis by identifying patterns, trends, and other common features" C2M2 IR-2i (MIL3): "Escalated cybersecurity events and declared incidents are correlated to support the discovery of patterns, trends, and other common features" C2M2 IR-3h (MIL3): "Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken"	Event information is analyzed and reviewed against threat advisory services.
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	· **ISA 62443-3-3:2013** SR 6.1 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	2			C2M2 IR-1e (MIL2): "There is a repository where cybersecurity events are logged based on the established criteria"	Monitoring of critical systems is performed and aggregated and logs are reviewed within 90 days.
		DE.AE-4: Impact of events is determined	· **COBIT 5** APO12.06 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4 · **PIPEDA**, Sch1, s.4.7 · **GAPP**, 1.2.6	1			C2M2 IR-2b: "Cybersecurity events are analyzed to support escalation and the declaration of cybersecurity incidents"	Potential business and operational impacts are assessed for every significant event.
		DE.AE-P1 - Policies for receiving and responding to privacy complaints or inquiries are established and such policies are	· PIPEDA, Sch1, s.4.1.4, 4.6, 4.8, 4.9, 4.10	X	X	1	A policy is published (ex. intranet, posters, bill insert) which advises customers that they have access to their personal information for	PIPEDA provides that the individual shall be able to address a challenge concerning privacy compliance. PIPEDA further provides that the information made available shall include: (a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
		communicated to customers	· GAPP, 6.0, 10.0				review and update, and how to contact the entity in the event of a privacy question or complaint.	be forwarded; (b) the means of gaining access to personal information held by the organization; (c) a description of the type of personal information held by the organization, including a general account of its use; (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and (e) what personal information is made available to related organizations (e.g., subsidiaries).
		DE.AE-5: Incident alert thresholds are established	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.2.3.10 · **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8 · **PIPEDA**, Sch1, s.4.7 · **GAPP**, 1.2.7	2			C2M2 IR-2a: "Criteria for cybersecurity event escalation are established, including cybersecurity incident declaration criteria"	The Cyber Security Incident Response Plan includes thresholds, process, and roles and responsibilities.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	· **CCS CSC** 14, 16 · **COBIT 5** DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 · **PIPEDA**, Sch1, s.4.7 · **GAPP**, 1.2.7	X	1		C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)" C2M2 SA-2b: "Operational environments are monitored for anomalous behaviour that may indicate a cybersecurity event"	Monitoring of critical systems is performed and logs are reviewed within 90 days.
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	· **ISA 62443-2-1:2009** 4.3.3.3.8 · **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20 · **PIPEDA**, Sch1, s.4.7 · **GAPP**, 1.2.7	X	2		C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)" C2M2 SA-2b: "Operational environments are monitored for anomalous behaviour that may indicate a cybersecurity event"	Physical monitoring is performed for locations that have critical assets.
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	· **ISA 62443-3-3:2013** SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 · **PIPEDA**, Sch1, s.4.7 · **GAPP**, 1.2.7	1			C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)" C2M2 SA-2b: "Operational environments are monitored for anomalous behaviour that may indicate a cybersecurity event"	Personnel is monitored for access to critical systems. Logs are reviewed within 90 days.
		DE.CM-4: Malicious code is detected	· **CCS CSC** 5 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1	X	1		C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)" C2M2 SA-2b: "Operational environments are monitored for anomalous behaviour that	Malware detection and isolation are performed for critical system environments.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
			· **NIST SP 800-53 Rev. 4** SI-3				may indicate a cybersecurity event"	
		DE.CM-5: Unauthorized mobile code is detected	· **ISA 62443-3-3:2013** SR 2.4 · **ISO/IEC 27001:2013** A.12.5.1 · **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44	2			C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)" C2M2 SA-2b: "Operational environments are monitored for anomalous behaviour that may indicate a cybersecurity event"	Security controls are applied to mobile devices that access critical systems.
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	· **COBIT 5** APO07.06 · **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4 · **GAPP**, 7.0	1			C2M2 EDM-2a: "Significant cybersecurity risks due to suppliers and other dependencies are identified and addressed" C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)" C2M2 SA-2b: "Operational environments are monitored for anomalous behaviour that may indicate a cybersecurity event"	Access points for all third parties with access to critical system environments are monitored.
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 · **GAPP**, 8.0	1			C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)" C2M2 SA-2b: "Operational environments are monitored for anomalous behaviour that may indicate a cybersecurity event"	Critical system environments are monitored for unauthorized personnel and activity.
		DE.CM-8: Vulnerability scans are performed	· **COBIT 5** BAI03.10 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-5	X	1		C2M2 TVM-2e (MIL2): "Cybersecurity vulnerability assessments are performed (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification tools)"	Vulnerability scans are performed for critical system environments at least every 2 years.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	· **CCS CSC** 5 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.4.3.1 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14	X	1		C2M2 WM-1a: "Cybersecurity responsibilities for the function are identified"	The Cyber Security Incident Response Plan includes thresholds, the process, and roles and responsibilities.
			· **ISA 62443-2-1:2009** 4.4.3.2	X	3		C2M2 IR-1d (MIL2): "Criteria are established for	Detection activities comply with all privacy, legal and regulatory requirements.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
		DE.DP-2: Detection activities comply with all applicable requirements	· **ISO/IEC 27001:2013** A.18.1.4 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4				cybersecurity event detection (e.g., what constitutes an event, where to look for events)" C2M2 IR-5a (MIL2): "Documented practices are followed for cybersecurity event and incident response as well as continuity of operations activities" C2M2 TVM-1d (MIIL2): "A threat profile for the function is established that includes characterization of likely intent, capability, and target of threats to the function"	
		DE.DP-3: Detection processes are tested	· **COBIT 5** APO13.02 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.14.2.8 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4	1			C2M2 IR-3e (MIL2): "Cybersecurity event and incident response plans are exercised at an organization-defined frequency"	The detection systems are tested at least annually.
		DE.DP-4: Event detection information is communicated to appropriate parties	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.9 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4	1			C2M2 IR-1b: "Detected cybersecurity events are reported" C2M2 IR-3c: "Reporting of escalated cybersecurity events and incidents is performed (e.g., internal reporting, DOE Form OE-417, ES-ISAC, ICS-CERT)" C2M2 ISC-1a: "Information is collected from and provided to selected individuals and/or organizations"	The Cyber Security Incident Response Plan includes thresholds, the process, and roles and responsibilities. A distributor shall make available information to appropriate parties in a manner that will not compromise the confidentiality of the information and the security of the distributor, but at a level of detail appropriate to inform other participants on cyber security risks and countermeasures. The sharing of infomration should be consisten with the Canadian Cyber Threat Exchange (CCTX) reporting best pracitecs and protocols including the use of Traffic Light Protocol (TLP) for sharing information.
