ONTARIO ENERGY BOARD

White Paper

Cybersecurity Framework to Protect Access to Electronic Operating Devices and Business Information Systems within Ontario's Non-Bulk Power Assets

June 1, 2017

775 Main Street E
Suite 1B
Milton, Ontario
Canada L9T 3Z3
P · 905.875.2075
F · 905.875.2062

www.aesi-inc.com

This page left intentionally blank.

TABLE OF CONTENTS

Executive Summary 1
1. Overview of the Project 4
1.1. Focus of the White Paper 6
2. The Problem 7
2.1. From the LDC Perspective 7
2.1.1. Threat Landscape 7
2.1.2. The Attack Surface 11
2.1.3. Ontario Bulk to Non-Bulk Interconnections 14
2.1.4. Great Lakes Power Transmission (GLPT) 18
2.1.5. Summary 18
2.2. Security Gaps and Issues Related to the Bulk to Non-Bulk Interfaces 19
2.3. Other Problems 23
2.3.1. Current and Emerging Standards and Guidelines 23
2.3.2. Environmental Scan 28
2.3.3. Privacy 38
2.3.4. Cybersecurity Insurance 42
2.4. From the OEBs Perspective 42
3. The Cybersecurity Framework Solution 45
3.1. Concept 45
3.2. Risk Profile Tool 46
3.3. NIST Controls and Privacy Principles 50
3.4. Initial Achievement Level 51
3.5. Metrics and Reporting 52
4. Implementation Plan 58
4.1. Support 62
4.2. Reporting 62
4.3. Evolution – coincident with maturity levels 63
5. Conclusions and Recommendations 66
Appendix A: Glossary of Terms and Abbreviations 67
Appendix B: Table of Figures 73
Appendix C: Informative References 74
Appendix D: Security Controls and Risk Profiles Requirements, Stage 1 75

AESI

White Paper:
Cybersecurity Framework

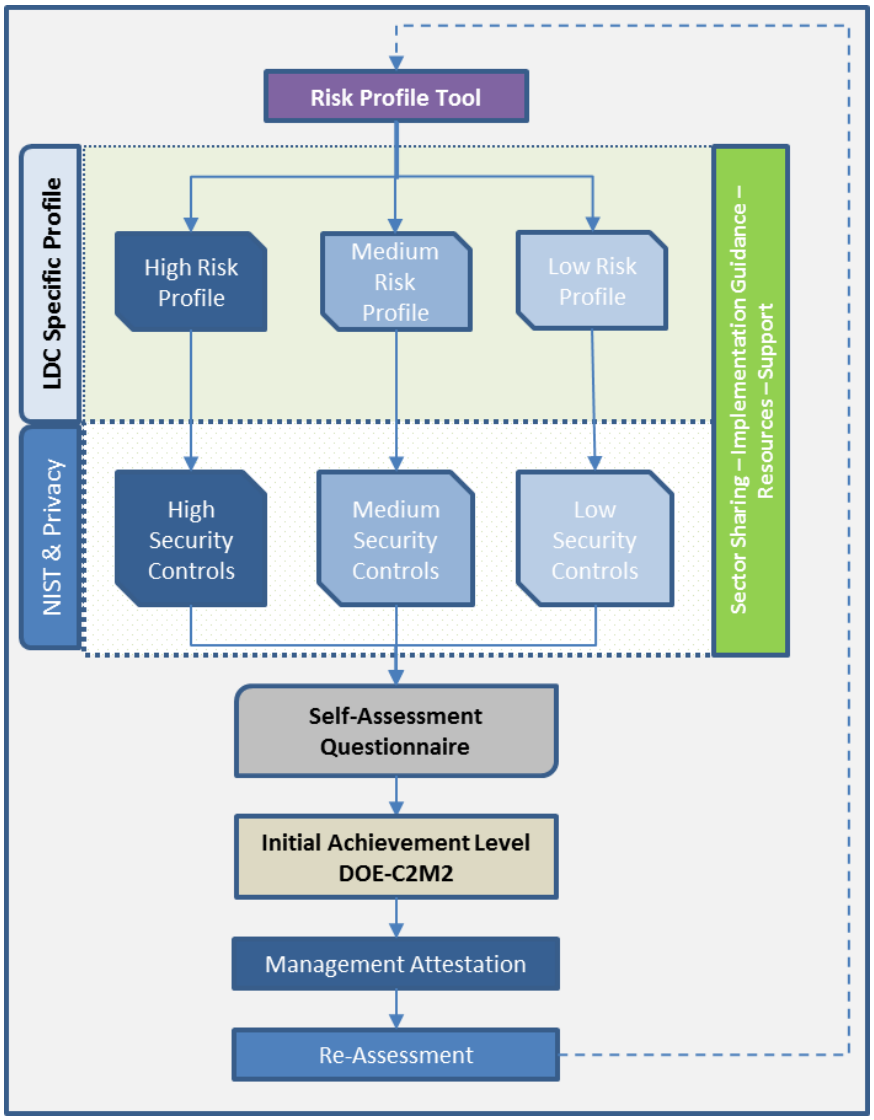
775 Main Street E, Suite 1B · Milton, Ontario · Canada L9T 3Z3 P · 905.875.2075 F · 905.875.2062 www.aesi-inc.com

EXECUTIVE SUMMARY

This White Paper is the culmination of five (5) Discussion Papers commissioned by the Ontario Energy Board (EB-2016-0032) to aid in the development of a regulatory Cyber Security Framework to provide oversight and validation of the Cyber Security measures taken by distributors and transmitters for non-bulk assets in Ontario for the protection of consumer privacy and the electricity system infrastructure. The intent of the series of Discussion Papers was to gauge the knowledge of Ontario distributors (also referred to as Local Distribution Companies (LDCs)) on the topics outlined in each Discussion Paper, and to provide preliminary research findings and recommendations to inform the recommendations presented in this White Paper. The Discussion Papers capture current activities, identify implementation risks and provide guidance towards the important elements and themes of the potential Cyber Security Framework.

Through extensive iteration with the Cyber Security Steering Committee and the Cyber Security Working Group and both qualitative and quantitative research methods, the Consultant Team (AESI Inc., DLA Piper and Richter) developed an Ontario LDC-specific Cyber Security Framework. The Cyber Security Framework uses the NIST Cybersecurity Framework as the cornerstone of the Framework, and uses insights from the Department of Energy (DOE) - Cybersecurity Capability Maturity Model (C2M2)[1], Privacy by Design and input from a wide variety of stakeholders. Conceptually, the Cyber Security Framework can be visualized as seen in Figure 1.

Figure 1: Ontario LDC Cybersecurity Framework, Stage 1



The Cyber Security Framework begins with a Risk Profile Tool, developed with input from the Cyber Security Working Group and specifically tailored to the inherent risks in Ontario's LDC community. The Risk Profile Tool allows each Ontario LDC to be categorized based on their inherent risk, in an objective fashion. Based on size, maturity and capability, Ontario LDCs will have different inherent risk profiles. Each risk profile will require that a varying degree of security controls be applied to ensure an adequate level of

[1] Cyber Security Capability Maturity Model (C2M2) Program

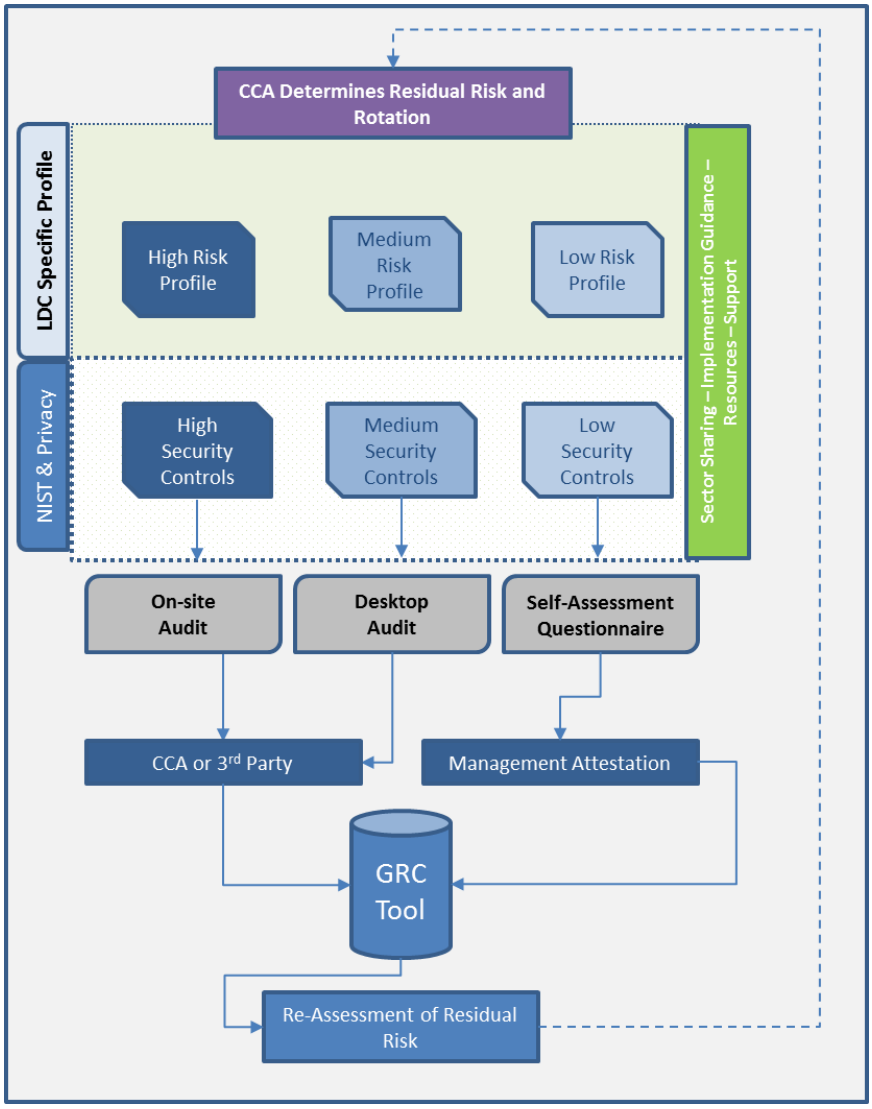
confidence in the entity's cybersecurity posture. Once a risk profile for the LDC is established using the tool, the security and privacy controls (based on the NIST Cybersecurity Framework[2], with the injection of Privacy by Design) are defined for High, Medium and Low (baseline) entities which is described in detail in Appendix D.

The implementation of these security controls are surrounded by dual resources for the LDC community. Recognizing that resources, both financial and human, are restrained in the Ontario market, a Cyber Security Exchange sponsored by the industry is proposed to provide the technical resources and information, such as implementation guidance and support, awareness training, and 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). The Cyber Security Exchange is important for the implementation of the security controls so that efforts are not multiplied across the industry. At the same time, the culture of sharing, already inherent in the Ontario LDC community, is encouraged and nurtured with this new requirement.

To monitor the progress, a metrics reporting scheme was also developed. Since an LDC's control environment and principles of reporting form an integral part of the compliance and assurance regime, the reporting elements outlined under the Cyber Security Framework should be considered as 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 compliance.

The initial reporting activities that LDCs will employ during "Stage 1" would include the completion of a self-assessment questionnaire (SAQ) to validate compliance with the security controls (NIST) subcategory elements. In addition, some organizations with very specific business models may find that some requirements do not apply. As responses will be linked to NIST subcategories, integration with the overall Framework will occur and provide the LDC with a roadmap for areas in which the organization is strong, in need of improvement, or void of a current reasonable control. The SAQ reporting will result in a "Management Attestation / Certification". This attestation should be provided by the LDC CEO, ensuring that

Figure 2: Ontario LDC Cybersecurity Framework, Stage 2: Components / Index for High/Medium/Low



[2] Cyberframework

appropriate attention and focus is undertaken to address both determining current compliance and the required follow-up remediation activities. Retention of this information should conform to information audit requirements.

By following the proposed Framework during Stage 1, the LDCs will have adopted a baseline of security controls, commensurate with their inherent risk profiles, with a maturity implementation level of 1 (MIL1) according to C2M2's implementation levels. During Stage 2, to evolve to a higher level of maturity, the LDCs will need to begin having their security controls evaluated as depicted in Figure 2. 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.

The Framework Version 1.0, as designed, has been built on industry best practices and authoritative standards and has been designed specifically for LDC / non-bulk system operators. Extensive feedback from the OEB's Cyber Security Working Group and Cyber Security Steering Committee was obtained and built into the Framework. The Framework has a phased implementation schedule and a significant amount of sector sharing and guidance will be applied to the process to assist the LDCs / non-bulk system operators. For the LDCs, specific guidance is provided to provide clarity of responsibilities and implementation. For the Ontario Energy Sector as a whole, we will expect to see an improved cyber security posture as the Cyber Security Framework is implemented.

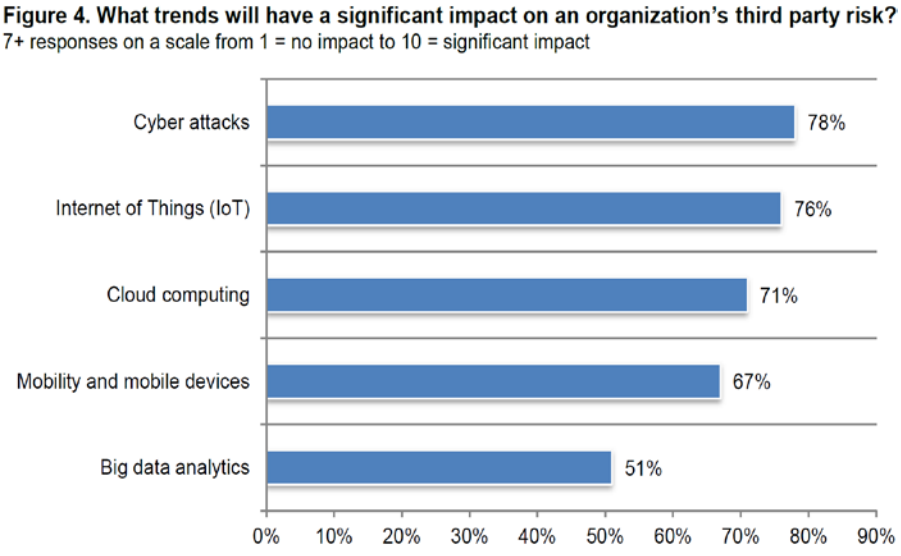
1. Overview of the Project

The Ontario Energy Board (OEB) regulates transmitters and distributors (also referred to as Local Distribution Companies (LDCs)) that operate Ontario's transmission and electricity distribution networks. Ontario's electricity transmitters and LDCs represent significant capital investments supplying electricity to large industrial and commercial customers and millions of consumers throughout the province, with total assets in the tens of billions.

In January, 2011, the OEB initiated a consultation with stakeholders on the Implementation of Smart Grid in Ontario (EB-2011-0004) which is one of five guiding objectives of the Board set out by the *Ontario Energy Board Act, 1998*.[3] The consultation examined technical issues, and the policies required to resolve them, as well as recommendations for future consideration. Both cybersecurity and privacy were identified by the working group as key issues that should be addressed as an increased threat to the industry.[4] As well, preliminary research identified that a considerable amount of existing material for cybersecurity and privacy issues developed in other industries could be drawn upon by the OEB. From 2013 to 2015, a Smart Grid Advisory Committee[5] existed to provide ongoing assistance to the OEB for issues related to the smart grid in Ontario.

The Ontario Energy Board has initiated this cyber security consultation to develop a policy and reporting requirements that provide a measureable assurance from Ontario's natural gas and electricity entities that they are taking appropriate action with respect to their security, reliability and privacy obligations. To create its baseline for assurance, the OEB can be guided by standards, models and best practices. However, while there is a plethora of voluntary cyber security standards, models and frameworks which have developed over the last several years, none have been specifically tailored for the non-bulk electricity sector. Further, none of the available frameworks put much emphasis on protecting customer information, as opposed to IT and OT infrastructure. In order to achieve the OEB's privacy and security objectives, the OEB is facilitating the development and implementation of a sector driven cyber security framework that leverages generic frameworks and models, to be the basis for assurance.

Figure 3: Ponemon – Impact of Third Party Risk



In early 2016, the OEB initiated a new policy consultation to continue and further the work started with the original consultation. Recognizing that the cyber threat was rapidly increasing and building upon the smart grid work, the OEB wanted to identify industry standards and best practices in order to establish a sector-wide framework for continuing to protect personal information and the reliable operation of the smart grid.[6] The OEB recognized that the risk of security breaches and exposure to cyber-attacks within the electrical energy sector have grown substantially with the implementation of smart

[3] Ontario Energy Board Act, 1998
[4] Staff discussion paper8.pdf
[5] www.ontarioenergyboard.ca/oeb/Industry/RegulatoryProceedings/PolicyInitiativesandConsultations/EnergyIssuesRelating toSmartGrid/SmartGridAdvisoryCommittee
[6] www.ontarioenergyboard.ca/oeb/Industry/RegulatoryProceedings/PolicyInitiativesandConsultations/PrivacySmartGrid EB-2016-003229

grids/digital grid, including net-metering and self-generation i.e., MicroFit. As well, the increasing demand for more real-time data exchange between entities within the province, and real-time data being requested by other business units within the LDCs to support their business functions, have broadened the cyber-attack surface for an LDC. The increasing use of automation, different communication networks, and the use of wireless networks, data flows, hand-held electronic devices, and the Internet of Things (IoT) creates attack vectors that have not been considered in the past. As a survey completed by Ponemon Research in May 2016 indicates[7], Figure 3, internet connected devices present an increasing risk via new attack vectors.

To assist in the development of a sector-driven common Cyber Security Framework for Ontario's non-bulk power sector, an industry Working Group was established and held its first meeting on June 30, 2016. The Cyber Security Working Group was composed of OEB staff, distributors and industry participants, including Burlington Hydro, Cornerstone Hydro Electric Concepts (CHEC), Electrical Distributors Association, Electrical Safety Association, Enbridge, Energy+ Inc., Enersource, Hydro Mississauga, Inc., Entegrus, ERTH Corp, Halton Hills Hydro, Horizon Utilities, Hydro One, Hydro Ottawa, London Hydro, Milton Hydro, Oakville Hydro, Orangeville Hydro, Oshawa PUC Networks Inc., Peterborough Utilities, PowerStream Inc., Renfrew Hydro, Thunder Bay Hydro, Toronto Hydro, Veridian. Representatives of the Ontario Ministry of Energy, the OEB, IESO, Electrical Safety Authority, and the natural gas utilities participated in the Cyber Security Working Group as stakeholders.

The Cyber Security Working Group received direction from the Cyber Security Steering Committee made up of executive representatives from the OEB as well as Enbridge, Gowlings, Hydro One, Hydro Ottawa, IESO, North Bay Hydro, Oshawa PUC Networks Inc., PowerStream Inc. and Toronto Hydro.

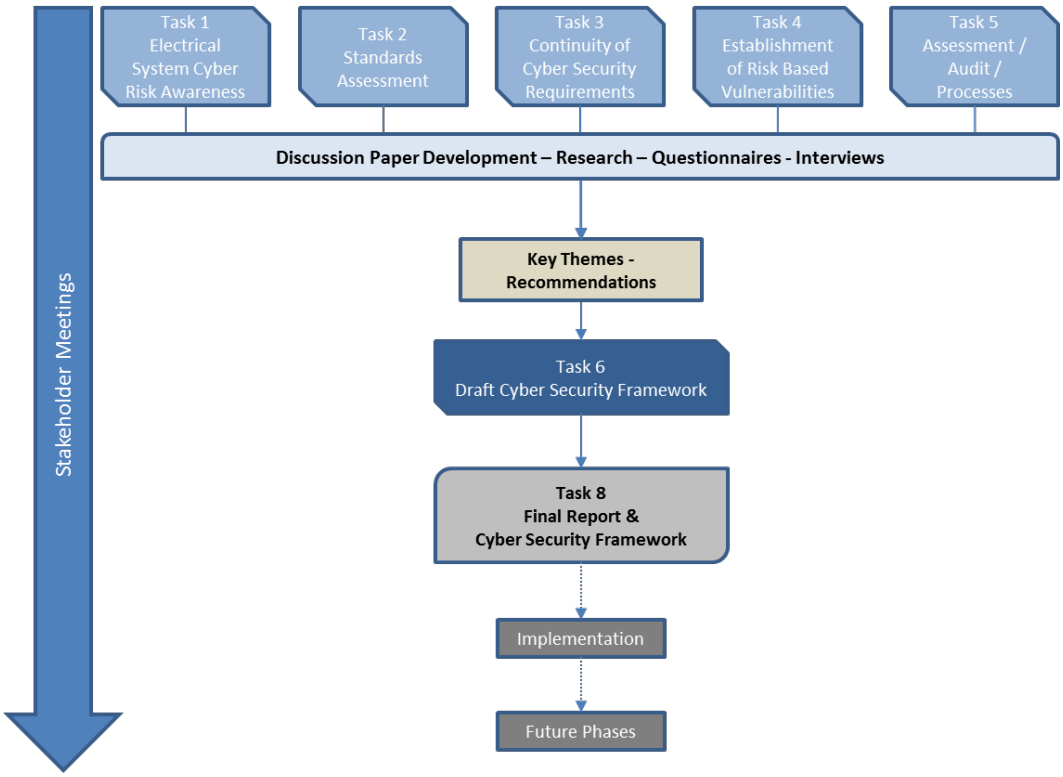
As part of the initiative, the OEB retained the services of the AESI Inc., DLA Piper and Richter (collectively known as the "Consultant Team") to:

1. Assess the state of current and proposed security standards, guidelines, and best practices applicable to the non-bulk electricity system infrastructure and distribution business systems.
2. Identify attack vectors and probabilities of successful penetration using established industry and Canadian and American government agencies' security risk methodologies.
3. Assist and guide OEB staff in stakeholder meetings/engagements, including those with senior executives, in the development of a security Framework for the non-bulk electricity system infrastructure and distribution business systems, including:
    a. Identification of the current security risks including cyber ("Security Risks") within Ontario's non-bulk transmission assets and distribution operating and business systems, including smart metering and AMI (Electricity System Infrastructure).
    b. Development of a security Framework to be applied across the sector.
    c. Recommendations for the application of existing and emerging standards, guidelines and best practices that would mitigate the risk levels identified to ensure that the OEB achieves its legislative mandate.
    d. Establishment of a maturity model to be applied within the Framework.
    e. Development of a risk assessment approach to guide sector entities.
    f. Development of a security verification methodology and reporting requirements to validate the efficacy of participants' security programs.
4. Provide recommendations for countermeasures that can be developed, including regulatory frameworks and policies, licensing requirements, potential changes to legislation, industry awareness and training, and assessments/auditing procedures.
5. Provide recommendations on how to incorporate customer information protection strategies into the regulatory Framework, such as with the use of Privacy by Design.

[7] 2016 Ponemon Study Tone At The Top And Third Party Risk-Final.pdf

To achieve the goals of the OEB project, the list of activities described above was divided into a series of Discussion Papers that would culminate in a White Paper and draft Cyber Security Framework with supporting tools and processes. An overview of the project is as follows:

Figure 4: Project Overview



The Discussion Papers rely on the insights of the Cyber Security Working Group using a variety of tools and methodologies to gather the information, as well as qualitative research. As part of the OEB's larger mandate, one can view each Discussion Paper as a weather vane for the current state of activities in the Ontario LDC community as well as an introductory view on practices in similar environments. Going forward, the OEB requires a systematic risk-based approach to ensure that cost-efficient protection, including consumer privacy, is seamless and consistently applied across the entire non-bulk electrical energy sector. The goal of this series of Discussion Papers is to support the OEB in the process of developing a regulatory Framework to provide oversight and validation of the adequacy of measures taken by distributors and transmitters for non-bulk assets.

1.1. Focus of the White Paper

This White Paper is the culmination of the five (5) Discussion Papers commissioned by the OEB to aid in the development of a regulatory Cyber Security Framework to provide oversight and validation of the Cyber Security measures taken by distributors and transmitters for non-bulk assets in Ontario for the protection of consumer privacy and the electricity system infrastructure. The intent of the series of Discussion Papers is to gauge the knowledge of Ontario LDCs on the topics outlined in each Discussion Paper, and to provide preliminary research findings and recommendations that inform the recommendations presented in this White Paper. The Discussion Papers capture current activities, identify implementation risks and provide guidance towards the important elements and themes of the potential Cyber Security framework.

The White Paper is structured to present the current state (The Problem) and the proposed future state (The Solution) incorporating elements from both the LDCs perspective and the OEBs perspective. This holistic

approach provides a compelling view that the recommendations presented are the best available to all parties within the current cost allocation models, appetite for change and compelling need to change privacy and security cultures and behaviors.

2. THE PROBLEM

2.1. From the LDC Perspective

2.1.1. Threat Landscape

Cybersecurity threats to LDCs are real. An Energy sector example of a recent and significant attack occurred January 2016. The Computer Emergency Response Team of Ukraine (CERT-UA) confirmed that a power outage across several western Ukrainian regions was a result of a cyber-attack. The attack left more than 57 power stations in a blackout state.[8] Even though some US experts indicated that the control systems in Ukraine were more secure than some in the US, in the end they still were not secure enough. Workers logging remotely into the SCADA network, that controlled the grid, were not required to use two-factor authentication[9], which allowed the attackers to hijack their credentials and gain crucial access to systems that controlled the breakers.[10]

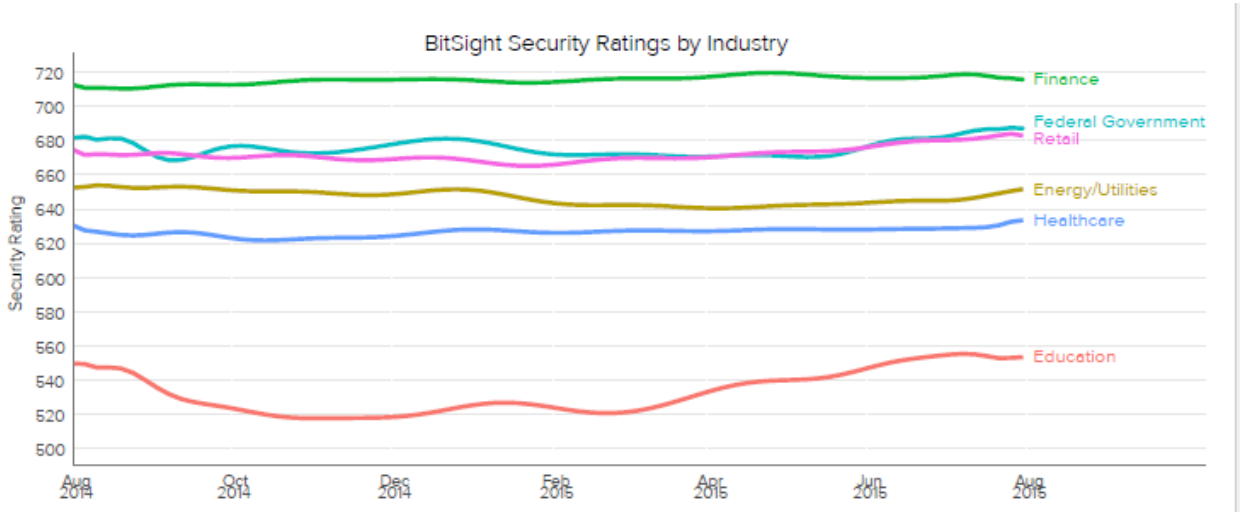
According to a 2015 Global State of Information Security® survey conducted by PricewaterhouseCoopers (PwC), there has been an increase in security incidents that are attributed to service provider and contractors and former partners, 23% and 45% respectively.[11]

One of the biggest issues with vendors is that they may secure their systems (although this greatly varies from vendor to vendor), but they look to the utility to secure the interconnections and each system as a whole. A holistic perspective is required by LDCs to protect the entire system.

In comparison to other industry sectors such as finance, government and retail, the energy and utilities sector has some improvements to make. The Third Annual BitSight Insights Industry Benchmark Report (September 2015) indicated that the energy and utility sector was performing lower than finance, government and retail.

[8] ISACA Whitepaper, “The Merging of Cybersecurity and Operational Technology”, July 2016
[9] Two-factor authentication (also known as 2FA) is a method of confirming a user's claimed identity by utilizing a combination of two different components. Two-factor authentication is a type of multi-factor authentication.
[10] Wired, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid”, Kim Zetter, March, 2016
[11] PricewaterhouseCoopers, 2015, Managing Cyber Risks in an Interconnected World. Key Findings From The Global State of Information Security Survey

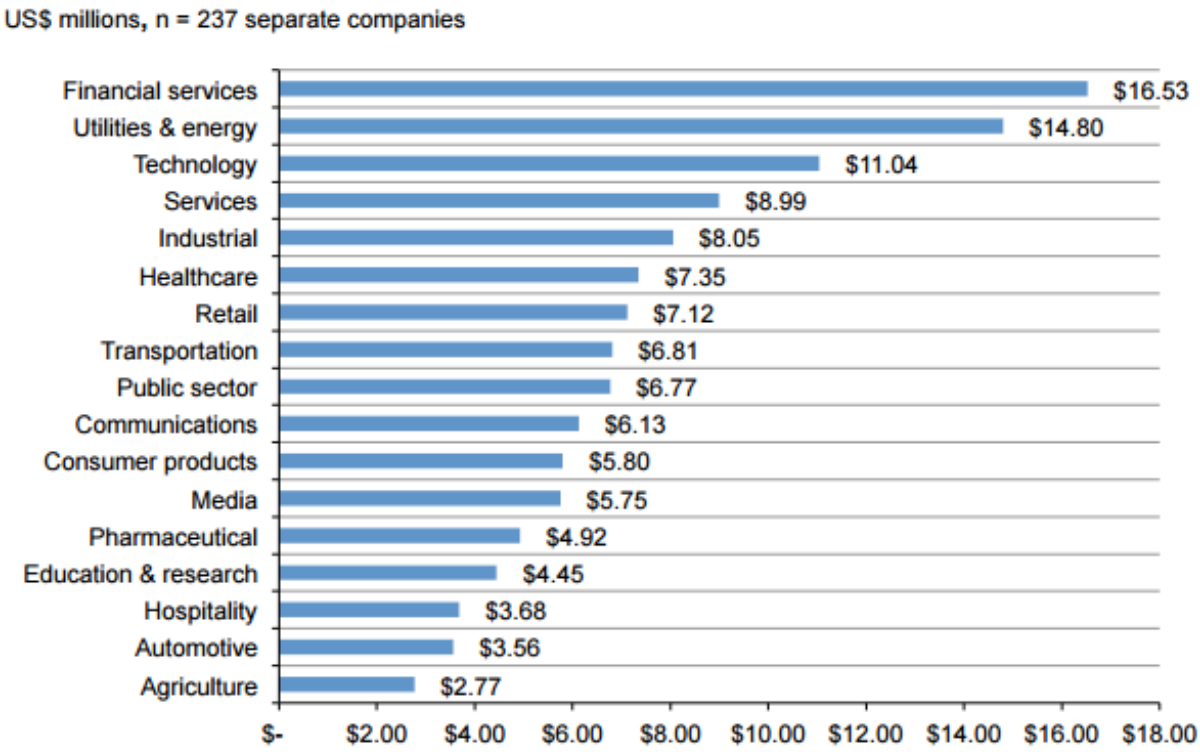
Figure 5: BitSight Insights Industry Benchmark Report[12]



The cyber threat problem for the energy sector is further elaborated in a 2016 Cost of Cyber Crime Study & the Risk of Business Innovation by the Ponemon Institute. The study, which looked at 237 different companies across various industries, showed that the energy and utilities sector experience $14.8 million per company of average annualized loss due to cybercrime. This was the second highest industry average, only to be outpaced by the finance industry.

[12] Figure 1 Third Annual BitSight Insights Industry Benchmark Report (September 2015)

Figure 6: Cost of Cyber Crime[13]



The United States Department of Energy (DOE) realizes the importance of cyber resilience for energy delivery systems through allocating funds and resources to combat the issues. It also recognizes the implications of the convergence of IT and OT and has provided extensive guidance to the industry.

Most early SCADA system designs did not anticipate the security threats posed by the integration of advances in computers and communication such as off-the-shelf software and operating systems, public telecommunication networks, and the Internet. Energy delivery systems have become more productive and efficient, but the energy sector is faced with an unprecedented challenge in protecting systems against cyber incidents and threats.[14]

Current Threat and Risk Landscape

For the Discussion Paper for Task #4, we examined the threat and risk landscape from three main sources:

- **Environmental scan** of over 150 vulnerability assessments of utilities in North America conducted over the past five (5) years.
- **Survey** sent to members of OEB Cyber Security Working Group (Cyber Security Working Group) conducted mid-August 2016 with results provided on August 26, 2016. The survey included questions concerning LDCs' risk assessment processes and the inclusion of cyber-risk in those processes.
- **Research** using industry recognized sources such as ISACA, Gartner, Info-Tech, US-CERT, Foresters and others, as cited, along with a point-of-view directed at identifying strategies for risk-based vulnerability management.

From these sources five main themes became evident:

[13] 2016 Cost of Cyber Crime Study & the Risk of Business Innovation by the Ponemon Institute
[14] Cybersecurity for energy delivery systems

Theme #1 - Miscellaneous errors

- The most significant threat to the industry is miscellaneous errors carried out by employees. This includes security breaches resulting from a lack of knowledge or misconstrued assumptions about security as well as misconfiguration. Examples of this include:
  - Delivery errors: Employees sending emails or documents to the wrong recipient
  - Publishing errors: Employees publishing information to forums, websites or portals that should be held in confidence
  - Gaffe: Firewall rule is misconfigured due to lack of knowledge or expertise

Theme #2 - The implications of the convergence of IT and OT

- Many basic security vulnerabilities are further exacerbated by the convergence of Information Technology (IT) and Operational Technology (OT). IT refers to the business / corporate systems while OT refers to the specific critical infrastructure operator systems such as control systems, substation systems, etc. Often OT systems are not secured to the same standard as IT systems due to different reasons such as lack of security in the original design. SCADA vendors have remote access for support and monitoring which leads to vulnerability, and SCADA networks are not monitored for security. The lack of network segmentation between IT and OT networks can also present security risks if controls are not in place.

Theme #3 – Human Resource Challenges

- LDCs of all sizes will need to start locating and retaining top cyber security talent while prioritizing current staff capabilities to deal with cyber security related issues. Once prioritized there may be difficulty resourcing and retaining talent with the skills and talent needed to manage cybersecurity threats especially in remote areas. Most small/medium LDCs per the Cyber Security Working Group survey have two to five (2-5) IT resources at most with the majority with two (2) IT resources not dedicated to cyber security issues.

Theme #4 - Third party access

- LDCs typically have a large (and typically growing) number of third parties that access their systems. Third party access is often not managed with the same focus as internal access. Third parties may not adhere to the same level of cyber security controls. An organization's security is only as strong as its weakest link. An organization's security is only as strong as its weakest link, and often the third parties are the weakest link. In addition, third parties represent a significant number of attack vectors into the LDC.

Theme #5 - Security tools that Detect, Respond and Recover not widely used

- This is an area that was also brought up by members of the Cyber Security Working Group through discussions. The research shows that much of the concentration of security controls has been on preventative measure, such as the implementation of security policies, firewalls, passwords and encryption. To date, LDCs on the whole have not deployed tools such as intrusion detection / intrusion prevention systems that can assist the LDC in detecting, responding and recovering from a cyber-attack. This ability is a key component of cyber resilience. The NIST Cybersecurity Framework addresses these aspects of cybersecurity.

Future Trends

A 2016 Industry Cybersecurity Threat Briefing prepared by Booz Allen[15] which analyzed 295 Industrial Control System breaches that the US Department of Homeland Security responded to in 2015 indicated the following emerging attack Vectors:

[15] Industry Cybersecurity Threat Briefing prepared by Booz Allen, Industrial Cybersecurity threat briefing

- **Ransomware** – The report cited three (3) recent examples in which ransomware were used to infect machines on the corporate networks of organizations in the energy sector:
  - April 25, 2016 – Board of Water & Light, Michigan
  - January 25, 2016 – Israeli Electricity Authority
  - Early 2016 – American Electric Power's corporate network

  The report warns that although ransomware has normally targeted corporate networks and has held corporate data ransom, it is very likely that future ransomware will be designed to hold industrial control systems ransom too.
- **Lack of expertise** – Another insight resulting specifically from the January 25, 2016 ransomware incident on the Israeli Electricity Authority illustrated the lack of education and awareness in the general public concerning cyber-attacks and how to categorize them. This incident took a few computers off-line at the Israeli Electric Authority, but did not affect any systems of electrical companies that maintain the electrical grid in Israel. In fact, the Israeli Electric Authority "is a government authority charged with providing utility services, setting tariffs, regulation and oversight of the electricity market in Israel."[16] It has no direct connection to systems that maintain the electrical grid in Israel. The media hype surrounding the calls over a "server cyber-attack" in this instance only created a disservice to the public and illustrates the "lack of expertise in the quantity required alongside the type of data needed to validate and assess all of the true attacks on infrastructure while appropriately classifying lesser events."[17]
- **SCADA Access as a Service –** The report indicated that a trend in Selling Access as a Service (SAaaS) to compromised industrial control systems (ICS) first appeared on the black market in 2015. While it recognized that demand for SAaaS was still low, it did indicate that there would be interest from terrorist and activists groups looking to create havoc or deliver a message.
- **Rootkit for PLCs –** an article posted on Dark Reading[18] on September 15, 2016 described a new attack on programmable logic controllers (PLCs). The attack was revealed at the Black Hat Europe conference. The title of the presentation was "Ghost in the PLC: Designing An Undetectable Programmable Logic Controller Rootkit". While SCADA systems have historically been the target of attack (e.g. Stuxnet), this emerging focus is on lower levels of the system. At this level attacks become much more difficult to detect. These attacks involve targeting the PLC runtime software to compromise the I/O peripherals. Because of the rudimentary nature of PLCs and the low overhead of the attack, traditional methods of detecting the attack, such as monitoring power usage, have proven ineffective. Because the PLC rootkit compromises low-level components of a PLC system and it is able to infect PLC manufactured by almost any vendor, it should be considered a cross-platform PLC threat.

In summary, as new technologies emerge and evolve, so too will the threats. Historically, technology vendors in the operational technology space have not embedded strong security measures into their solutions. Furthermore, hackers will continue to find new avenues of attack, even against existing systems which means that LDCs need to be increasingly vigilant. This was further recognized during discussions with the Cyber Security Working Group, calling for a centralized Cyber Security Exchange where information concerning weaknesses in technologies along with solutions could be shared.

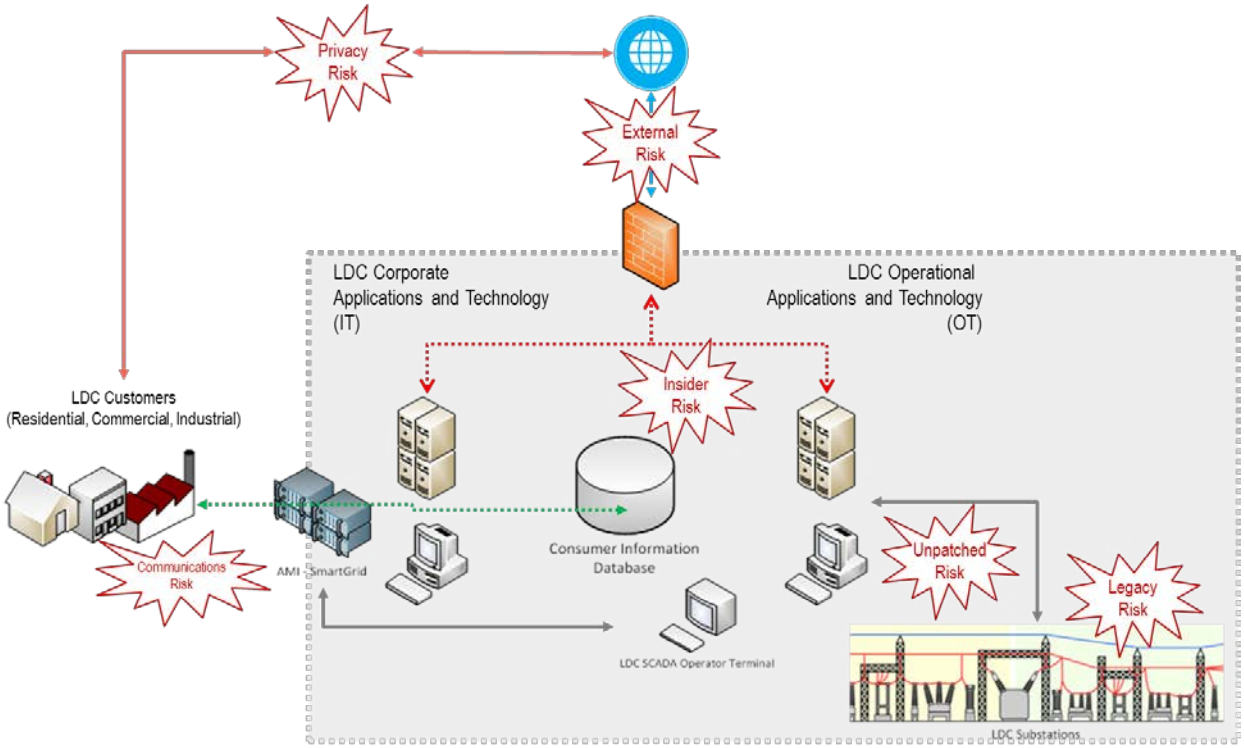
2.1.2. The Attack Surface

In cyber security, "Attack Surface" is a term used to reference the potential attack points. "Attack vectors" are the means used to exploit the attack surface. The aim for all entities is to minimize the attack surface and the attack vectors. Taking the perspective of an LDC, the following diagram illustrates the typical cyber-attack surface and

[16] Electricity Authority (Israel)
[17] Context for the claim of a cyber-attack on the israeli electric grid
[18] Researchers create undetectable rootkit

risks associated with the IT and OT aspects of the LDC. With increasing automation (e.g. AMI, distribution automation, OT automation in general) the attack surface for LDCs is growing.

Figure 7: LDC Attack Surface Vulnerabilities

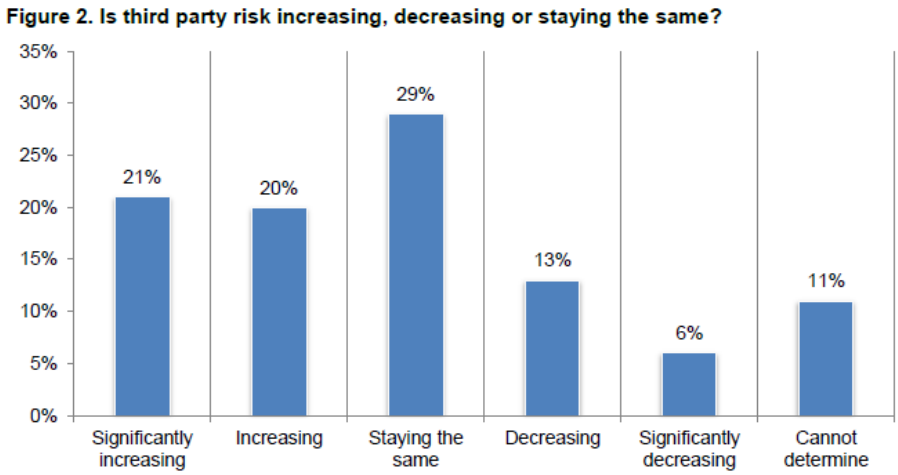


Third Parties

In North America, grid operators have had a trusted view of their "grid neighbours" such as transmission operators, generation operators, ISOs, etc. in which they do not think that strong security controls are required. But in the world of Cyber Security, there needs to be an untrusted viewpoint for effective protection. This means that all external parties to the LDC should be considered untrusted at all times. Connections and information exchange should only happen under strict access control arrangements. Some LDCs have done this and also requested that their third party suppliers abide by the LDC's Security Policy. Given that the grid operators have worked in a trusted mode for over one hundred years, this is a cultural perspective that needs to be addressed. The Framework developed from this project will give the LDCs the vehicle to align access control and security philosophies.