		DE.DP-5: Detection processes are continuously improved	· **COBIT 5** APO11.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14	1			C2M2 IR-3h (MIL3): "Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken" C2M2 IR-3k (MIL3): "Cybersecurity event and incident response plans are reviewed and updated at an organization-defined frequency"	Detection processes are reviewed at least annually and improvements are made where applicable.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed	**RS.RP-1:** Response plan is executed during or after an event	· **COBIT 5** BAI01.10 · **CCS CSC** 18 · **ISA 62443-2-1:2009** 4.3.4.5.1	X	X	2	C2M2 IR-3d (MIL2): "Cybersecurity event and incident response is performed according to	The Response Plan with thresholds, roles and responsibilities, and the process is executed.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
	and maintained, to ensure timely response to detected cybersecurity events.		· **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 · **GAPP**, 1.2.7				defined procedures that address all phases of the incident life-cycle (e.g., triage, handling, communication, coordination, and closure)"	
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	· **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8 · **PIPEDA**, Such 1, 4.1 · **GAPP**, 1.1.2, 1.2.7	X	X	2	C2M2 IR-3a: "Cybersecurity event and incident response personnel are identified and roles are assigned"	The Response Plan with thresholds, roles and responsibilities, and the process is executed.
		RS.CO-2: Events are reported consistent with established criteria	· **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 · **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8 · **PIPEDA**, Such 1, 4.7 · **GAPP**, 1.2.7	X	X	2	C2M2 IR-1a: "There is a point of contact (person or role) to whom cybersecurity events could be reported" C2M2 IR-1b: "Detected cybersecurity events are reported"	The Response Plan with thresholds, roles and responsibilities, and the process is executed.
		RS.CO-3: Information is shared consistent with response plans	· **ISA 62443-2-1:2009** 4.3.4.5.2 · **ISO/IEC 27001:2013** A.16.1.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4	X	3		C2M2 ISC-1a: "Information is collected from and provided to selected individuals and/or organizations" C2M2 ISC-1b: "Responsibility for cybersecurity reporting obligations are assigned to personnel (e.g., internal reporting, DOE Form OE-417, ES-ISAC, ICS-CERT, law enforcement)" C2M2 ISC-1c: "Information-sharing stakeholders are identified based on their relevance to the continued operation of the function (e.g., connected utilities, vendors, sector organizations, regulators, internal entities)"	The Response Plan with thresholds, roles and responsibilities, and the process is executed.
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· **ISA 62443-2-1:2009** 4.3.4.5.5 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 · **PIPEDA**, Such 1, 4.7 · **GAPP**, 1.2.7	X	1		C2M2 IR-3d (MIL2): "Cybersecurity event and incident response is performed according to defined procedures that address all phases of the incident life-cycle (e.g., triage, handling, communication, coordination, and closure)" C2M2 IR-5b (MIL2): "Stakeholders for cybersecurity event and incident response as well as	The Response Plan with thresholds, roles and responsibilities, and the process is executed.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
							continuity of operations activities are identified and involved"	
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	· **NIST SP 800-53 Rev. 4** PM-15, SI-5	X	X	2	C2M2 ISC-1a: "Information is collected from and provided to selected individuals and/or organizations"	The Response Plan with thresholds, roles and responsibilities, and the process is executed.
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	· **COBIT 5** DSS02.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	X	1		C2M2 IR-1e (MIL2): "There is a repository where cybersecurity events are logged based on the established criteria"	Notifications are provided and the highest priority notifications are investigated within 24 hours.
		RS.AN-2: The impact of the incident is understood	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** CP-2, IR-4 · **GAPP**, 1.2.7	X	1		C2M2 IR-2d (MIL2): "Criteria for cybersecurity event escalation, including cybersecurity incident criteria, are established based on the potential impact to the function" C2M2 TVM-1d (MIL2): "A threat profile for the function is established that includes characterization of likely intent, capability, and target of threats to the function"	Potential business and operational impacts are assessed for every significant event.
		RS.AN-3: Forensics are performed	· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · **ISO/IEC 27001:2013** A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-7, IR-4	1			C2M2 IR-3d (MIL2): "Cybersecurity event and incident response is performed according to defined procedures that address all phases of the incident life-cycle (e.g., triage, handling, communication, coordination, and closure)"	Forensics are performed for impactful incidents and events, and adjustments are made to controls as appropriate. Computer Forensics being defined as "the preservation, identification, extraction, documentation and interpretation of computer data." (as defined by Kruse, Heiser in 2002 publication "Computer Forensics: Incident Response Essentials".)
		RS.AN-4: Incidents are categorized consistent with response plans	· **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8 · **GAPP**, 1.2.7	X	2		C2M2 IR-2a: "Criteria for cybersecurity event escalation are established, including cybersecurity incident declaration criteria"	The Response Plan with thresholds, roles and responsibilities, and process is executed.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	· **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4	X	1		C2M2 IR-3b: "Responses to escalated cybersecurity events and incidents are implemented to limit impact to the function and restore normal operations"	High priority incidents are contained and adjustments are made to controls as appropriate.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
			· **GAPP**, 1.2.7					
		RS.MI-2: Incidents are mitigated	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4 · **GAPP**, 1.2.7	X	1		C2M2 IR-3b: "Responses to escalated cybersecurity events and incidents are implemented to limit impact to the function and restore normal operations"	Previous incidents and threat advisory services are reviewed and used to mitigate potential future incidents.
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	· **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5	X	1		C2M2 TVM-2c: "Cybersecurity vulnerabilities that are considered important to the function are addressed (e.g., implement mitigating controls, apply cybersecurity patches)"	High priority vulnerabilities as defined by threat advisory services and/or vendors are addressed and mitigated.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	· **COBIT 5** BAI01.13 · **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 · **GAPP**, 1.2.7	X	X	2	C2M2 IR-3h (MIL3): "Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken"	Subsequent to the execution of the Response Plan within 30 days lessons learned are identified and incorporated into the security controls and Response Plan.
		RS.IM-2: Response strategies are updated	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 · **GAPP**, 1.2.7	X	X	2	C2M2 IR-3h (MIL3): "Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken" C2M2 IR-3k (MIL3): "Cybersecurity event and incident response plans are reviewed and updated at an organization-defined frequency"	Subsequent to the execution of the Response Plan within 30 days lessons learned are identified and incorporated into the security controls and Response Plan.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	· **CCS CSC** 8 · **COBIT 5** DSS02.05, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8 · **GAPP**, 1.2.7	X	X	1	C2M2 IR-3b: "Responses to escalated cybersecurity events and incidents are implemented to limit impact to the function and restore normal operations"	The Formal Recovery Plan is executed upon detection of an applicable event.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	· **COBIT 5** BAI05.07 · **ISA 62443-2-1** 4.4.3.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 · **GAPP**, 1.2.7	X	1		C2M2 IR-3h (MIL3): "Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken" C2M2 IR-4i (MIL3): "The results of continuity plan testing and/or activation are	Subsequent to the execution of the Response Plan within 30 days lessons learned are identified and incorporated into the security controls and Response Plan.