For each LDC, there can be an extensive number of third party interconnections. For example, one mid-sized LDC has 17 third parties that have access to its systems in some shape or form. Clearly, access control needs to be implemented for these interconnections. It is expected that the third party risks will be further assessed in Phase 2 of this project. As a survey completed by Ponemon Research in

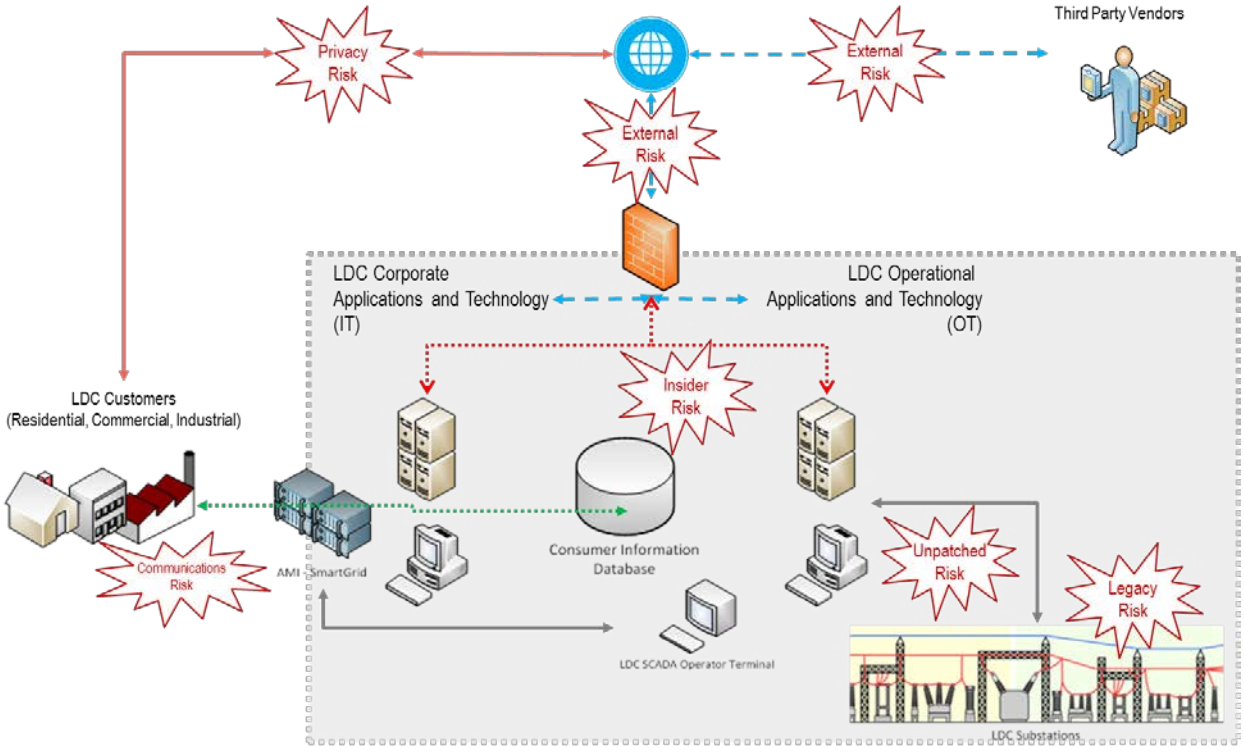
Figure 8: Ponemon Third Party Risk



May 2016[19], Figure 8 indicates, third party risk is increasing and becoming a higher priority to mitigate than before for many organizations.

The following diagram illustrates the additional attack vectors coming into the LDC from the third parties. The magnitude of the risk from these attack vectors is a function of the number and type of third party interconnections.

Figure 9: Additional Third Parties Attack Vectors



And lastly, supply chain, asset management and vendor management issues can impact the bulk to non-bulk systems just as any of the above risks. These will be further identified and analyzed in Phase 2 of the project.

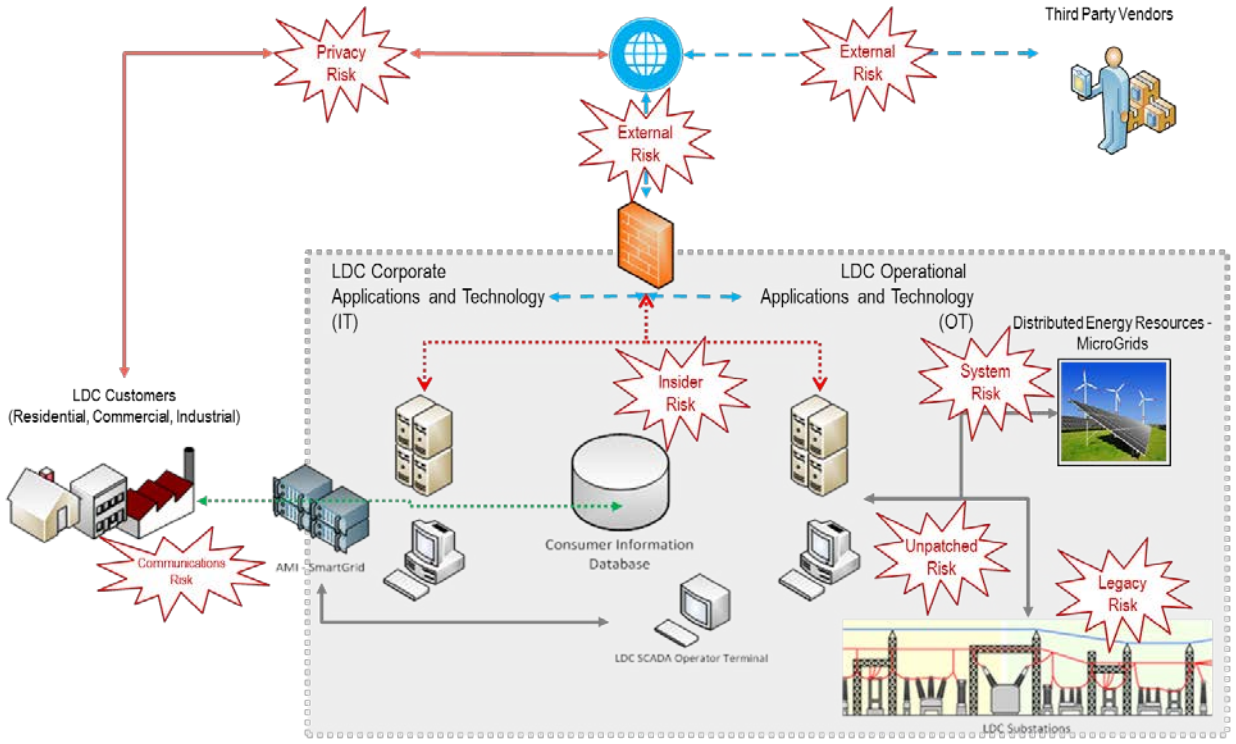
Distributed Energy Resources (DERs) / Microgrids

Within the non-bulk system there will be an increasing proliferation of distributed energy resources / microgrids. These systems present various forms of attack vectors, especially when control systems are involved with the distributed generation / microgrid implementation. For LDCs that are planning to implement such systems, they should implement a defense-in-depth[20] security solution (i.e. layers of security), and ideally implement that at the start. Cyber Security can be much more effective if implemented as a foundational set of elements, as opposed to using a "bolt-on" vs "security designed in" approach afterwards.

[19] 2016 Ponemon Study Tone At The Top And Third Party Risk-Final.pdf

[20] The idea behind defense in depth is to manage risk with diverse defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense will hopefully prevent a full breach. This principle is well known, even beyond the security community; for example, it is a famous principle for programming language design: Defense in Depth: Have a series of defenses so that if an error isn't caught by one, it will probably be caught by another.MacLennan, Bruce. Principles of Programming Languages. Holt,Rinehart and Winston, 1987. Defense in Depth

Figure 10: DERs and Microgrids – Additional Attack Vectors



2.1.3. Ontario Bulk to Non-Bulk Interconnections

This section addresses Ontario's bulk to non-bulk interconnections from the perspective of potential security gaps and attack vectors.

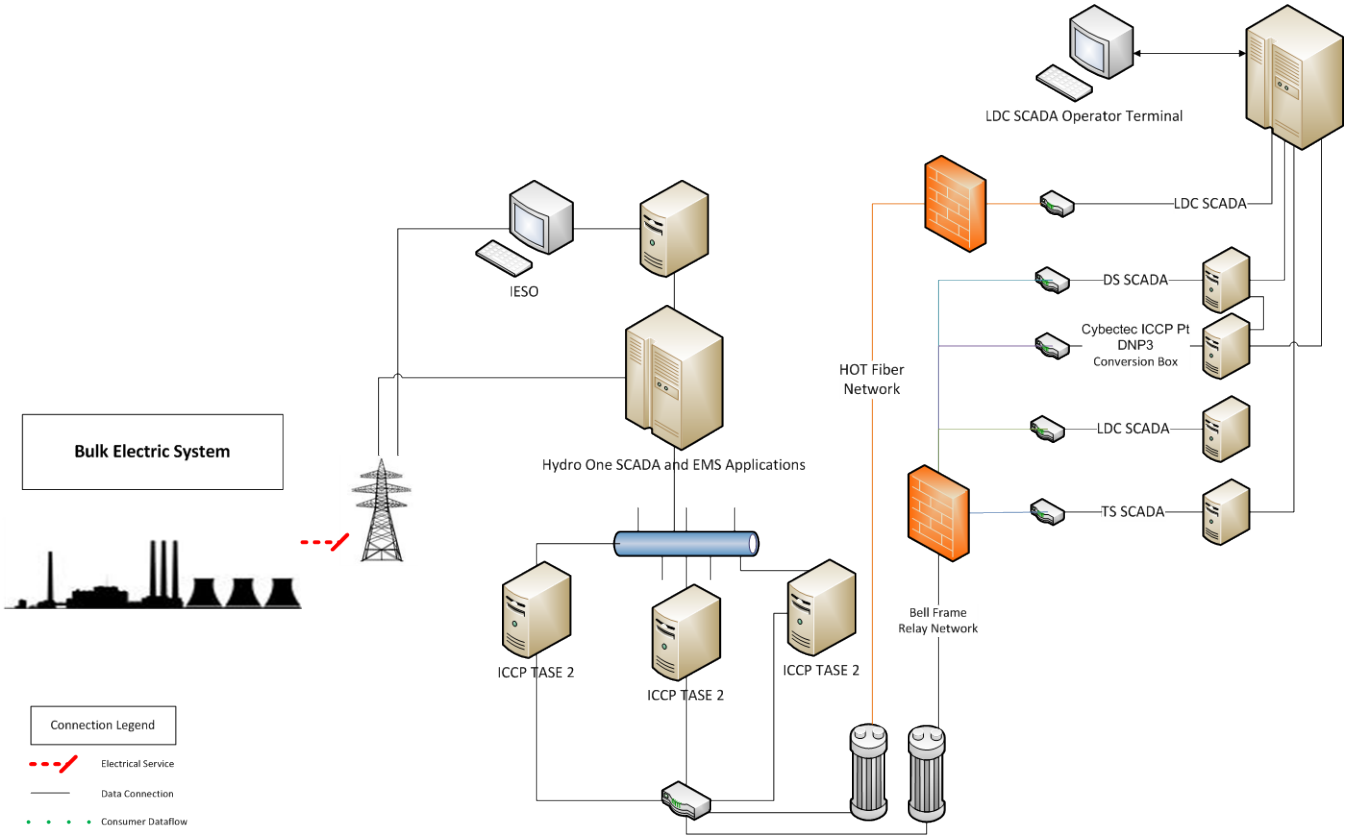
Environmental Scan

In Ontario, Hydro One Networks Inc. (HONI) has approximately 29,000 km of transmission lines which represents approximately 97% of the transmission lines in the province. Great Lakes Power Transmission Inc. (GLPT) has approximately 560 km of transmission lines which represents approximately 1.5% of the transmission lines in the province. As of October 31, 2016, Hydro One completed the purchase of Great Lakes Power Transmission and it will begin to operate under the name Hydro One Sault Ste. Marie in early 2017 and will continue to operate as a standalone licensed transmitter. Accordingly, for the purposes of this analysis, we will review the non-bulk interconnections with HONI and for clarity view GLPT as a separate entity in the interim.

Hydro One Networks Inc. (HONI)

HONI has both Inter-Control Center Communications Protocol (ICCP) and Transformer Station (TS) interconnections with the non-bulk system. TSs reduce voltage to distribution levels. ICCP is used between HONI's control centres and LDC control systems for control system data and grid monitoring. There are approximately 45 ICCP connections between HONI and the LDCs.

Figure 11: ICCP Topology



ICCP is an IEC 60870-6/TASE.2 sanctioned protocol and was developed to enable data exchange over Wide Area Networks between utility control centers, Independent System Operators (ISOs), Regional Transmission Operators (RTOs), and Generators. ICCP itself does not provide an authentication mechanism. Encryption is included in the Secure ICCP version of the standard which was identified as part of the DOE's Roadmap to Achieve Energy Delivery Systems Cybersecurity project.[21]

In a separate initiative, Sandia National Laboratories developed a comprehensive report entitled Secure ICCP Integration Considerations and Recommendations that is a very useful reference document for securing ICCP connections[22].

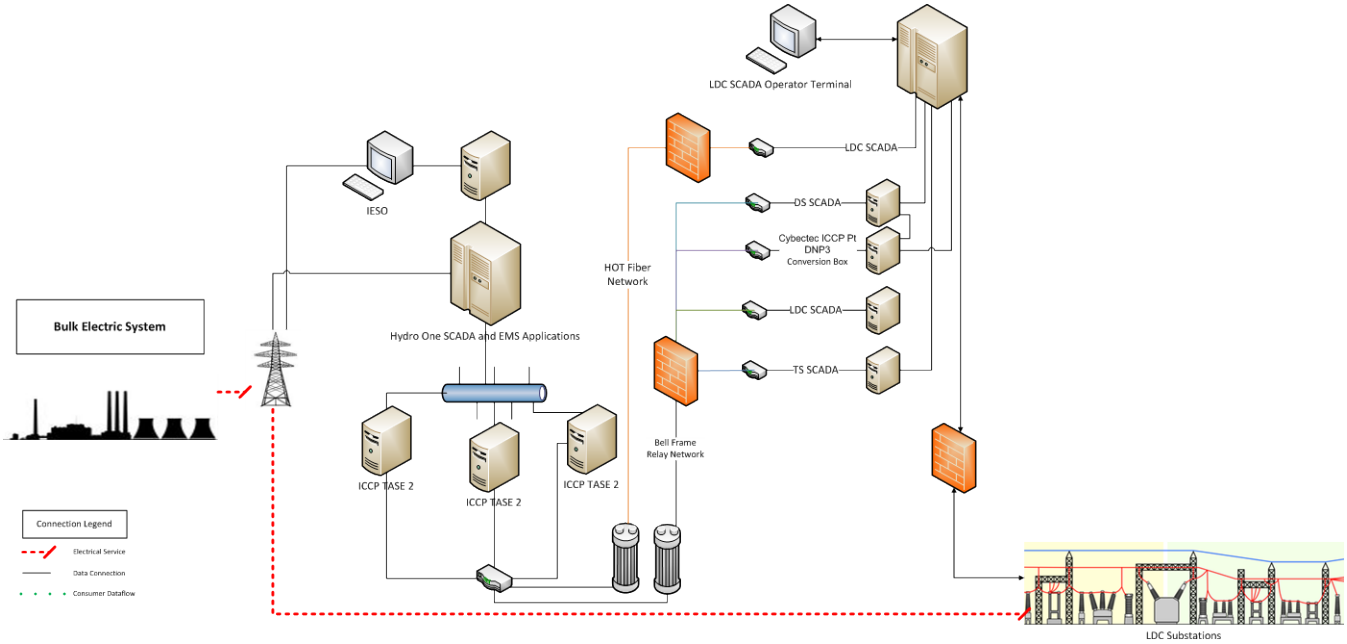
The Sandia report provides for the following recommendations in implementing ICCP connections:

- Network administrators should negotiate Service-Level Agreements (SLAs) that provide appropriate Quality of Service (QoS) for ICCP data streams.
- Utility sites that will not transition rapidly to Secure ICCP should consider using OpenSSL, IPSec, and data link encryption to provide inter-node data security for standard ICCP communication.
- Use a flat Public Key Infrastructure (PKI) Certificate Hierarchy for single-company domains and a tiered hierarchy for multiple-company domains.

HONI also has TS connections with the LDCs as shown in the following visual.

[21] Roadmap to Achieve Energy Delivery Systems Cybersecurity project.pdf
[22] Secure ICCP Integration.pdf

Figure 12: HONI TS Connection



HONI operates the bulk high voltage system that serves LDCs and HONI has a number of transmission connected customers, but the HONI transmission business does not typically connect with the end-user. LDCs or Hydro One Distribution typically take power from the transmission system that is stepped down in voltage level and distribute the power through the urban and rural communities to the residential, commercial and industrial end-users. Based on this, there are typically four scenarios for delivering power to the end-user:

Number	Type	Description	Potential Cyber Vulnerabilities
1	Direct	The end-user is directly connected to the transmission system via a transmission level substation	Wholesale meter – custody transfer grade ITS HONI/Customer Communication
2	LDC	The end-user is an LDC and is directly connected to the transmission system via an LDC-owned transmission level substation	LDC Communications to HONI via RTU LDC Communications to IESO LDC/Customer Communications
3	HONI/LDC	The end-user is an LDC and is connected to the transmission system via a HONI owned transmission level substation. HONI supplies the LDC using some or all of the distribution level feeders	LDC Communications to HONI via RTU HONI Communications to IESO

Number	Type	Description	Potential Cyber Vulnerabilities
4	Embedded	The end-user is an LDC and is connected to the transmission system via a HONI owned transmission level substation and HONI owned feeders. The LDC is only assigned to a fraction of a distribution feeder. There are other loads on the feeder in addition to the LDC	HONI Communications to IESO HONI/Customer communications

From this table, we can identify a number of unique cyber vulnerabilities:

- Wholesale meters and custody transfer applications
- HONI/LDC communications (DNP3[23] per TIR)
- HONI/IESO communications (DNP3 over MPLS[24] per Market requirements)
- LDC/IESO communications(DNP3 over MPLS per Market requirements)
- HONI/End-user communications (DNP3 per TCA)

Although DNP3 is a public and open protocol with its architecture readily available, it is referenced in IEEE 1379-2000 which recommends a set of best practices for implementing SCADA Master to RTU/IED communications. IEEE 1379 also includes encryption as well as other practices to enhance the security of the protocol.

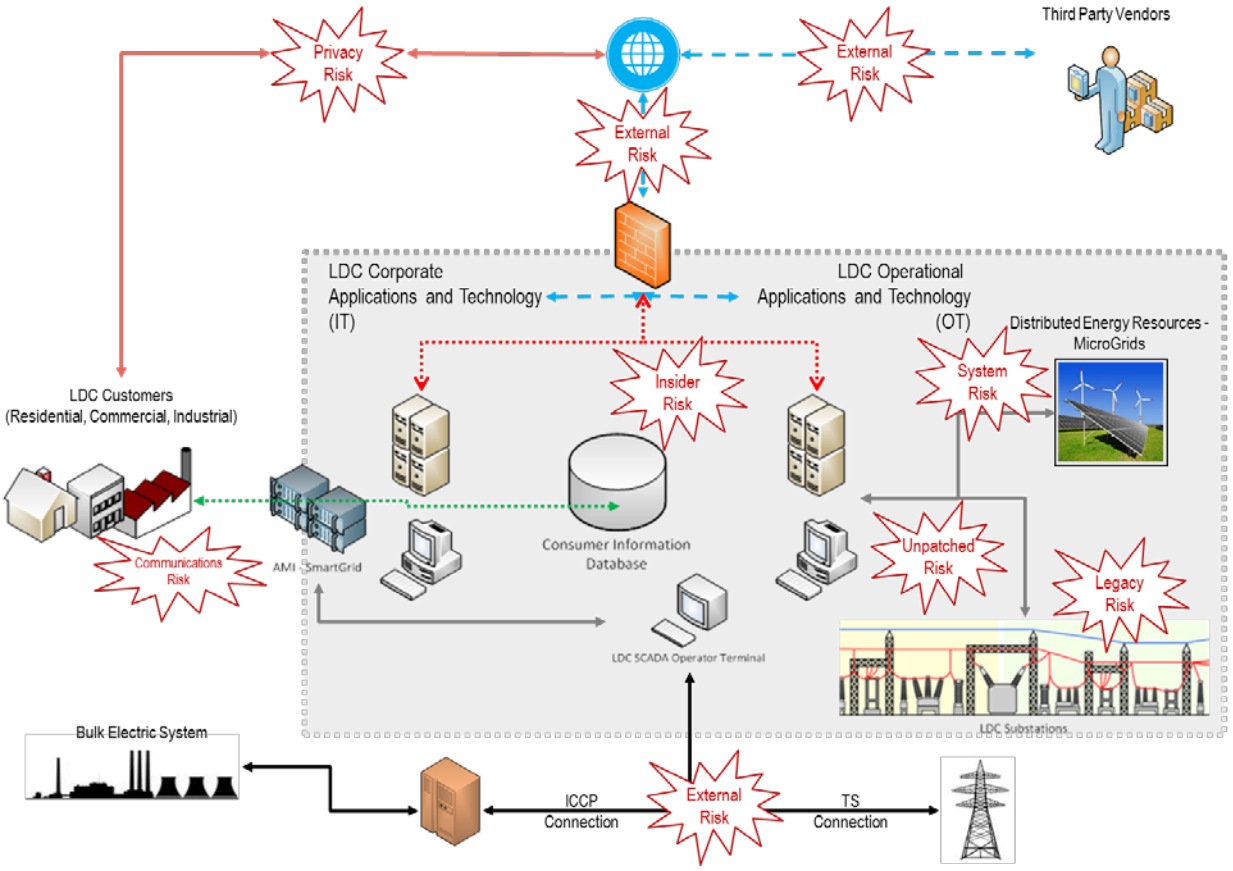
Physical security is also an important requirement of the overall security envelope. At the TS level this is no different. For example, local equipment can be operated, breakers can be tripped and lines can be isolated. To go one step further, transfer trips could be initiated or existing serial protocols could be analyzed, representing risks to the LDC. Also, there are potential risks associated with Hydro One Operating Schedules which require further research.

The following figure illustrates the additional attack vectors to an LDC from the ICCP and TS connections previously described:

[23] DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies. Usage in other industries is not common. It was developed for communications between various types of data acquisition and control equipment. It plays a crucial role in SCADA systems, where it is used by SCADA Master Stations (aka Control Centers), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). It is primarily used for communications between a master station and RTUs or IEDs. ICCP, the Inter-Control Center Communications Protocol (a part of IEC 60870-6), is used for inter-master station communications.

[24] Multiprotocol Label Switching (MPLS) is 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.

Figure 13: Additional Bulk System Vulnerabilities



2.1.4. Great Lakes Power Transmission (GLPT)

GLPT has the following interconnections:

- ICCP connections to Brookfield and HONI
- MPLS (a form of Wide Area Network communications) to IESO
- Serial DNP3 connection to two wind farms and a steel company

With respect to the non-bulk system, GLPT has one TS interconnection with the Sault Public Utilities Commission (PUC) Solar Park.

HONI has been successful in the acquisition of GLPT, it is expected that the GLPT interconnections will conform to HONI's standards. This should be monitored as it impacts the LDCs.

2.1.5. Summary

As with all utilities, LDCs have a considerable cyber-attack surface. There are additional cyber-attack vectors from the bulk system via the ICCP links and the TS interconnections.

Recommended industry best practices should be applied to secure the ICCP link at the LDC side by the LDC. Access control, authentication and encryption should also be considered. The ICCP link should also be secured at the IESO or HONI side using industry best practices.

The non-ICCP TS interconnections are typically implemented by Hydro One using DNP3. These DNP3 links should be secured at the customer side by Hydro One, as they own the equipment, and also by the customer as they own the end devices generating the information. HONI should have accountability for verifying that all links are secure, including verification of the direct transmission connected customers.

IESO connections are typically implemented over the MPLS communication network using 16 bit DNP3. The IESO coordinates installation of and maintains the MPLS network. Equipment typically consists of a DNP3 device, an MPLS router and modems.

Should Hydro One and other BES contributors wish to consider the continued use of DNP3 as a communications protocol, then they should consider implementing the security practices outlined in IEEE1379-2000, which could be overlaid onto the NIST Cybersecurity Framework Protect function.

2.2. Security Gaps and Issues Related to the Bulk to Non-Bulk Interfaces

There are gaps in the NERC CIP standards that apply to the bulk system. The primary gaps that affect the non-bulk system are a) the nature and focus of the NERC CIP standards; and b) minimal controls for Low Impact Bulk Electric Systems. These are described below.

The nature and focus of the NERC CIP standards is on large assets, the implementation of the cyber and physical security operational and procedural controls on the identified and categorized BES Cyber Systems at the entity's facilities (Control Centers, Transmission and Generation assets) with reliability as the overriding objective. Also, the fundamental premise for the NERC CIP standards is compliance. It has been widely understood that an entity can be compliant with the NERC CIP standards but not necessarily secure. With the focus on large assets and compliance, the NERC standards do not address other important issues such as privacy, safety, business risk or brand / reputational risk.

With the focus on individual assets, the NERC CIP standards do not include detection or protection mechanisms for coordinated attacks. With daily advancements in hacking technology and practices, coordinated attacks are prevalent and can lead to significant damages.

The NERC CIP standards in their current form exclude communications. This is one of the largest gaps in the NERC CIP standards that can affect the non-bulk systems. Any communications links, such as ICCP between the LDCs and the bulk system, are not addressed in the NERC CIP standards, and therefore the appropriate levels of security controls may not be applied.

As described in Discussion Paper #2, the NERC CIP standards are applied to the Bulk Electric System (BES) Cyber Systems commensurate with the Impact rating of that system. Low Impact calls for the least amount of security controls and only includes the following:

> **Section 1.** Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).
>
> **Section 2.** Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any.
>
> **Section 3.** Electronic Access Controls: Each Responsible Entity shall:
>
> **3.1** For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access; and
>
> **3.2** Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

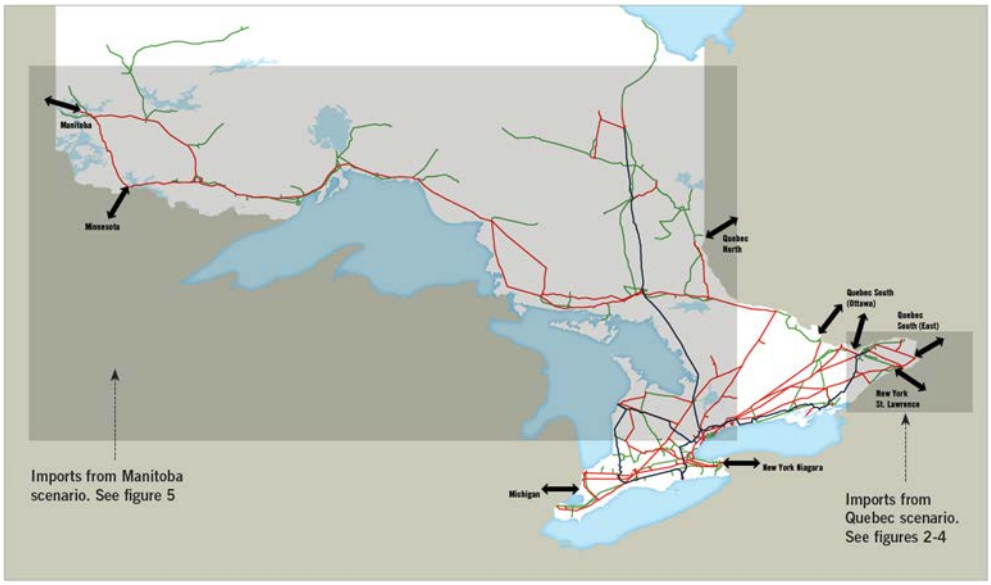
4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security CIP-003-6 — Cyber Security — Security Management Controls Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

It can be seen that the NERC CIP standards do not necessarily guarantee that the bulk system that interconnects with the LDC will be secure.

The IESO also has interconnections with both the bulk and non-bulk systems in Ontario[25].

Figure 14: IESO Interties



And lastly, supply chain issues can impact the bulk to non-bulk systems just as any of the above risks. These will be further identified and analyzed in Phase 2 of the project.

[25] Intertie Report 20141014.pdf

Results from Cyber Security Working Group Meeting #3

The review of the environmental scan as well as the technical research on connection types revealed that the level of awareness of these issues might not be at the top of an LDCs IT priority list. In order to understand in greater detail the level of domain knowledge, the Cyber Security Working Group was engaged as part of the review of Discussion Paper #3. During the Cyber Security Working Group meeting on October 5th, 2016, three (3) subgroups of the Cyber Security Working Group were asked to discuss and respond to the following questions:

- Provide your perspective on Distributed Energy Resources (DERs) / Microgrids and the Bulk System Interconnections.
- Discuss and comment on communication and implementation considerations with respect to the Bulk System Interconnections.

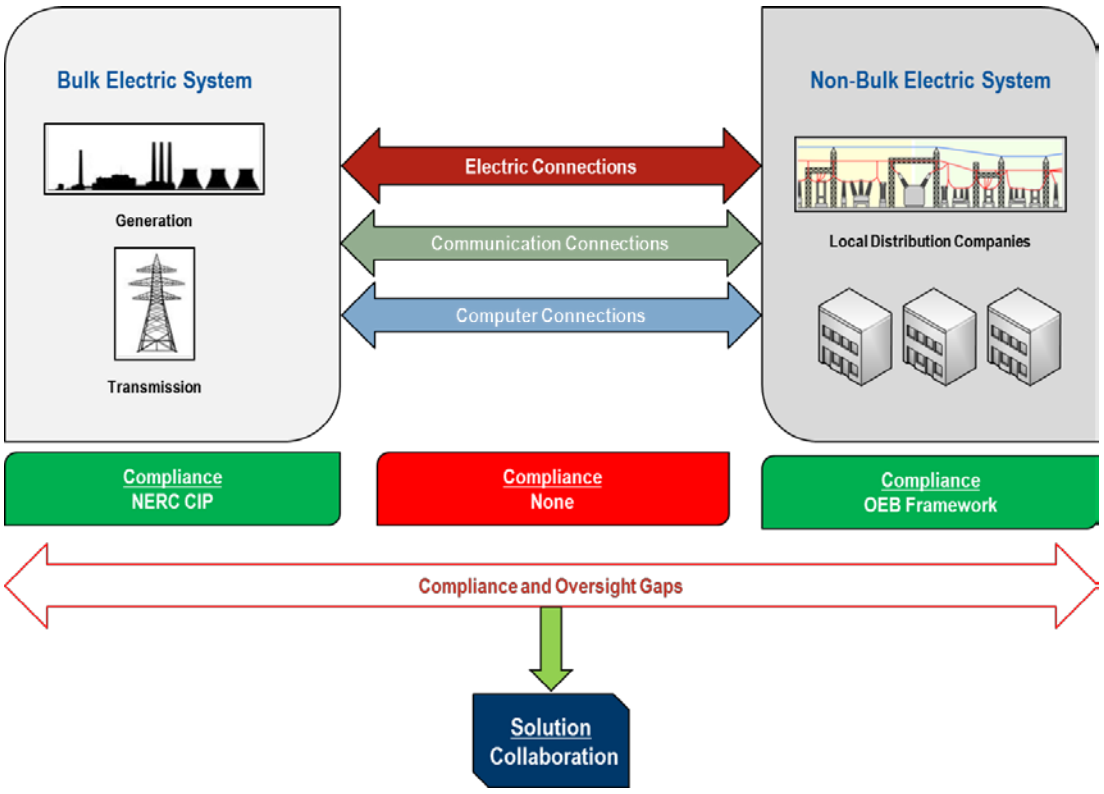
Regarding core issues with respect to DERs / Microgrids and the Bulk System Interconnections, the Working Group stated that all agreements are operational in nature and do not include cyber or physical security. It was also stated that mapping data flows is critical and that a standard reference architecture is required.

In the area of communication and implementation, the Working Group stated that more communication in regularly scheduled sessions between the LDCs, HONI and the IESO is required.

Summary

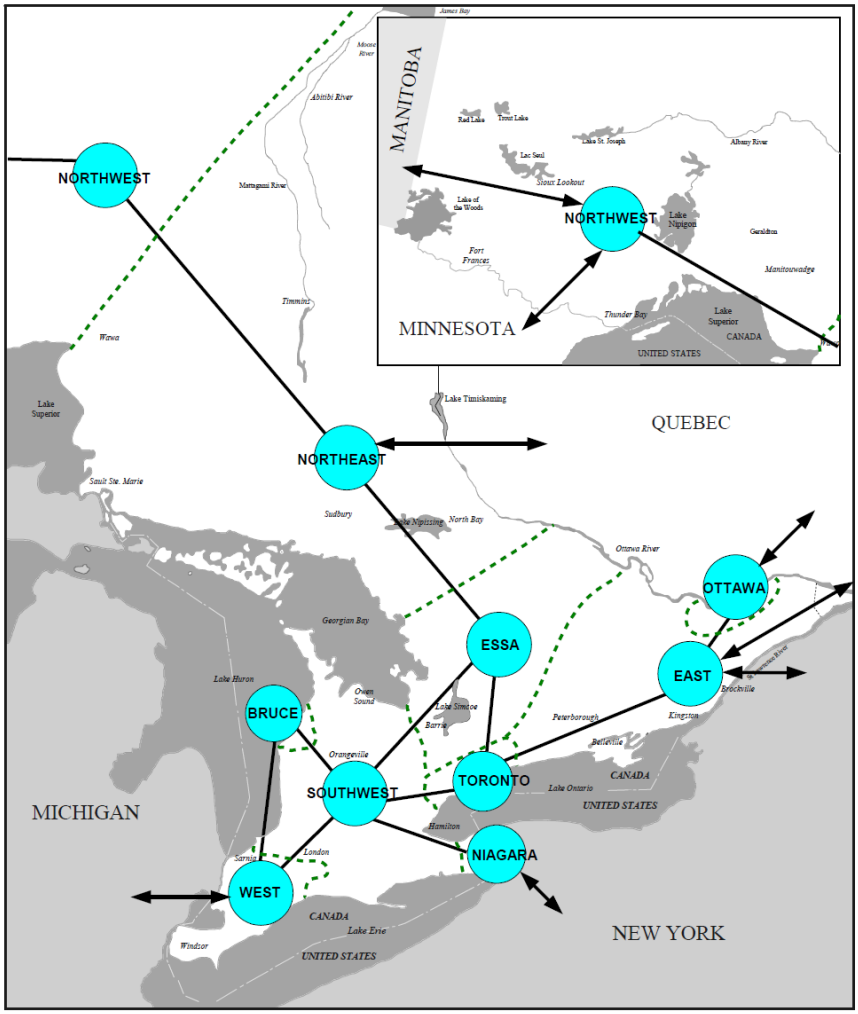
In addition to the interconnection issues described in Section 2, there are other issues from the bulk system that can impact the security of non-bulk operators. These issues include the nature and focus of the NERC CIP standards and minimal controls for Low Impact Bulk Electric Systems. Other NERC CIP weaknesses, such as no inclusion of communication networks, no detection and protection mechanisms for coordinated attacks, and no privacy controls can also significantly impact the non-bulk system.

Figure 15: Bulk to Non-Bulk



Other factors such as the IESO interconnections also need to be reviewed in more technical detail. As this map from the IESO shows, transmission connection between inter-provincial and international entities may present vulnerabilities to an Ontario LDC:

Figure 16: IESO Connection[26]



[26] Ont Tx System 2015jun.pdf

2.3. Other Problems

2.3.1. Current and Emerging Standards and Guidelines

This section addresses the challenges associated with standards as it relates to Ontario's non-bulk system.

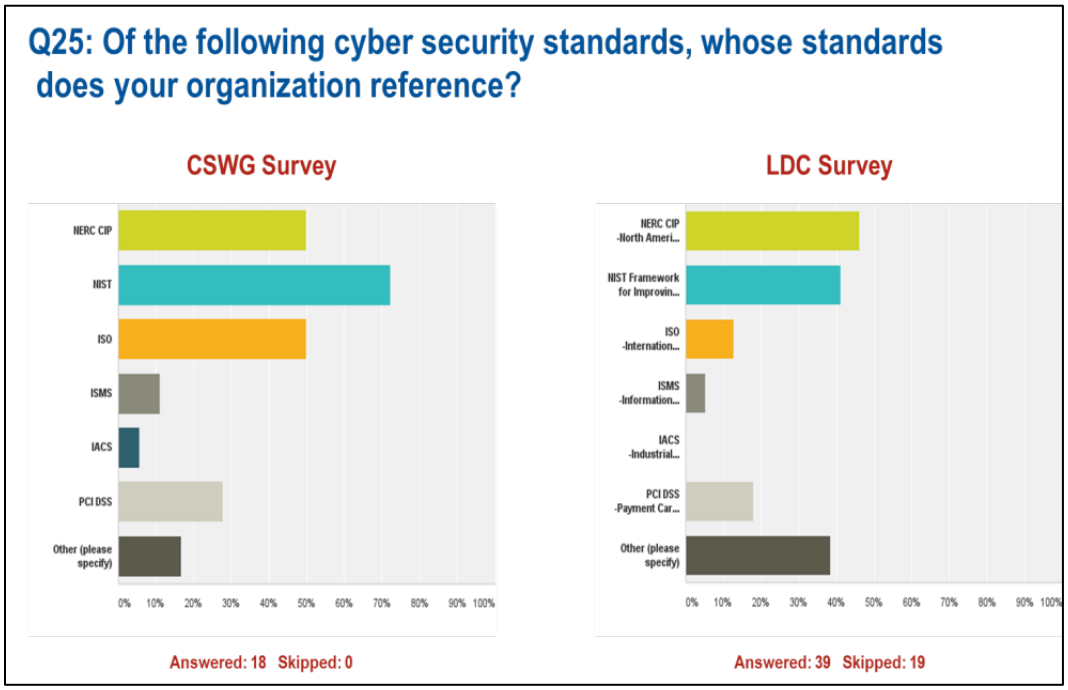
Results from Cyber Security Working Group & Broader LDC Questionnaire

A questionnaire was prepared for the Cyber Security Working Group in August 2016 to probe into Cyber Security awareness, standards, and risk management processes. A total of eighteen (18) Cyber Security Working Group members responded.

The same survey was conducted across a larger population of LDCs during the last week of September 2016. There were a total of fifty eight (58) LDC respondents. The results from the full survey are more representative of the LDCs in Ontario and demonstrate that the LDCs represented in the Cyber Security Working Group have more mature Cyber Security programs as compared to the larger LDC population.

The following slides summarize the results of the standards portion of the survey.

Figure 17: Survey Results - Question 25

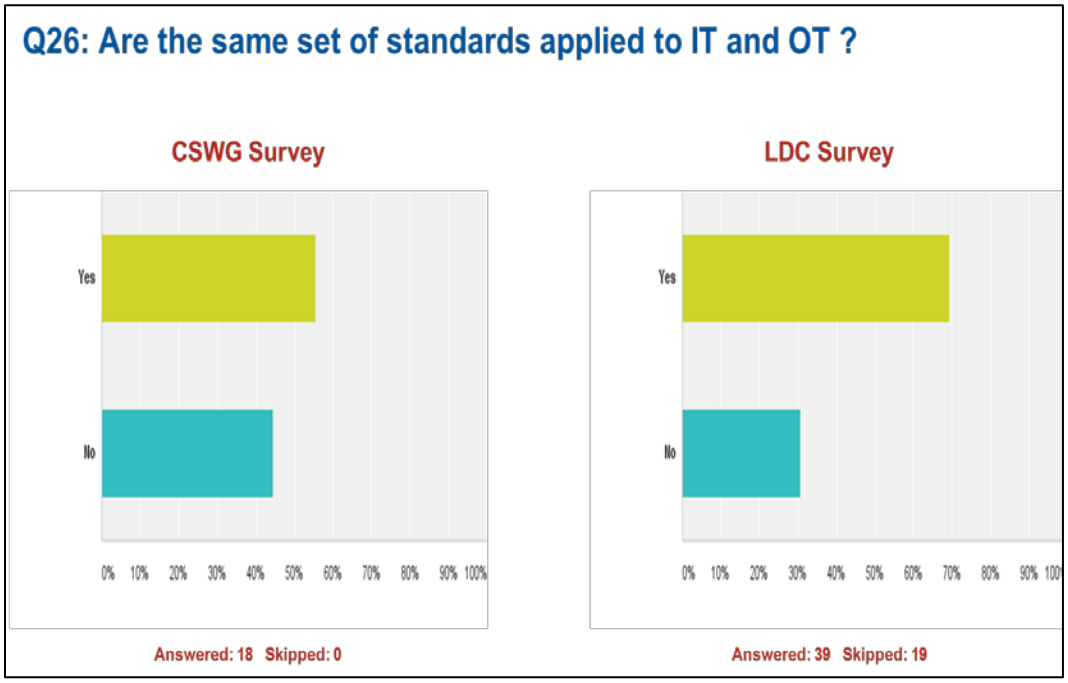


Considerations:

- These results are indicative of the industry in which entities today use several standards for Cyber Security. Unfortunately, there is no "off-the-shelf" standardized solution for utilities.
- The Cyber Security Working Group respondents showed a higher degree of reference to NIST than the broader LDC population, although the take up of NIST by the broader LDC population at 40% is impressive.

- Given the support and momentum behind the NIST Framework, we fully expect it to become the *de facto* standard framework for critical infrastructure.

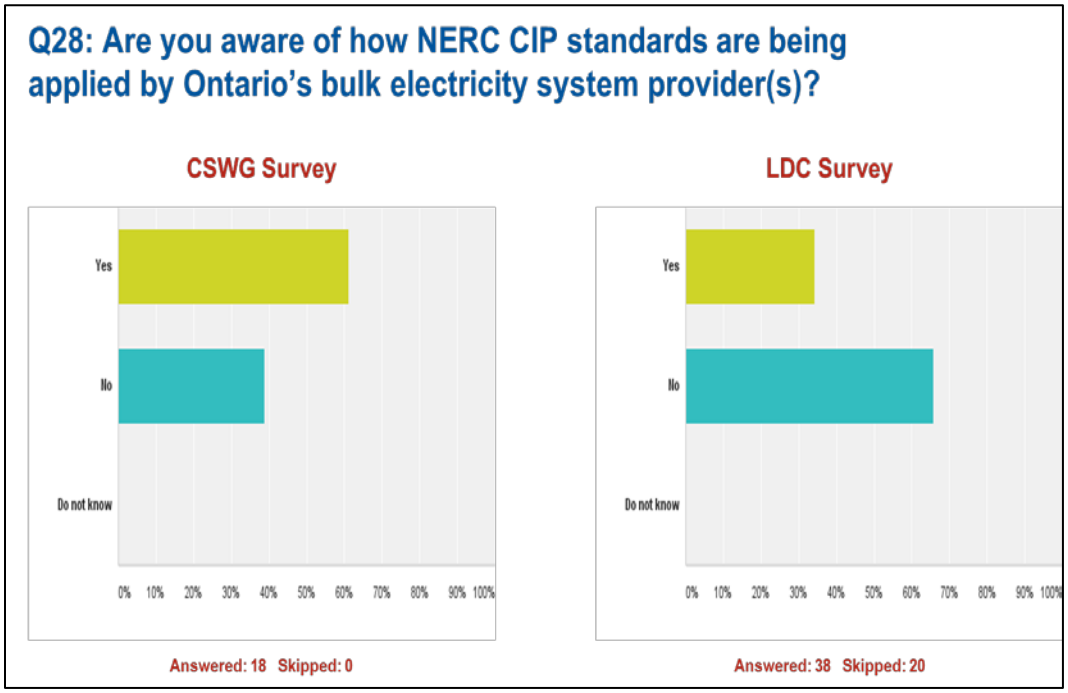
Figure 18: Survey Results - Question 26



Considerations:

- "IT" refers to Information Technology and the corporate business systems and applications. "OT" refers to Operational Technology which is the systems and applications that are related to grid operations (e.g. SCADA, Smart Metering, Substation systems, etc.).
- There is no right answer to this question. However, if different standards are applied to IT and OT, then there should be some overarching framework to connect them. The NIST Cybersecurity Framework is growing in terms of uptake and implementation by distribution utilities in North America as that overarching framework.
- Highly mature IT departments may favour more IT-centric standards such as ISO, while highly mature OT departments may favour more OT-centric standards such as NIST SP-800-82. Once again, these can be brought together from a governance and management perspective in an overarching framework such as the NIST Framework.