Function	Category	Subcategory	Informative References	Implementation Priority (1 = High, 2 = Med, 3= Low, X = From Lower Risk Profile)			Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
				High Risk	Med Risk	Low Risk Baseline		
							compared to recovery objectives, and plans are improved accordingly" C2M2 IR-3k (MIL3): "Restored assets are configured appropriately and inventory information is updated following execution of continuity plans"	
		RC.IM-2: Recovery strategies are updated	· **COBIT 5** BAI07.08 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 · **GAPP**, 1.2.7	X	X	2	C2M2 IR-3h (MIL3): "Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken" C2M2 IR-3k (MIL3): Cybersecurity event and incident response plans are reviewed and updated at an organization-defined frequency"	Subsequent to the execution of the Response Plan within 30 days lessons learned are identified and incorporated into the security controls and Response Plan.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	· **COBIT 5** EDM03.02 · **GAPP**, 1.2.7	X	X	1	C2M2 RM-1c (MIL3): "Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available"	Upon detection of a significant incident, the appropriate forms of public relations are engaged.
		RC.CO-2: Reputation after an event is repaired	· **COBIT 5** MEA03.02 · **GAPP**, 1.2.7	X	1		C2M2 IR-3d (MIL2): "Cybersecurity event and incident response is performed according to defined procedures that address all phases of the incident life-cycle (e.g., triage, handling, communication, coordination, and closure)"	Upon detection of a significant incident, the appropriate forms of public relations are engaged.
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	· **NIST SP 800-53 Rev. 4** CP-2, IR-4 · **GAPP**, 1.2.7	X	X	2	C2M2 IR-3d (MIL2): "Cybersecurity event and incident response is performed according to defined procedures that address all phases of the incident life-cycle (e.g., triage, handling, communication, coordination, and closure)"	The Recovery Plan with thresholds, roles & responsibilities and the process is executed.