Figure 19: Survey Results - Question 28



Considerations:

- These results illustrate the differences in awareness of NERC CIP between the Cyber Security Working Group and the broader LDC group.
- The gaps and cyber risks between the non-bulk and bulk systems is further explored in the Discussion Paper for Task #3.

Results from Cyber Security Working Group Session #2

The questionnaire results were reviewed in the August 29, 2016 Cyber Security Working Group meeting with facilitation to probe deeper into areas such as IT / OT gaps and awareness of the NIST Cybersecurity Framework.

The following statements were made by the Cyber Security Working Group with respect to standards:

- There are cultural issues between the IT and OT groups within LDCs. The group re-affirmed widely held ideas that the system priorities of IT groups are Confidentiality, Integrity, and Availability while OT groups reverse the order and prioritize Availability, Integrity and Confidentiality. Some made the point that governance needs to converge IT, OT and telecom from the perspective of standards and overall approach.
- Some LDCs tried to implement NERC CIP, but didn't complete the implementation. They found it to be too much to implement in full.
- Generally, there is a good degree of awareness of the NIST Cybersecurity Framework.[27]

During the same session, a workshop and break-out session focused on the following questions:

1. How would you implement the NIST Framework in your organization?

[27] This is among the Cyber Security Working Group members, but we don't expect it would be the same for other small to mid-sized LDCs as latter as less mature from a cyber perspective on the whole.

2. Where would you start?

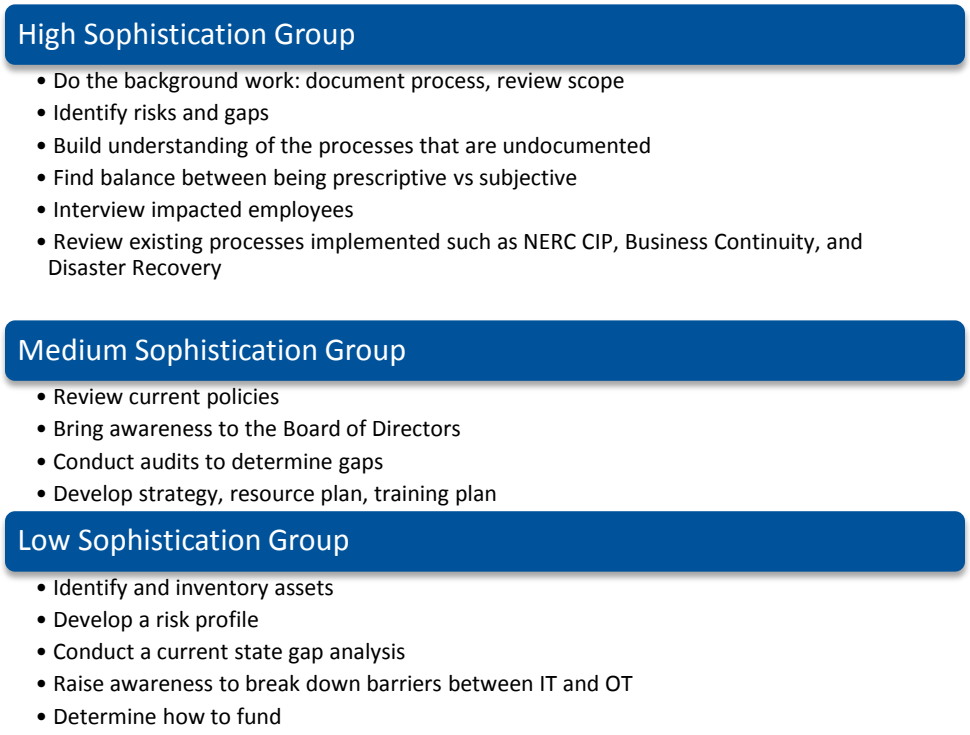
Three groups were assigned as follows:

- Those with a high degree of awareness of the NIST Framework
- Those with a medium degree of awareness of the NIST Framework
- Those with a low degree of awareness of the NIST Framework

The results were telling. All three groups struggled to define an easy-to-implement plan. The groups only had a limited amount of time, **thirty (30) minutes,** to develop this plan. In reality, the LDC would need to dedicate more time to the planning process. However, our sense is that, even with more time, the LDCs will need support in the area of planning, and certainly implementation. The degree of technical, implementation and governance support required will be a factor of the maturity and resources available to the LDC.

The following summarizes the implementation approach from the three groups.

Figure 20: Implementation Approaches



Given the inherent difficulty in implementation, we recommend that the Framework developed from this project be supported with extensive implementation plan guides and support resources.

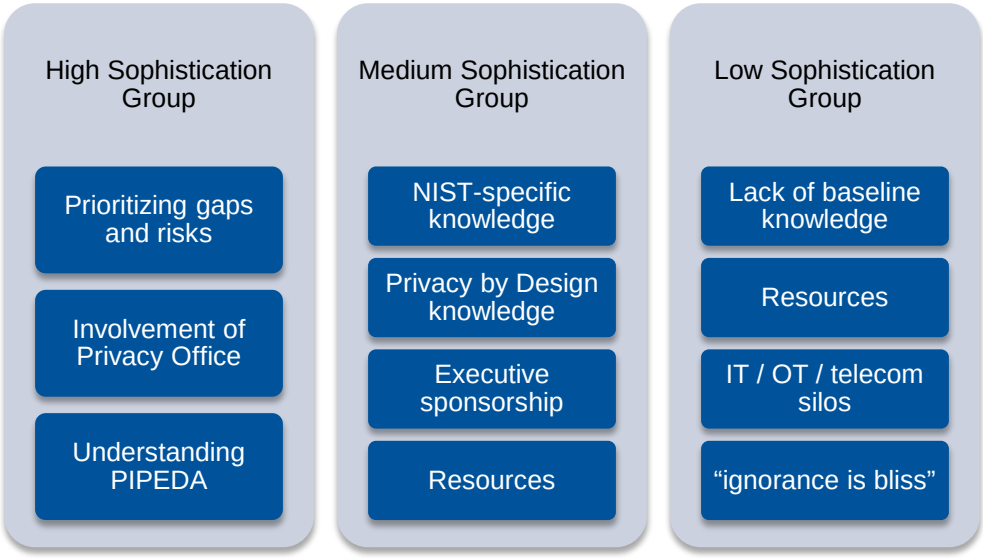
Results from Cyber Security Working Group Session #3

During the Cyber Security Working Group meeting on October 5th, 2016, three (3) subgroups of the Cyber Security Working Group were assigned to play the role of a Least Sophisticated LDC, a Medium Sophisticated LDC and a Highly Sophisticated LDC, and they were asked to discuss and respond to the following questions related to implementation of the NIST Cybersecurity Framework and Privacy by Design:

1. What challenges do you see with implementing the cyber security framework?
2. What do you see the reporting on the framework to look like?
3. What does the implementation look like to you?

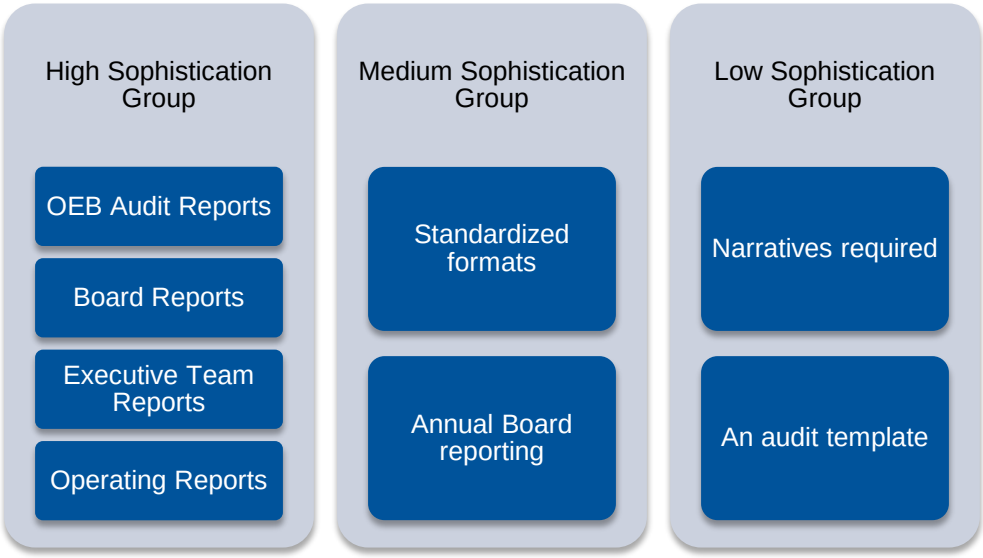
The following tables summarize the results:

Figure 21: Implementation Perspectives



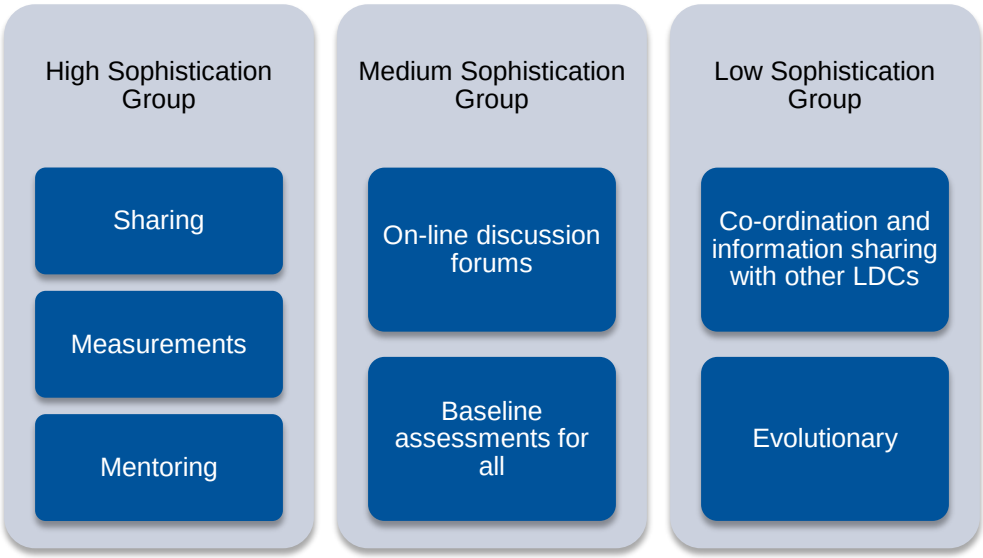
As a building theme in these Discussion Papers, the results of this activity show that even the most sophisticated LDCs will require assistance in all areas in implementing the Framework.

Figure 22: What would Reporting look like?



The Medium and Low Sophistication groups had a considerable number of questions in their workgroups, indicating that guidance on reporting would be of value.

Figure 23: What does Implementation look like to you?



Sharing was a common suggested recommendation across all areas, and this will be further detailed in the development of the Framework.

2.3.2. Environmental Scan

In this section, we review and assess influential bodies from the US, the NIST Cybersecurity Framework, the NERC CIP standards, and practices in other sectors.

APPA

In the US, there are approximately two thousand (2,000) public power distribution utilities that are very similar to LDCs. The US public power utilities span from small (<2,000 customers), medium and through to large size (> 1 million customers). Many of the public power electric utilities are governed by their municipality and have additional water, gas and telecommunication utilities.

In public power, there are approximately seventy (70) Joint Action Agencies that provide power, services and support to related groups of public power distribution utilities. The American Public Power Association (APPA) is the industry trade group that supports these public power utilities and the Joint Action Agencies.

The APPA has for many years supported their members in the area of Cyber Security. In fact, Cyber Security is one of the top six strategic priorities for the APPA. As a result, the APPA has dedicated a portion of their web site to grid security. There is an extensive amount of information and resources for their members on this site.[28]

In July 2016, the APPA announced that it (along with the NRECA) has received $15M in funding from the US Department of Energy (DOE) for enhancements for grid security for its members.[29] In the press release, it was stated “APPA and NRECA will use the funds to develop security tools, educational resources, updated guidelines, and training on common strategies that member utilities can use to improve their cyber and physical security culture. Activities to bolster security capabilities will include exercises, utility site assessments, and comprehensive information sharing.”

[28] American Public Power Association
[29] APPA to Receive DOE Funding for Grid Security Enhancements

As a trade association, we do not foresee that the APPA will develop their own Cyber Security standards but will reference and leverage industry standards. As part of the guidelines referenced in the press release[30], the APPA is aiming to develop a Cyber Security framework similar to the one in the OEB project. Given that the funding is from US DOE, we highly anticipate that the NIST Cybersecurity Framework and the US DOE ES-C2M2 model will be relevant for the APPA work.

There is a potential future collaboration opportunity for the industry with the APPA, which AESI can facilitate. Collaboration can result in information and resource sharing and knowledge transfer.

NRECA

In the US, there are approximately eight hundred and forty (840) distribution co-op utilities that are very similar to LDCs, and approximately sixty (65) Generation & Transmission (G&T) entities. The G&Ts provide power, services and support for related groups of distribution co-op utilities. The National Rural Electric Cooperative Association (NRECA) is the industry trade group that supports the distribution co-ops and the G&Ts.

As with the APPA, the NRECA has for many years identified Cyber Security as a priority for reliability and resilience and has supported its members in this area. The NRECA has developed a Reliability and Cybersecurity section on its web page that includes support resources and news for their members: http://www.nreca.coop/nreca-on-the-issues/energy-operations/reliability-cybersecurity/

Further, the NRECA has developed a very comprehensive Cyber Security guide (131 pages) for their members: http://www.nreca.coop/nreca-on-the-issues/energy-operations/reliability-cybersecurity/.

The preface to the guide includes the following statement: “This guide helps cooperatives think about security in a systematic way, consistent with the current Federal thinking. The basic concept is not “do this and you are secure” but a commitment to a process of continuous improvement.”

The Executive Summary of this Cyber Security guide includes the following text, which is excellent guidance for the OEB project given the similarities between co-ops and Ontario distributors:

> “This document provides practical security best practices and controls designed to help an electric cooperative improve the security posture of its smart grid. There is a large volume of guidance from organizations such as the National Institute of Standards and Technology (NIST), North American Electric Reliability Corporation (NERC), Federal Energy Regulatory Commission (FERC), and others that you are encouraged to review (referenced later in this document). The goal of this document is not to supplant or replace the other extensive work on this topic, but rather to boil security guidance down to a more digestible set that electric cooperatives can more naturally internalize and start adopting today. Condensing best practices into such a set required the authors of this document to make trade-offs and use their experience to focus on the most important “do first” types of activities. While not comprehensive by design, the guidance in this document represents actionable best practices and controls that organizations can begin to adopt to mitigate some of today’s top security risks. Every organization’s environment is different. While most best practices and guidelines described in this document are applicable to all environments, your organization may discover that some are less relevant to your particular installation. Further, the specific implementation details will differ according to the technology choices that your organization has already made, your technology road map, available resources, and other factors. To maintain its focus on a condensed set of best practices, this guide does not delve into lower-level implementation details (although some examples are provided for reference). It is also important to note that adding or modifying existing security controls should be done with care and sufficient planning. Your environment will require testing to ensure that changes to controls do not break important functionality or introduce new risks. The guidance in this document should be used as a

[30] APPA to Receive DOE Funding for Grid Security Enhancements

> description of what needs to be done, but your organization should introduce changes to your environment in a careful and thoughtful manner. Security improvement does not happen overnight; it is a gradual process."

This guide includes reference to many Cyber Security standards and frameworks which are outlined in **Appendix C: Informative References.**

With respect to the NIST Framework for Improving Critical Infrastructure Cybersecurity, it is stated in this guide that:

> "NIST's Framework for Improving Critical Infrastructure Cybersecurity (referenced above) calls for a business-driven and organization-specific risk management approach for protecting critical infrastructure. Inspired by NIST IR 7628, earlier versions of this guide, and other sources, NIST has captured a solid set of security best practices that align with the guidance offered here. NIST continues its efforts to create and harmonize interoperability and cyber security guidelines, and our organization should continue to stay abreast of those changes."

It should be noted that the NRECA typically provides extensive technical detail for their members, and this guide and the Cyber Security portion of their web site are no exceptions.

US Department of Energy

The US Department of Energy (DOE) has put considerable focus on Cyber Security for critical infrastructure for 10+ years. Their website http://energy.gov/oe/services/cybersecurity has an extensive amount of valuable resources and tools freely available, including reference documents, news articles and blogs.

DOE lists a number of reference documents including the NIST Cybersecurity Framework, the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)[31], and the NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity. The first version of the NISTIR 7628 document was a key input into the development of the NIST Cybersecurity Framework.

Also, DOE states the following:

> *"The Office of Electricity Delivery and Energy Reliability (OE) supports the Administration's strategic comprehensive approach to cybersecurity for the grid by:*
>
> - *Facilitating public-private partnerships to accelerate cybersecurity efforts for the grid of the 21st century;*
> - *Funding research and development of advanced technology to create a secure and resilient electricity infrastructure;*
> - *Supporting the development of cybersecurity standards to provide a baseline to protect against known vulnerabilities;*
> - *Facilitating timely sharing of actionable and relevant threat information;*
> - *Advancing risk management strategies to improve decision making;*
> - *Supporting sector incident management and response; and*
> - *Enhancing and augmenting the cybersecurity workforce within the electric sector."*

As can be seen above, DOE does not develop new standards but rather they support the development of standards for the industry. We would recommend the same approach for the OEB.

The US DOE supports the NIST Cybersecurity Standard as well as the ES-C2M2 model. In Discussion Paper #4, we describe the strengths of ES-C2MS model but based on direct feedback from the Cyber Security Working

[31] Electricity Subsector Cybersecurity Capability Maturity Model

Group during the August 29th breakout session, the complexity of the ES-C2M2 model would make it very difficult to implement in its entirety for any LDC.

NIST

The National Institute of Standards and Technology (NIST) facilitated the development of a critical infrastructure cybersecurity framework in response to a Presidential Executive Order in 2013[32]. It is stated in this Executive Order that

> "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

The result of this Executive Order was a comprehensive document issued in February 2014 entitled Framework for Improving Critical Infrastructure Cybersecurity: http://www.nist.gov/cyberframework/.

This framework has endorsement from many influential entities such as US DOE, US Department of Homeland Security, the White House, and others like Intel, Chevron, Walgreens, Pepco, Apple, QVC, and the Bank of America[33]. It is our view that adoption of the NIST Framework is increasing and that it will become a *de facto* framework for critical infrastructure cyber security.

In the NIST Framework it is stated that:

> "Due to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk. This approach is necessary regardless of an organization's size, threat exposure, or cybersecurity sophistication today". It is also stated "To ensure extensibility and enable technical innovation, the Framework is technology neutral. The Framework relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience"

The purpose of the NIST Framework is stated as:

> …"the Framework provides a common taxonomy and mechanism for organizations to:
>
> *1) Describe their current cybersecurity posture;*
> *2) Describe their target state for cybersecurity;*
> *3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;*
> *4) Assess progress toward the target state;*
> *5) Communicate among internal and external stakeholders about cybersecurity risk.*

The Framework complements, and does not replace, an organization's risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one...."

[32] Executive Order Improving Critical Infrastructure Cybersecurity
[33] Newsletter Update Cybersecurity Framework

The following shows the structure of the NIST framework and progression of detail from Functions[34] through to Categories and Subcategories:

Figure 24: NIST Framework Core Structure

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

[34] The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References, such as existing standards, guidelines, and practices for each Subcategory. Cybersecurity Framework FAQS Framework Components

The following table defines the Categories associated with each Function:

Figure 25: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	**IDENTIFY**	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	**PROTECT**	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	**DETECT**	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	**RESPOND**	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	**RECOVER**	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

As the name suggests, the NIST Cybersecurity Framework is a framework, not a standard in itself. Rather, it is a collection of standards organized logically for all critical infrastructure operators (including small to mid-sized distribution utilities) to use effectively for their cybersecurity program.

The following shows how the Functions cascade into Categories, which further cascade into Informative Resources, the latter of which are standards:

Figure 26: NIST Functions, Categories, Subcategories and Informative References

Function	Category	Subcategory	Informative References
RS	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**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 - **ISO/IEC 27001:2013** A.16.1.5 - NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	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
		RS.CO-2: Events are reported consistent with established criteria	- I**SA 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
		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
		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
		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

This is an extremely comprehensive and guiding model.

Based on the fact that the NIST Cybersecurity Framework is gaining great momentum as becoming the *de facto* Cyber Security framework for critical infrastructure; the ability of the framework to apply to small, medium and large-sized LDCs; and the Cyber Security Working Group response; it is our view that the NIST Cybersecurity Framework has tremendous applicability for the OEB Framework.

NERC CIP

The North American Electric Reliability Corporation (NERC) is an independent, not-for-profit organization, whose mission is to ensure the reliability of the Bulk Electric System (BES) in North America.

NERC oversees and assures the reliability of the BES by issuing and enforcing Reliability Standards. NERC is recognized as the Electric Reliability Organization for Ontario by the Ontario Ministry of Energy

There are two (2) types of Standards:

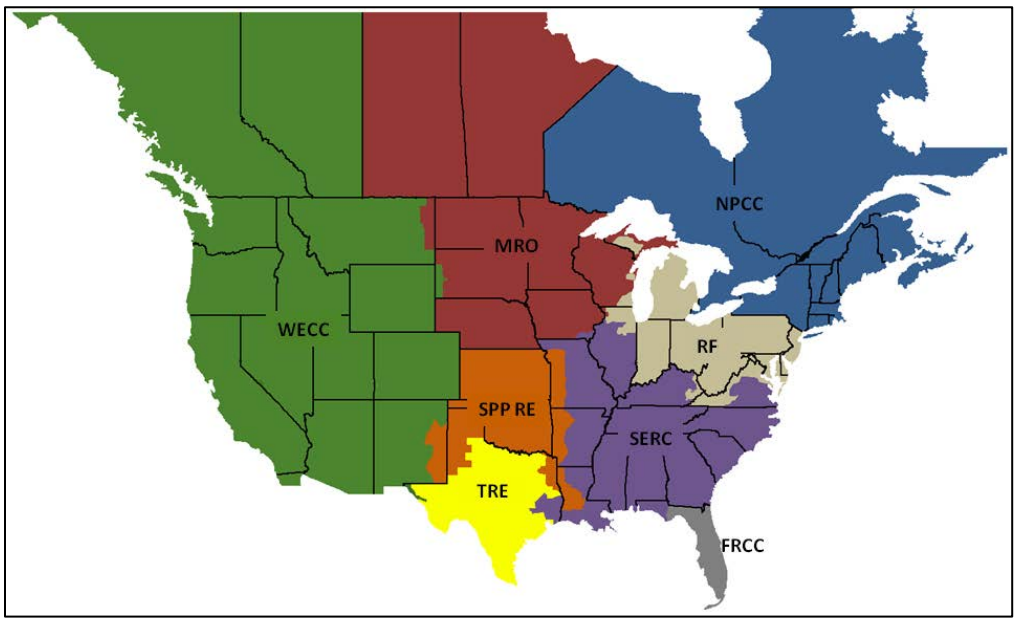
1. Operations and Planning Standards (Non-CIP) – FERC Order 693
2. Critical Infrastructure Protection (CIP) Standards (addresses cyber and physical security) – FERC Order 706/791

In the US, “Guidelines” became mandatory, enforceable, and can carry stiff penalties (Non-CIP 2007 and CIP 2009). NERC Standards have been mandatory and enforceable in Ontario since April 2002.

Under NERC, there are 8 Regional Entities:

1. Northeast Power Coordinating Council (NPCC) Note: Ontario is part of the NPCC
2. Reliability First Corporation (RFC)
3. Florida Reliability Coordinating Council (FRCC)
4. SERC Reliability Corporation (SERC)
5. Midwest Reliability Organization (MRO)
6. Southwest Power Pool, RE (SPP)
7. Texas Regional Entity (TRE)
8. Western Electricity Coordinating Council (WECC)

Figure 27: NERC Regional Entities35



In Ontario, NPCC compliance, assessment and enforcement is overseen by the IESO's Market Assessment and Compliance Division (MACD).

Specific to Cyber Security, the following are the NERC CIP standards:

- CIP-002-5.1 - BES Cyber System Categorization
- CIP-003-6 - Security Management Controls
- CIP-004-6 - Personnel & Training
- CIP-005-5 - Electronic Security Perimeter(s)
- CIP-006-6 - Physical Security of BES Cyber Systems
- CIP-007-6 - Systems Security Management
- CIP-008-5 - Incident Reporting and Response Planning
- CIP-009-6 - Recovery Plans for BES Cyber Systems
- CIP-010-2 - Configuration Change Management and Vulnerability Assessments

[35] Regional Entities

- CIP-011-2 - Information Protection
- CIP-014-2 - Physical Security (of Transmission Stations)

Each of the above is further detailed in “Requirements” and “Measures” and is assigned according to the High, Medium or Low Impact on the applicable BES Cyber System.

The NERC CIP set of standards is not prescriptive i.e. the standards do not tell you exactly how to implement them. They tell you what to do, not how to do it. Further, the NERC CIP set of standards does not reference other standards, guidelines or best practices.

The NERC CIP standards by design are very focused on large critical assets and to protect the bulk powers systems against compromise that could lead to misoperation or instability. They have some excellent attributes, but do not map perfectly to the Cyber Security requirements of Ontario LDCs and non-bulk entities. The NERC CIP standards do not address business risks or privacy and do not provide standards-based implementation guidance. Further, as reported by the Cyber Security Working Group, the NERC CIP standards are difficult to apply for LDCs.

Cross-Sector View: Natural Gas Industry

For this project, we will take a cross-sector view to consider best practices and the status of Cyber Security within those sectors. We will start with a perspective on the petroleum and natural gas industries.

The American Petroleum Institute (API) represents the US oil and natural gas industries and has approximately six hundred and fifty (650) members. In a February 2016 letter from the API to NIST, the API stated that:

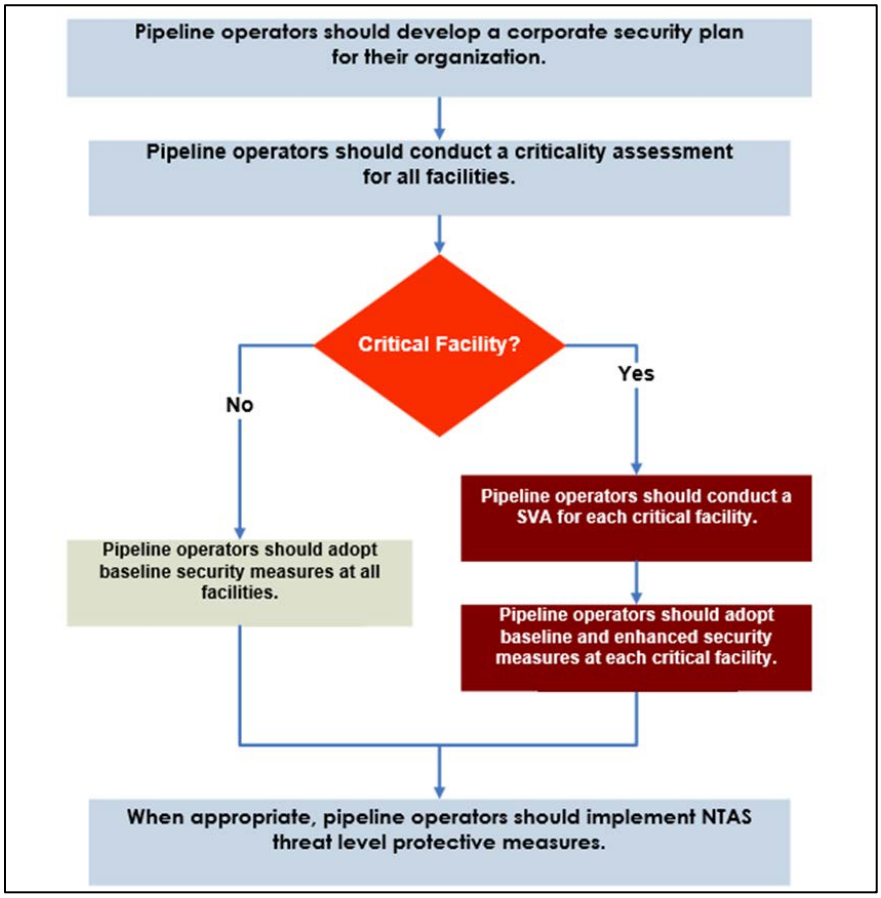
> “Cybersecurity is a priority for the oil and natural gas industry and API members. As operators and service providers of energy critical infrastructure in the United States and globally, protecting networks from cyber attacks is a priority of API’s members. API remains strongly supportive of the NIST Framework for Improving Critical Infrastructure Cybersecurity. The Framework has been widely-used by the oil and natural gas industry represented by API’s member companies.”[36]

The gas industry is lagging the electric industry in terms of Cyber Security focus and maturity. However, there has been increasing focus on this issue and both the American Gas Association (AGA) and the Canadian Energy Pipeline Association (CEPA) are facilitating discussions amongst their members. The AGA makes reference to the NIST Cybersecurity Framework as guidance.

In the US, pipeline security is voluntary. The US Department of Homeland Security has developed the following process as recommended for pipeline operators:

[36] 2016 – Letter from API to NIST.pdf

Figure 28: DHS Process[37][38]



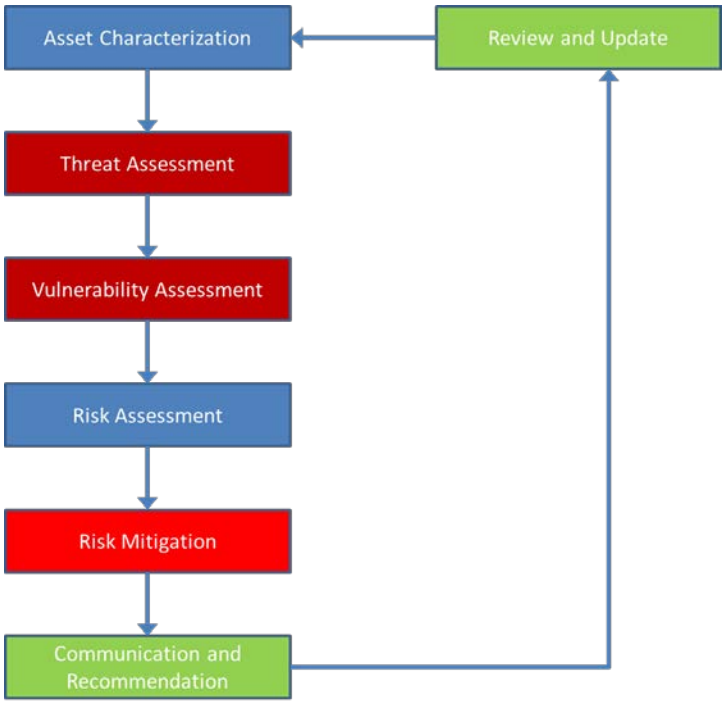
For gas transmission entities in Canada, the National Energy Board of Canada has mandated that the CSA Z246.1 standard "Security Management for Petroleum and Natural Gas Industry System" will apply. This standard calls for a Security Management Program (SMP) aligned with the "Plan, Do, Check, Act" model. Governance for the program includes:

- senior management accountability for the SMP
- roles and responsibilities for the development, implementation, control, review, continual improvement, and approval of the SMP across the organization, based on the security risk management process
- responsibility for the SMP, including sufficient resources to implement and maintain it
- security policy that provides clear direction, accountability, and oversight for the SMP
- SMP awareness, roles and responsibilities, accountability, training, and continual improvement for employees and on-site personnel

The following illustrates the CSA Z246 standard from a process flow perspective:

[37] SVA means Security Vulnerability Assessment
[38] NTAS means National Terrorism Advisory System

Figure 29: CSA Z246 Process



There are no such Cyber Security standards that we know of designed specifically for gas distributors in Canada.

Since LDCs and gas distributors share many commonalities including the type of systems and applications, this Framework project has the opportunity to benefit Ontario's gas distributors and others in the gas industry in Canada. The Framework could be further developed so that gas distributors can adopt the Framework as well.

Summary

There are potential future collaboration opportunities for the industry with the APPA and the NRECA. It is recommended that these collaboration opportunities be explored. AESI can assist by facilitating discussions.

There are 75+ in total Cyber Security standards and frameworks for available to critical infrastructure operators in North America. The key issues are applicability and ease of implementation.

Based on industry endorsement and applicability to LDCs, in our view the NIST Cybersecurity Framework provides the most appropriate perspective for Ontario's LDCs and non-bulk operators. As per the US, we do not recommend that the OEB develop its own cyber security standards

2.3.3. Privacy

Security and privacy are inextricably linked, but are different concepts. From a business practices perspective, security is about protecting and controlling information. Privacy, on the other hand, is about recognizing that while the company retains the physical control of the data, the decisions about how to collect, use and disclose personal information should reflect individual consent and personal preferences. Of course, security is integral to privacy, because without strong information security measures, privacy breaches will occur.

Environmental Scan

Privacy law in Ontario[39] has two key two purposes:

1. to govern how organizations are allowed to collect, use, and disclose personal information; and
2. to enable individuals to access and manage their personal information collected by organizations.

"Personal information" is defined broadly in privacy legislation and jurisprudence as information about an identifiable individual. More specifically, this means that any information that can be used to distinguish an individual or trace an individual or can be linked to an individual is personal information. Examples of personal information include one's name, contact information, biographical information, individual preferences, transaction history, driver's license number, social insurance number, and passport number. Even asset information, such as an Internet Protocol address, that links to a particular person or a small, well-defined group of people is personal information.

Strictly speaking, information about corporate customers is not "personal information" governed by privacy law, which protects individuals only. However, we suggest that the privacy concepts discussed in this White Paper can and should be applied to deal with proprietary or confidential customer information of all sorts, including information about commercial customers.

All privacy statutes governing entities operating in Ontario, MFIPPA, PIPEDA and FIPPA, are based upon the "Fair Information Practice Principles". [40] The Fair Information Practice Principles have their roots in guidance adopted by the Organization for Economic Cooperation and Development (OECD) member countries (including Canada) in 1980.[41] The Fair Information Practice Principles were identified as eight (8) general principles that should be adhered to when collecting, using or disclosing personal information.[42]

The Fair Information Practice Principles underlie and are articulated in a Schedule to PIPEDA as ten (10) tenets of Canadian privacy protection (collectively referred to herein as the Fair Information Principles or FIPs):

1. **Accountability:** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
2. **Identifying Purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. **Consent:** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
4. **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure and Retention:** 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. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
6. **Accuracy:** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

[39] As reflected in three key statutes, the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), the Personal Information Protection Electronic Documents Act (PIPEDA), and the Freedom of Information Protection of Privacy Act (FIPPA). There is also a personal health information statute in Ontario, which is not applicable.

[40] For an overview of privacy legislation in Canada, see: Privacy Laws in Canada

[41] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980: www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[42] The original eight (8) Fair Information Practice Principles are: Collection Limitation Principle; Data Quality Principle, Purpose Specification Principle, Use Limitation Principle; Security Safeguards Principle, Openness Principle; Individual Participation Principle; and Accountability Principle.

7. **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. **Openness:** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. **Individual Access:** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging Compliance:** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.[43]

These FIPs can be expressed as privacy practices. Once a FIP is expressed as a practice or conduct, it can then be integrated into the OEB Cyber Security Framework, and the OEB can monitor compliance with it.

Review and Assessment

Privacy by Design (PbD) is a methodology for protecting privacy based on the FIPs that is, in our view, directly applicable to the Framework. PbD was developed in the 1990s by former Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian. It prescribes an approach to privacy protection that is characterized by proactive rather than reactive measures, and anticipates and prevents privacy invasive events before they happen. PbD promotes inserting privacy and data protection into information technologies, organization processes, networked architectures and entire systems of governance and oversight. [44] In doing so, PbD aims to prevent privacy breaches from occurring.[45]

PbD advances seven (7) Foundational Principles[46], which can be summarized as follows:

1. **Proactive not Reactive; Preventative not Remedial:** PbD aims to prevent privacy breaches from occurring.
2. **Privacy as the Default Setting:** If an individual does nothing, and makes no choice, their privacy remains intact.
3. **Privacy embedded into Design:** Privacy becomes an essential component of the core functionality of design and architecture of IT systems and business practices.
4. **Full Functionality - Positive Sum, not Zero-Sum:** There is no need to sacrifice functionality or security in the name of privacy as PbD can accommodate all legitimate interests.
5. **End-to-End Security - Full Lifecycle Protection:** Strong security measures are essential to privacy and must be present throughout the entire lifecycle management of information.
6. **Visibility and Transparency - Keep it Open:** PbD seeks to ensure that business practices and technologies are operating according to stated promises and objectives.
7. **Respect for User Privacy - Keep it User-Centric:** Users must be empowered to control decisions regarding their personal information.

[43] In 2009, the American Institute of Certified Public Accountants and the Canadian Institute of Accountants (now CPA Canada) put together a useful guide based on what are referred to as the "Generally Accepted Privacy Principles" (GAPP). The GAPP are ten (10) principles that are worded slightly differently from the FIPs, but can be mapped directly to PIPEDA and the FIPs. The GAAP Guide includes a chart that contains illustrative controls and procedures that a business might consider as part of its privacy program. For more information on the GAPP Guide, see Generally Accepted Privacy Principles

[44] Cavoukian A., Privacy by Design, Information and Privacy Commissioner of Ontario: January 2009, Revised September 2013.

[45] PbD does not suggest measures to deal with privacy breaches after they have occurred. By analogy to the NIST Cybersecurity Framework, PbD equates to the second element of the NIST Framework, which is "*Protect*".

[46] Cavoukian A., Privacy by Design, Information and Privacy Commissioner of Ontario: January 2009, Revised September 2013.

It is important to acknowledge that many LDCs build onto existing legacy systems, and do not begin from scratch with new information technologies, networked architectures and systems of governance. That does not mean that PbD is inapplicable or "too late" for them. That being said, PbD should not simply be bolted-on as an afterthought; instead, PbD principles can be built into legacy systems as opportunities arise, such as while implementing new Smart Grid initiatives and refining cybersecurity infrastructure.[47]

Privacy and the Smart Grid

Indeed, it is recognized in the privacy literature that PbD is applicable to utility operations. In particular, there has been significant writing in this area relating to the Smart Grid.[48] In the context of the Smart Grid, privacy professionals take the position that, by linking any personally identifiable information with energy use information, the energy use information is rendered personal information in its own right. The rationale for consumer energy use data being personal information is that the Smart Grid increases the granularity of information collected on household energy usage to the point that it can allow one to glean intimate details about the customer's household activities.

The applicability of PbD to utility operations is underscored by the fact that former Ontario Information and Privacy Commissioner, Dr. Ann Cavoukian, has translated her seven (7) Foundational Principles for PbD into seven (7) best practices for the Smart Grid[49]:

1. Smart Grid systems should feature privacy principles in their overall project governance framework and proactively embed privacy requirements into their designs, in order to prevent privacy-invasive events from occurring;
2. Smart Grid systems must ensure that privacy is the default — the "no action required" mode of protecting one's privacy — its presence is ensured;
3. Smart Grid systems must make privacy a core functionality in the design and architecture of Smart Grid systems and practices — an essential design feature;
4. Smart Grid systems must avoid any unnecessary trade-offs between privacy and legitimate objectives of Smart Grid projects;
5. Smart Grid systems must build in privacy end-to-end, throughout the entire life cycle of any personal information collected;
6. Smart Grid systems must be visible and transparent to consumers — engaging in accountable business practices — to ensure that new Smart Grid systems operate according to stated objectives;
7. Smart Grid systems must be designed with respect for consumer privacy, as a core foundational requirement.

Summary

The NIST Smart Grid Privacy Working Group has recognized that PbD complements crucial cybersecurity measures for utilities. In August 2010, PbD was specifically endorsed by the NIST Smart Grid Privacy Working Group in their report entitled "NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol 2, Privacy and the

[47] "Security-by-Design" is a related concept often used along with PbD. The European Security Research and Innovation Forum, in a 2009 Report, defined the "Security-by-Design" concept as follows: "Security must be embedded in the technology and system development from the early stages of conceptualisation and design". [http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/security/pdf/esrif_final_report_en.pdf at page 204]. The Framework under development , in totality, will be an expansion of the security-by-design concept, and therefore there will be no further discussion of security-by-design as a separate concept in this Discussion Paper.

[48] See, for example, Cavoukian A., Operationalizing Privacy by Design: The Ontario Smart Grid Case Study, February , 2011; Cavoukian A., Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid, June 2010; Cavoukian, A., Polonetsky, J. & Wolf, C., SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation, IDIS (2010) 3: 275. doi:10.1007/s12394-010-0046-y; Cavoukian A., Polonetsky J., Winn C., Privacy by Design and Third Party Access to Customer Energy Usage Data , The Future of Privacy Forum, January 2013; Cavoukian A., Building Privacy into Ontario's Smart Meter Data Management System: A Control Framework, May 2012.

[49] Cavoukian A., Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid, June 2010

Smart Grid". The Report recommends that, using the PbD methodology, privacy protections be built into systems and processes for the Smart Grid.

As a result of the foregoing review, we recommend embedding PbD principles into the OEB Cyber Security Framework.[50] We recommend doing so by introducing privacy controls that operationalize the FIPs into the NIST Cybersecurity Framework among the crucial security controls which they complement.

2.3.4. Cybersecurity Insurance

Cyber insurance is quickly gaining popularity as one way to transfer cybersecurity risk and to address residual risk. There are many insurance providers that provide cyber security and privacy options for Ontario's LDCs.

It is our understanding that greater than 70% of LDCs have purchased cyber insurance policies. LDCs can select the insurance packages that they require from any insurance provider whether that is from MEARIE (insurance reciprocal), AIG, AON, HUB International or others.

2.4. From the OEBs Perspective

The Ontario Energy Board (OEB) oversees the Province's electricity and natural gas sectors through effective, fair and transparent regulation and in accordance with the objectives set out in the governing statutory framework.[51]

As an independent regulatory body, the OEB makes decisions and provides advice to the government in order to contribute to a sustainable, reliable energy sector and to help consumers get value from their natural gas and electricity services.[52] This is accomplished through:

- Establishing rates and prices that are reasonable to consumers and that allow utilities to invest in the system;
- Encouraging higher performance from natural gas and electricity utilities and measuring progress;
- Making the consumer's own usage, and the broader energy issues, easier to understand;
- Looking out for consumer interests, investigating complaints and applying penalties, where appropriate; and
- Thinking about the long-term needs of the energy sector and developing a regulatory policy to meet emerging challenges.[53]

The OEB mandate is established by the provincial government and is embodied in legislation, regulation and directives.[54] In November 2010, the Minister of Energy issued a Directive to the Board in relation to the

[50] The key is to recognize and take advantage of opportunities to improve privacy protection and build it into systems. For example, consider an LDC that is embarking on a redesign of its physical access control systems which will consist of entryway consoles that recognize information on ID badges. Before the new system is implemented is the time to ask: What information collected by this system will be personal information? How confidential is this information? Are there vulnerabilities in the system that can result in harm to the individual? Is all of this information required for the system to function properly? Can specific controls be put in place, such as anonymizing the data, to mitigate the risk of harm? Risk assessment strategies to identify privacy vulnerabilities are discussed in more detail in a later section of this White Paper.