APPENDIX F – PARTICIPANTS

An extensive number of executives, experts and policy makers participated in the projects' workshops and expert interviews throughout 2016. OEB would like to thank the members of the Cyber Security Steering Committee and Cyber Security Working Group Members for providing their thoughtful insights and advisory efforts in relation to developing the Ontario Cyber Security Framework. The OEB is deeply indebted to all of those who have provided their valuable thought-leadership and expertise to this Framework's development.

Table 1 - Cyber Security Steering Committee Members (CSSC)

Hydro One - Rick Haier - Colin Penny	Gowlings - David McFadden
Toronto Hydro - Robert Wong	IESO - Doug Thomas - Ben Blakel
Oshawa PUC - Jayesh Shah	EDA - Todd Wilcox
Hydro Ottawa - Mark Fernandes	University of Toronto - Deepa Kundur
North Bay Hydro - Darren Renaud	Veridian - Falguni Shah
	PowerStream - William Schmidt

Table 2 - Cyber Security Working Group Members (CSWG)

Alectra Utilities / Halton Hills - Indy Butany-DeSouza - Natalie Yeates - Dan Cantwell - Ken Craft	IESO - Jason Hammerschmidt	Oakville Hydro - Wendy Young
Halton Hills - David Smelsky - Kevin Bush	Hydro One - Susan Greenough	Thunder Bay Hydro - David Morden - Dan Gaudette
Energy+ - Heath Higgens - Paul Martinello	Powerstream - Terry Lageer	London Hydro - Mike Flegel
Waterloo North - Marianne Blasman	Toronto Hydro - Martin Loeffler - Preslav Rusev - Kaleb Ruch	Ministry of Energy - Christine Dade
Enersource* - Gia DeJulio - Michael Murphy	Hydro Ottawa - Jojo Maalouf	Peterborough Hydro - Nick Powers
Veridian - Larry Lam	Burlington Hydro - John Matos	Entegrus - Dave Cullen - Hugh Bridgen
EDA - Kathi Farmer - Justin Rangooni	Enbridge Gas / Spectra - Biju Misra - Hugh MacMillan	Union Gas - Patrick McMahon - Gord Doermer - Vanessa Innis - Colleen L'Abbe - Mark Kitchen - Mike Packer - Francois Trofim-Breuer
ErthCorp - David Williams	Cornerstone Hydro Electric Concept Association - Kenneth Robertson	Electrical Safety Authority - Carl Lemp
Renfrew Hydro - Jordy Leavoy	Orangeville Hydro - Amy Long - Suzanne Presseault	

Table 3 – Ontario Energy Board

Stuart Wright	Brian Hewson	Charlie Floriano	Andres Mand	Michael Lesychyn

Table 4 – AESI, RICHTER and DLA PIPER

Doug Westlund	Joe Raso	Stephanie Meyer	Darryl Fraser	Raymond Vankrimpen	Terry McNally	Christina Howitt	Kelly Friedman