[51] 2012 - OEB – Energy Sector Regulations Overview - The OEB's mandate and powers in relation to the energy sector are set out principally in three statutes – the Ontario Energy Board Act, 1998, the Electricity Act, 1998 and the Energy Consumer Protection Act, 2010 – and in regulations made under those statutes.

[52] 2017 - OEB – Mission and Mandate

[53] 2017 - OEB – Mission and Mandate

[54] 2017 - OEB – What Laws Guide our Actions - The OEB mandate and authority come from the *Ontario Energy Board Act, 1998*, the *Electricity Act, 1998*, and a number of other provincial statutes including: the *Energy Consumer Protection Act,*

implementation and promotion of the Smart Grid in the Province. The Board was guided by ten (10) government policy objectives[55], which included security and privacy as two key objectives as follows:

v. *Security*: Cyber security and physical security should be provided to protect data, access points, and the overall electricity grid from unauthorized access and malicious attacks; and

vi. *Privacy*: Respect and protect the privacy of customers. Integrate privacy requirements into smart grid planning and design from an early stage, including the completion of privacy impact assessments.

An integral part of the OEB's regulatory mandate is to protect the interests of consumers.[56] Its mission is to promote a viable, sustainable and efficient energy sector that serves the public interest and assists consumers in obtaining reliable energy services that are cost effective.[57]

The OEB's three (3) year business plan outlines key objectives and initiatives, including key trends and issues in the broader operating environment and in particular, technological innovation which affects consumer protection.

Privacy and security of customer information and the electrical grid are a priority for the OEB. The OEB recognises the need to ensure that its own regulatory policies and processes address these changes in a manner that reflects the OEB's public interest and consumer protection mandates. The OEB has placed obligations on electricity transmitters, electricity and natural gas distributors through licences and codes to ensure customer information is protected and to incorporate security risk mitigation as part of their distribution and asset management plans.

- Retail Settlement Code (RSC)[58] which establishes a distributor's obligations and responsibilities associated with financial settlement among retailers and customers and provides for tracking and facilitating customer transfers among competitive retailers;
- Distribution System Code (DSC)[59] which establishes the obligations of a distributor with respect to the services and terms of service to be offered to customers and retailers and provides minimum technical operating standards of distribution systems;
- Standard Supply Service Code for Electricity Distributors SSSC[60] specifically referenced an electricity distributor's obligation to maintain the confidentiality of consumer-specific information[61.]
- Affiliates Relations Code (ARC) sets out the standards and conditions for the interaction between gas distributors, transmitters and storage companies and their respective affiliated companies. It also sets out the standards and conditions for the interaction between electricity distributors and transmitters and their respective affiliated companies.[62]

2010, the *Municipal Franchises Act*, the *Oil, Gas and Salt Resources Act*, the *Assessment Act*, and the *Toronto District Heating Corporation Act*.

[55] 2010 - Minister Directive Smart Grid – The OEB shall be guided by the policy objectives of the government p.2-3.

[56] Section 1 - Ontario Energy Board Act, 1998, S.O. 1998 - The first of five objectives of the OEB is to protect the interests of consumers with respect to prices and the adequacy, reliability and quality of electricity service.

[57] P.4 – OEB Business Plan 2017

[58] 2015 – Retail Settlement Code

[59] 2015 – Distributions System Code

[60] 2017 – Standard Supply Service Code for Electricity Distributors

[61] 2017 – Standard Supply Service Code for Electricity Distributors – "consumer-specific information" means information relating to a specific consumer obtained by any person through the process of selling or offering to sell electricity to the consumer, and includes information obtained without the consent of such consumer.

[62] 2017 – Rules, Codes, and Requirements

A distributor is required to maintain consumer confidentiality in accordance with the distributor's licence, which sets out restrictions on the use of customer information. For example, in the electricity distribution licences[63] it states:

> *15 Restrictions on Provision of Information*
>
> *15.1 The Licensee shall not use information regarding a consumer, retailer, wholesaler or generator obtained for one purpose for any other purpose without the written consent of the consumer, retailer, wholesaler or generator.*
>
> *15.2 The Licensee shall not disclose information regarding a consumer, retailer, wholesaler or generator to any other party without the written consent of the consumer, retailer, wholesaler or generator, except where such information is required to be disclosed:*
>
> > *a) To comply with any legislative or regulatory requirements, including the conditions of this License;*
> >
> > *b) For billing, settlement or market operations purposes;*
> >
> > *c) For law enforcement purposes; or*
> >
> > *d) To a debt collection agency for the processing of past due accounts of the consumer, retailer, wholesaler or generator.*
>
> *15.3 The Licensee may disclose information regarding consumers, retailers, wholesalers or generators where the information has been sufficiently aggregated such that their particular information cannot reasonably be identified.*
>
> *15.4 The Licensee shall inform consumers, retailers, wholesalers and generators of the conditions under which their information may be released to a third party without their consent.*
>
> *15.5 If the Licensee discloses information under this section, the Licensee shall ensure that the information provided will not be used for any other purpose except the purpose for which it was disclosed.*

The OEB has determined that in order to achieve its privacy and security objectives, it would facilitate the development and implementation of a sector driven cyber security Framework that leverages these generic frameworks and models, and articulates essential privacy and security best practices and can be the basis for repeatable and verifiable reporting on these essential practices. The overall goal of the OEB is to mitigate the risk of unauthorised access to business and operating systems that could result from the increased use of automation, electronic communications and data flows.[64] This approach can provide the OEB with the necessary assurance of compliance, while providing flexibility to the regulated entities, in how they operationalize their security posture.

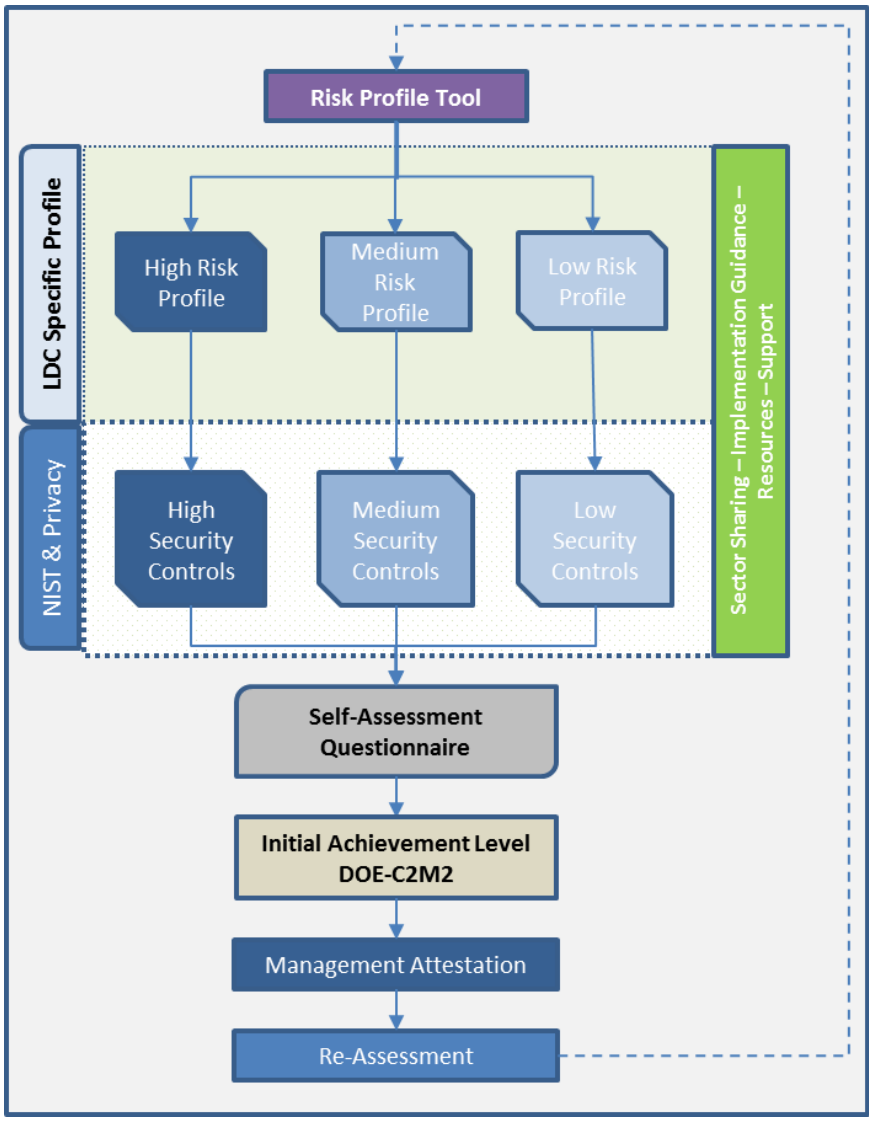
[63] 2008 - Electricity Distribution Licence
[64] 2017 – OEB Energy Policy Initiatives

3. The Cybersecurity Framework Solution

3.1. Concept

Through the Cyber Security Working Group and both qualitative and quantitative research methods, the Consultant Team (AESI Inc., DLA Piper and Richter) developed an Ontario LDC-specific Cyber Security Framework, based on the NIST Cybersecurity Framework, with influences from the DOE-C2M2, Privacy by Design and input from a wide variety of stakeholders. Conceptually, the Cyber Security Framework developed can be visualized as follows:

Figure 30: Ontario LDC Cybersecurity Framework



Based on the meetings with the Cyber Security Working Group, the following criteria for the Cyber Security Framework were incorporated:

- Needs to be prescriptive with criteria, not subjective

- Support is required for the LDCs
- Guidance resources and shared resources to be provided
- Needs to reflect risk profiles
- Needs to be phased-in in stages
- Needs to be quantitative and defensible

3.2. Risk Profile Tool

The Cyber Security Framework begins with a Risk Profile Tool, developed with input from the Cyber Security Working Group and specifically tailored to the inherent risks in Ontario's LDC community. The Tool allows each Ontario LDC to be categorized objectively. Based on size, maturity and capability, each Ontario LDCs 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 a 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 Risk Profile Tool is based on the following questions with weighed scoring to produce a Risk Profile number. The following is the current Risk Profile Tool, which will continue to be updated based on further reviews and feedback:

Figure 31: 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 work from home and remote offices
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 centres
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

#	Question	Response				Risk Factor				Additional Context
8	Does your entity process credit card transactions or pre-authorized bank payments?	Yes	No			3	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.
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?	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	10-50	>50		1	3	5		Third parties include third party vendors, service providers, etc.
15	Does your entity outsource any IT or OT services?	Yes	No			5	0			This refers to any application that is outsourced
16	Does your entity have a SCADA 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

#	Question	Response				Risk Factor				Additional Context
21	Does your entity have Distribution Automation technology?	Yes	No			3	0			This refers to automated technology (e.g. reclosers / breaker control) deployed within the service territory
22	Does your entity provide smart energy technology for your customers?	Yes	No			3	0			This include 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	1-10	10-50	>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 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.
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.

#	Question	Response				Risk Factor				Additional Context
35	Does your entity have Distributed Energy Resources / Microgrids connected to your systems?	Yes	No			3	0			This refers to any solar / wind / renewable systems and / or full microgrid 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 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 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.
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.

The Risk Profile Tool calculates the profile score and, based on the research, an LDC can be categorized as High, Medium or Low (baseline).

Based on initial testing and piloting with five (5) representative LDCs, the following ranges for High, Medium and Low were developed:

Figure 32: Risk Profile Ranges

Type	Range
Max Resultant Risk Factor:	190
Min Resultant Risk Factor:	10
Low Risk Profile Range:	0 -70
Medium Risk Profile Range:	71 – 120
High Risk Profile Range:	121 - 190

To validate the efficacy of the Tool and the delineation between the profiles, a Cyber Security Working Group was held on November 21, 2016 to test the Tool with LDCs of various perceived levels of risk. Three groups were each given a scenario which mimics the profile one would expect from running the Tool for an entity that has either a high, medium or low level of inherent risk. As a result of the testing, the ranges for each of the profiles were adjusted and additional questions were added to the risk profile tool for the next iteration. As well, the group appreciated the ease of use and objectivity of the tool.

3.3. NIST Controls and Privacy Principles

Regardless of whether an entity has a High, Medium or Low Risk Profile, privacy compliance is mandatory. Accordingly, we have 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, we have created 11 privacy controls that express the other nine (9) Fair Information Principles, and we have incorporated them in among 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 33: 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, Sch 1, s.4.1, 4.2, 4.3 GAPP, 1.2.3, 8.2.1

#	Category	Subcategory	Informative References
2	Asset Management	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
3	Business Environment	D.BE-P1 - Senior management is committed to a privacy respectful culture	PIPEDA, Sch 1, 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
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. The GAPP are 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.

3.4. Initial Achievement Level

Given that all LDCs / non-bulk system operators are at a starting point, we need to pick an initial level for each of the risk profiles. We also wanted to align to 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 Cyber Security Working Group meetings, we conducted a breakout session to test the applicability of various maturity models. The working group provided feedback that the 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 providing an integrated approach.

The following are the Maturity Indicator Levels (MIL) in the C2M2 model:

Figure 34: Initial Achievement Level

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

For the initial achievement levels for the three risk profiles we have selected MIL1 as the starting point. There will be a specified period of time allocated for the LDCs to attain the initial achievement levels. And then from there, as appropriate, maturity progress will be required (i.e. MIL1 to MIL2/3) over time.

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

3.5. 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 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 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

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

Figure 35: SAQ Definitions

Response	Definition
Yes	The expected testing has been performed and all elements of the requirement have been met
Yes with CCW[65]	The expected testing has been performed and the requirement has been met with the assistance of a compensating control.
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.

Figure 36: SAQ Model

			Check one response for each question				
Function	**Subcategory**	**Expected Testing Response**	**Yes**	**Yes with CCW**	**No**	**N/A**	**Not Tested**
IDENTIFY (ID)	**ID.AM-1**: Physical devices and systems within the organization are inventoried	- Review written policy and procedures - Review asset management inventory files					
	ID.AM-3: Organizational communication and data flows are mapped	- Review written policy and procedures - Interview personnel					
PROTECT (PR)	**PR.AC-3:** Remote access is managed	- Review written policy and procedures - Examine privileged and general user IDs and associated authorizations					
	PR.AT-1: All users are informed and trained	- Review training material - Review list of staff training programs and associated completion checklists					

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

Management Attestation / Certification

The SAQ reporting will result in a "Management Attestation" such as outlined below. This attestation should be provide by the LDC CEO, ensuring that appropriate attention and focus is undertaken to address both determining current compliance and the potential follow-up remediation activities required.

Figure 37: Compliance Rating

	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.

As the Framework evolves along with the maturity of the LDC, "Stage 2" of the reporting and audit assurance process will be implemented. This stage will involve more rigor regarding the assessment of the LDC control environment as it relates to cybersecurity and associated elements (i.e., policies, processes, resources, etc.).

Within this stage, the CCA or centralized compliance authority will establish risk-based and rotational testing consisting of:

- Self-assessments
- Desktop audits
- On-site tests, by CCA or accredited independent 3rd party

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).

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[66]. Identifying key risk indicators as a standard reporting and measurement metric across the LDCs will assist the OEB 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 the LDC is in agreement with the OEB in terms of the KRI being 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[67].

[66] ISACA, The Risk IT Framework Excerpt, 2009, The Risk IT Framework Excerpt, 2009
[67] ISACA, The Risk IT Framework Excerpt, 2009, The Risk IT Framework Excerpt, 2009

- 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 performance of the industry.

The measurement of KRIs will show the following benefits to the OEB, 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 of improvement by analysis of trends
- Assist in continuously improving the governance, risk and compliance environment

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

Industry best practice

The following table highlights research conducted in Task #4. It made the following recommendations based on industry best practice. The table also provides a response into how the Framework and its elements have included the recommendations in this implementation plan.

Figure 38: Implementation Plan Recommendations

Recommendation from Task #4	Implementation Plan Response
Flexibility – the risk based strategies should be flexible enough to integrate with existing risk management efforts of the LDCs.	We have leveraged the NIST Cyber Security Framework along with other existing standards and information references in the development of the Framework as described above. This includes addressing privacy as well. The model follows the risk management principles and concepts as discussed in Task #4 discussion paper (Establishment of Risk Based Vulnerabilities). Since the solution is based on existing standards and information resources, an LDC that has existing risk management practices should be able to readily adopt the Framework.

Recommendation from Task #4	Implementation Plan Response
Sufficient guidance – there will be the need to have a clear set of processes associated with the use of the Framework including specific informative references and illustrative controls. This sufficient guidance can be leverage against existing tools and models such as C2M2 and Privacy by Design.	Guidance can be categorized as follows: *Framework guidance* While this plan provides a tactical view as to how the Framework can be implemented, it only calls out where sufficient guidance will need to be developed during implementation. Using a two stage approach, as described below, will allow for easier adoption with less upfront guidance required. *Cybersecurity maturity guidance* Additionally, as information is gathered from the reporting elements of the Framework, the industry may want to provide standard guidance for areas where they view the sector as needing additional knowledge. A few of these areas became evident through the research conducted in the Discussion Paper for Task #4.
Leverage existing tools – The NIST cyber security framework is being adopted very widely and already has a number of organisations building out implementation approaches and tool kits. Examine these and leverage what would be of greatest value to this program. For example US-CERT has a voluntary NIST self-assessment program that has a myriad of tools to assist organisations in communications, assessments[68]	The Framework is based on NIST's Cybersecurity Framework (NIST Cyber Security Framework) and includes interwoven elements of privacy from informative resources such as PIPEDA and GAPP. The AESI team are also leveraging existing connections with the NIST development team to ensure we are able to adequately leverage existing tools.
Additional collaboration and study – the initiative could benefit from additional collaboration and study of risk management processes that are already in use at the LDCs. This could be done by sampling from a smaller volunteer group. This additional examination could provide insights on how elements for the Framework will integrate with existing efforts by the LDCs.	To address additional collaboration and study we will recommend pilot test groups in Stage 1 and Stage 2 of the implementation plan. This will provide insights to be gathered and improvements to be made to the Framework elements.
Phased and non-linear approach – "Walk before you run", implement the program in phases that allow the LDCs to absorb the framework tools and guidance in manageable chunks. If the LDCs can benefit from some immediate guidance that is easily and efficiently implemented without affecting alignment to the Framework then consider doing it sooner than later.	The two-staged approach, as described below, will allow the LDCs and the industry to absorb the Framework and its elements in manageable chunks.

[68] Critical Infrastructure Cyber Community Voluntary Program

Cyber Security Working Group Recommendations

Several CSWG meetings and individual interviews with a cross section of LDC members were conducted over the course of the project. We heard from the CSWG during these sessions and have directly reflected there feedback within different important elements of the Framework, as follows:

- Guidance must be concise and specific
- Leverage pilot test groups
- Tools should leverage risk profiles of LDCs as opposed to size
- Tools such as the NIST Cybersecurity Framework and the DOE C2M2 model can be very useful but direction is needed on use and support is required
- LDC Executives and Boards should be engaged and active in the implementation of the Framework
- There should be a phased-in implementation period, one that is manageable by LDC's with the ability for them to express when they perceive themselves ready to progress to the next phase
- Specific information about controls should remain in the LDC, not shared outwardly

We have factored all of these recommendations into the Framework.

4. Implementation Plan

The following is our recommended implementation plan:

Figure 39: Implementation Plan

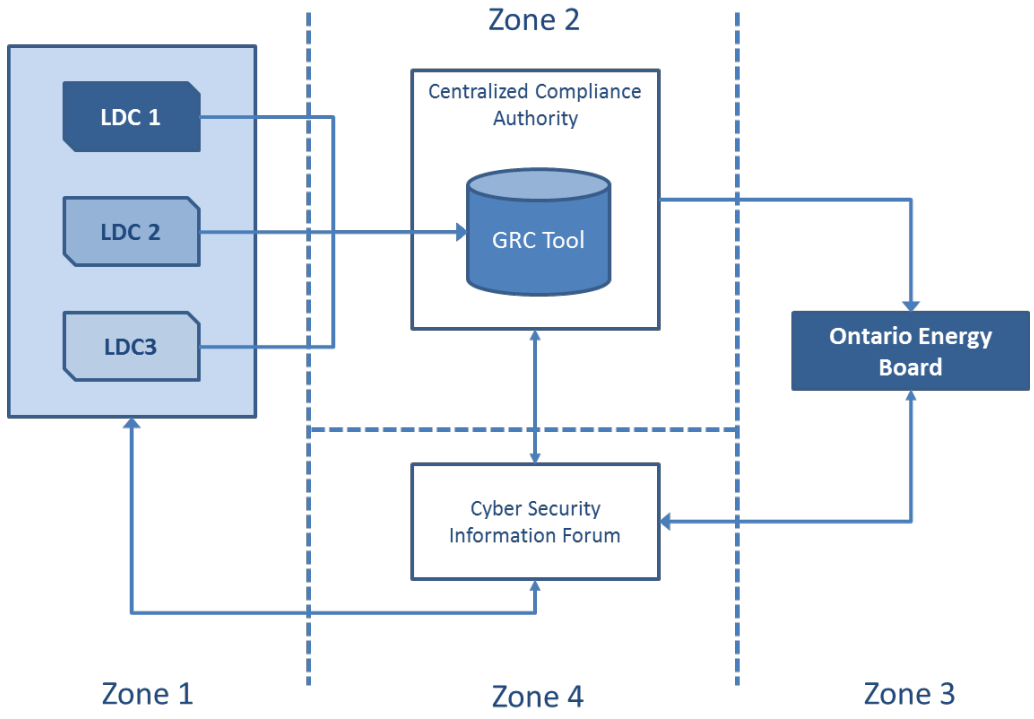
Framework Element	Stage 1 - Baseline	Stage 2 - Maturity
Risk Profile Tool	- Objective to establish baseline controls and security (the implementation of the Risk Profile Tool will result in articulated corresponding controls to be implement) - Determines inherent risk, makes recommendations for baseline 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

Framework Element	Stage 1 - Baseline	Stage 2 - Maturity
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

Information flow and zones

The following model serves as a reference for a discussion on information flow between LDCs 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 40: 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
- Develops specific reports back to the individual LDCs along with benchmarking against their peers.

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. Based on information collected, the OEB develops initiatives and guidance for the sector as well as driving policy.

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 41: 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 attestation section	➔	➔ Collected and archived	Attestation summary status provided	N/A

4.1. 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 encourage and nurtured.

4.2. Reporting

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 on 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 42: 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

4.3. Evolution – coincident with maturity levels

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 to their inherent risk profile with maturity implementation level of 1 (MIL1) in accordance to C2M2's implementation levels. The following table from C2M2 describes the maturity implementation levels.

Figure 43: 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 more complete or 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 more complete or 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 level of control expected in Stage 2 can be illustrated as follows:

Figure 44: 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

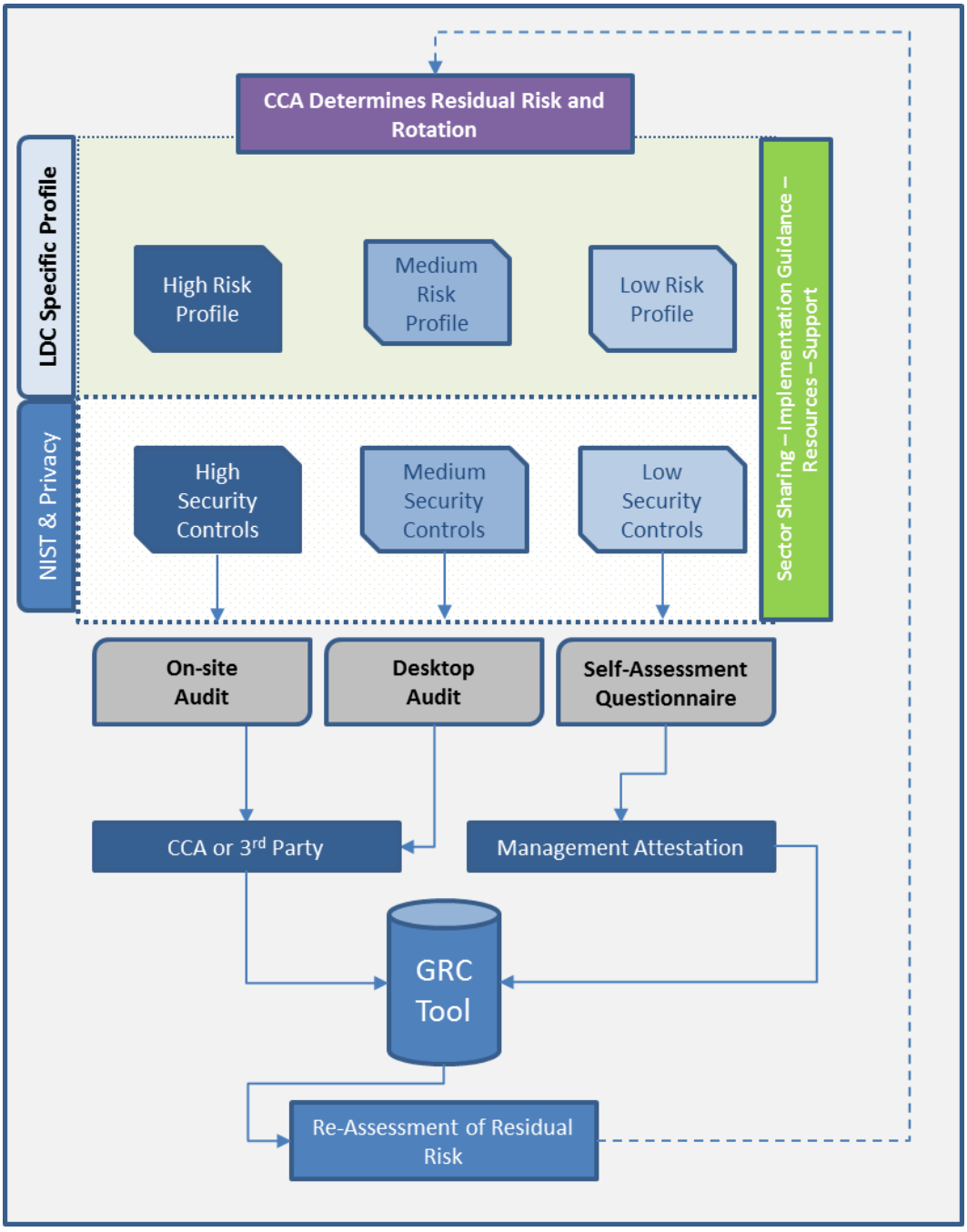
MIL2 → C2M2 ACM-1c,d

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

As such, the conceptual framework for Stage 2 would be as follows:

Figure 45: Ontario LDC Cybersecurity Framework, Stage 2



5. Conclusions and Recommendations

In keeping with OEB and the Cyber Security Working Group's framework guiding principles this Whitepaper has outlined a Cyber Security Framework that is:

- **Flexible and sustainable** – using the NIST Cyber Security Framework allows the Framework to accommodate constantly evolving technologies. The NIST Cyber Security Framework "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes."[69] Since the NIST Cyber Security Framework does not specify technology controls (e.g. firewalls) in its taxonomy it is flexible to adapt to cybersecurity outcomes of evolving technologies.
- **Measurable** – several mechanisms have been specified in this Whitepaper that will communicate the implementation success. In Stage 1, as LDCs report against the baseline of controls, success can be measured as a function of the LDCs meeting those baselines. As the Framework evolves in Stage 2, an outline for the development of KRIs is provided. As the KRIs are adopted uniformly by the LDCs, the OEB will be provided date that will enable audit and compliance activities as well as set guidance and initiatives
- **Efficient and aligned –** since the Framework is based on NIST Cyber Security Framework and is a taxonomy it can build off the efforts that LDCs have already begun, making it efficient and cost effective. It is not a reinvention of the wheel. This Framework has embedded privacy to ensure privacy regulations are met. It inherently makes reference to informative resources that are aligned with globally recognized standards such as C2M2, ISO 27001, GAPP, PIPEDA, COBiT and others.
- **Continuous improvement –** as a result of the development of the Framework and collective feedback from the Cyber Security Working Group, 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 will support continuous improvement and is a significant part of the illustrative information flow.
- **Innovation** Use of a Governance, Risk and Compliance (GRC) tool to automate, protect, segregate, summarize and report on the cybersecurity posture of individual LDCs and the sector as a whole. An information flow model is described which leverages a GRC tool to provide LDCs with the ability to securely collect and report information on their specific controls in an anonymous fashion thereby contributing to the knowledge of how the sector as a whole is dealing with cyber risks. This has the benefit of providing the OEB with the information that it requires to guide policy initiative for addressing cyber risks to the sector. It also has the benefit of allowing LDCs to benchmark their cyber security posture against their peers.

The outline of the Framework in this Whitepaper is only the beginning. The OEB and Cyber Security Working Group will need to continue to build off this work, in particular:

- Developing guidance and templates
- Continuing outreach and collaboration
- Piloting and improving the tools
- Developing detailed implementation plans

[69] Cybersecurity Framework FAQS Relationship Between Framework and Other Approaches

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.

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.

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[70] 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.

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 power necessary to meet regular demand. As the electricity grid continues to modernize, 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 (ES-ISAC): Gathers and analyzes 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.

[70] 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.

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).

Framework: Provide guidelines without being too detailed or rigid. Frameworks give the organization 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 are three pillars that work together for the purpose of assuring that an organization meets its objectives. Governance is the combination of processes established and executed by the board of directors that are reflected in the organization's structure and how it is managed and led toward achieving goals. Risk management is predicting and managing risks that could hinder the organization to achieve its objectives. Compliance with the company's policies and procedures, laws and regulations, strong and efficient governance is considered key to an organization's success. GRC is a discipline that aims to synchronize 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.

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.

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.

International Organization for Standardization (ISO): ISO is an independent, non-governmental international organization 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.

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 (LDCs): 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) monitors the operation of Ontario's electricity market and fosters compliance with the Ontario market rules and North American reliability standards. It does this through its prevention, monitoring, auditing, investigation, and enforcement activities.

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

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.

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 organization (ERO) for 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.

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.

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

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 web sites.

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.

Personal Information Protection Electronic Documents Act (PIPEDA): Governs how private sector organizations 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 organization'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 both 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 Operators (RTOs): An entity that is independent from 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.

Scorecard: Is a strategic planning and management system that is used to align business activities to the vision and strategy of the organization, improve internal and external communications, and monitor organization performance against strategic goals.

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 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.

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 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

Figure 1: Ontario LDC Cybersecurity Framework, Stage 1 1
Figure 2: Ontario LDC Cybersecurity Framework, Stage 2: Components / Index for High/Medium/Low 2
Figure 3: Ponemon – Impact of Third Party Risk 4
Figure 4: Project Overview 6
Figure 5: BitSight Insights Industry Benchmark Report 8
Figure 6: Cost of Cyber Crime 9
Figure 7: LDC Attack Surface Vulnerabilities 12
Figure 8: Ponemon Third Party Risk 12
Figure 9: Additional Third Parties Attack Vectors 13
Figure 10: DERs and Microgrids – Additional Attack Vectors 14
Figure 11: ICCP Topology 15
Figure 12: HONI TS Connection 16
Figure 13: Additional Bulk System Vulnerabilities 18
Figure 14: IESO Interties 20
Figure 15: Bulk to Non-Bulk 21
Figure 16: IESO Connection 22
Figure 17: Survey Results - Question 25 23
Figure 18: Survey Results - Question 26 24
Figure 19: Survey Results - Question 28 25
Figure 20: Implementation Approaches 26
Figure 21: Implementation Perspectives 27
Figure 22: What would Reporting look like? 27
Figure 23: What does Implementation look like to you? 28
Figure 24: NIST Framework Core Structure 32
Figure 25: Function and Category Unique Identifiers 33
Figure 26: NIST Functions, Categories, Subcategories and Informative References 34
Figure 27: NERC Regional Entities 35
Figure 28: DHS Process 37
Figure 29: CSA Z246 Process 38
Figure 30: Ontario LDC Cybersecurity Framework 45
Figure 31: Risk Profile Tool 46
Figure 32: Risk Profile Ranges 50
Figure 33: Privacy Controls 50
Figure 34: Initial Achievement Level 52
Figure 35: SAQ Definitions 53
Figure 36: SAQ Model 53
Figure 37: Compliance Rating 54
Figure 38: Implementation Plan Recommendations 55
Figure 39: Implementation Plan 58
Figure 40: GRC Model 59
Figure 41: Zone Reporting Elements 62
Figure 42: Audit Review Activity 63
Figure 43: C2M2 Maturity Implementation Levels 63
Figure 44: Stage 2 Controls 64
Figure 45: Ontario LDC Cybersecurity Framework, Stage 2 65

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: Security Controls and Risk Profiles Requirements, Stage 1

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
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	☑	☑	☑	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 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.
		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	☑	☑	☑	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 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.
		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	☑	☑	☑	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 flows maps may include a number of different artifacts, 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.
		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	·**PIPEDA**, Sch 1, s.4.1, 4.2, 4.3 ·**GAAP**, 1.2.3, 8.2.1	☑	☑	☑	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.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
		collection, use and disclosure of such information, and the sensitivity of such information.						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	☑	☑	☑	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 suppler, 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	☑	☑		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 assets exposure in the attack surface (i.e. inherent security risk profile). For example, a web server in a DMZ would might normally be considered high risk due to high visibility to the public.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
		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	☑	☑	☑	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 and third-party stakeholders (e.g., suppliers, customers, partners) are established	·**COBIT 5** APO01.02, DSS06.03 ·**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-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 specific task that involve 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	☑	☑	☑	C2M2 EDM-1b: "Important customer dependencies are identified (i.e., external parties that are dependent on the delivery of the function including operating partners)"	Artifacts 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 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	·**COBIT 5** APO02.06, APO03.01 ·**NIST SP 800-53 Rev. 4** PM-8	☑	☑	☑	C2M2 EDM-1b: "Important customer dependencies are identified (i.e., external	Artifacts 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:

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
		its industry sector is identified and communicated					parties that are dependent on the delivery of the function including operating partners)"	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 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	☑	☑	☑	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	☑	☑	☑	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 depend, including operating partners)"	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 assets exposure in the attack surface (i.e. inherent security risk profile). For example, a web server in a DMZ would might normally be considered high risk due to high visibility to the public.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
		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	☑	☑	☑	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	☑	☑		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 artifacts 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

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
								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 inform the management of cybersecurity risk.	**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 ·**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	☑	☑	☑	A security policy has been developed and communicated to all employees.	An information security policy is 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 - 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	☑	☑	☑	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 specific task that involve information security.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
								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)	☑	☑	☑	Legal and regulatory requirements have been reviewed and understood.	
		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	☑	☑	☑	A policy requires reasonable efforts to ensure that customers are notified of the purposes for which their information is collected, how it is used and when and how it will be disclosed.	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 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	☑	☑	☑	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	☑	☑	☑	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.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**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	☑	☑	☑	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 organizations risk assessment process, 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 artifacts similar to the above exist, they should also be addressing cybersecurity related risks.
		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	☑	☑		C2M2 TVM-2a: "Information sources to support cybersecurity vulnerability discovery are identified (e.g., ES-ISAC, ICyber Security-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 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.
		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	☑	☑	☑	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	☑	☑		C2M2 TVM-1a: "Information sources to support threat management activities are identified (e.g., ES-ISAC, ICyber Security-CERT, US-CERT, industry associates, vendors, federal briefings)" C2M2 TVM-1b:	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. 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

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
							"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, ICyber Security-CERT, US-CERT, industry associations, vendors, federal briefings, internal assessments)" C2M2 TVM-2b: "Cybersecurity vulnerability information is gathered and interpreted for the function"	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	☑			C2M2 TVM-1a: "Information sources to support threat management activities are identified (e.g., ES-ISAC, ICyber Security-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 organizations 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	☑			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, and impacts are used to determine risk	·**COBIT 5** APO12.02 ·**ISO/IEC 27001:2013** A.12.6.1 ·**NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16	☑			C2M2 RM-1c (MIL3): "Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing,	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

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
							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)"	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	☑			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	☑	☑	☑	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 process, cybersecurity related risks are identified, registered and a risk mitigation plan is in place. Indicators that an organization does this include artifacts such as: - Risk strategy - Threat risk assessments - Risk register - Enterprise risk management program If artifacts similar to the above exist, they should also be addressing cybersecurity related risks. The processes documented in artifacts 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	·**COBIT 5** APO12.06 ·**ISA 62443-2-1:2009** 4.3.2.6.5 ·**NIST SP 800-53 Rev. 4** PM-9	☑	☑		C2M2 RM-1c (MIL3): "Organizational risk criteria (objective criteria that the	As part of the organization's risk management processes a set of criteria exist that enable the organization to consistently evaluate risks.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
		expressed					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 organization-specific risk taxonomy is documented and is used in risk management activities"	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.
		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	☑	☑		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	☑	☑	☑	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	☑	☑	☑	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,	An access control policy is in place and is followed for provisioning, changing or terminating access for employees and services to the organizations 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

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
							keys)" C2M2 IAM-1c: "Identities are deprovisioned when no longer required"	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 an 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 ·**NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 ·**GAPP**, 8.2.3	☑	☑	☑	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"	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 centers should be highly restricted. Typical controls include: - Visitor sign-in sheets - 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	☑	☑	☑	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,	☑	☑	☑	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.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
			AC-6, AC-16					
		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	☑	☑		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 consistent with related policies, procedures, and agreements.	**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 ·**NIST SP 800-53 Rev. 4** AT-2, PM-13 ·**GAPP**, 1.2.10, 5.1.1, 10.2.5	☑	☑	☑	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 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 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	☑	☑	☑	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.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
		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	☑	☑	☑	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 are adhered 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	☑	☑	☑	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, ·**NIST SP 800-53 Rev. 4** AT-3, PM-13 ·**PIPEDA**, Sch1, s.4.1 ·**GAAP**, 1.1.2	☑	☑	☑	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 business issue. This should be reflected in board meeting minutes and be a part of board meeting agendas.
		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	☑	☑	☑	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	**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	☑	☑	☑	C2M2 TVM-1c: "Threats that are considered important to the function are addressed (e.g., implement mitigating	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

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
	risk strategy to protect the confidentiality, integrity, and availability of information.		·**NIST SP 800-53 Rev. 4** SC-28 ·**PIPEDA**, Sch1, s.4.7 ·**GAPP**, 8.2.1				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)"	- 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	☑	☑	☑	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 ·**GAPP**, 8.2.1	☑	☑		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.
		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	☑	☑		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 use of memory, disk space and network speed and throughput. These metrics are trended over time to provide management a view as 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.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
		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	☑	☑		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	☑			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	☑			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 commitment, and coordination among organizational entities), processes, and procedures are maintained and used	**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 ·**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	☑			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: "Configuration baselines are used to configure assets at deployment"	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. Typically organizations have: - Build books - Hardening standards - Configuration Management database - Change management processes
		PR.IP-2: A System Development Life Cycle to manage systems is	·**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,	☑			C2M2 ACM-3d (MIL2): "Change management practices address the full	Typically organizations have a formal system development lifecycle. Popular ones include “waterfall”; “spiral”; “Agile software development”; “rapid prototyping”; “incremental”;

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
	to manage protection of information systems and assets.	implemented	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				life cycle of assets (i.e., acquisition, deployment, operation, retirement)"	and “synchronize and stabilize”. This should be formally documented. For cybersecurity organizations should consider: - Using secure coding techniques such as OWASP - 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	☑	☑		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. [source: https://en.wikipedia.org/wiki/Change_management_(ITSM)] 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	☑	☑	☑	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 ·**PIPEDA**, Sch1, s.4.7 ·**GAPP**, 8.2.1, 8.2.3	☑	☑	☑	C2M2 ACM-4f (MIL3): "Asset inventory, configuration, and change management policies include compliance requirements for specified standards and/or guidelines" C2M2 RM-3f (MIL3):	An operations manual should exist to ensure the operating environment for physical assets meet the manufacturer's recommended requirements for operations. In data centers 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	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
							"Change logs include 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	☑	☑	☑	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	☑	☑		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	☑			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, ICyber Security-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 it's 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	☑	☑	☑	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	☑	☑		C2M2 IR-3e (MIL2): "Cybersecurity event and	Typically organizations will conduct disaster recovery exercises to test the availability of systems during a crisis.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
			·**ISO/IEC 27001:2013** A.17.1.3 ·**NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14 ·**PIPEDA**, Sch1, s.4.7 ·**GAPP**, 1.2.7, 8.2.7				incident response plans are exercised at an organization- defined frequency" C2M2 IR-4f (MIL2): "Cybersecurity event and incident response plans address OT and IT assets important to the delivery of the function"	This should be conducted at least annually. Some organizations also test their security incident response plans through threat scenario and table top exercises. This is highly recommended.
		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	☑	☑	☑	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	☑	☑	☑	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	☑	☑		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	☑			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	·**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	☑			C2M2 SA-1a: "Logging is occurring for assets important to the function where possible" C2M2 IR-1c:	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	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
		that prevents unauthorized access	·**NIST SP 800-53 Rev. 4** MA-4 ·**PIPEDA**, Sch1, s.4.7 ·**GAPP**, 8.0				"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 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	☑			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 behavior. This could include the misuse of privileged access, failed login attempt and other system events that could be indicative of an attack. 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	☑	☑	☑	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	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.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
							required"	
		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 ·**GAPP**, 8.0	☑	☑	☑	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.
		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	☑	☑	☑	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	☑	☑		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	☑			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"	Event information is analyzed and reviewed against threat advisory services.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
							C2M2 IR-3h (MIL3): "Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken"	
		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	☑			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	☑			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 communicated to customers	·**PIPEDA**, Sch1, s.4.1.4, 4.6, 4.8, 4.9, 4.10 ·**GAPP**, 6.0, 10.0	☑	☑	☑	A policy is published (ex. intranet, posters, bill insert) which advises customers that they have access to their personal information for review and update, and how to contact the entity in the event of a privacy question or complaint.	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 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	☑			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	**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	☑	☑		C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)" C2M2 SA-2b: "Operational environments are	Monitoring of critical systems is performed and logs are reviewed within 90 days.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
	and verify the effectiveness of protective measures.						monitored for anomalous behavior that may indicate a cybersecurity event"	
		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	☑	☑		C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)" C2M2 SA-2b: "Operational environments are monitored for anomalous behavior 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	☑			C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)" C2M2 SA-2b: "Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event"	Personnel are 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 ·**NIST SP 800-53 Rev. 4** SI-3	☑	☑		C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)" C2M2 SA-2b: "Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event"	Malware detection and isolation is performed for critical system environments.
		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	☑			C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)" C2M2 SA-2b	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	☑			C2M2 EDM-2a: "Significant cybersecurity risks due to suppliers and other dependencies are identified and addressed" C2M2 SA-2a: "Cybersecurity monitoring activities are performed	Access points for all third parties with access to critical system environments are monitored.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
							(e.g., periodic reviews of log data)" C2M2 SA-2b: "Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event"	
		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	☑			C2M2 SA-2a: "Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)" C2M2 SA-2b: "Operational environments are monitored for anomalous behavior 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	☑	☑		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	☑	☑		C2M2 WM-1a: "Cybersecurity responsibilities for the function are identified"	The Cyber Security Incident Response Plan includes thresholds, process, and roles and responsibilities.
		DE.DP-2: Detection activities comply with all applicable requirements	·**ISA 62443-2-1:2009** 4.4.3.2 ·**ISO/IEC 27001:2013** A.18.1.4 ·**NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4	☑	☑		C2M2 IR-1d (MIL2): "Criteria are established for 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	Detection activities comply with all privacy, legal and regulatory requirements.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
							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	☑			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	☑			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, ICyber Security-CERT)" C2M2 ISC-1a: "Information is collected from and provided to selected individuals and/or organizations"	The Cyber Security Incident Response Plan includes thresholds, process, and roles and responsibilities.
		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	☑			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 and maintained, to ensure timely response to detected cybersecurity events.	**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 ·**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	☑	☑	☑	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,	The Response Plan with thresholds, roles and responsibilities, and process is executed.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
							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**, Sch 1, 4.1 ·**GAPP**, 1.1.2, 1.2.7	☑	☑	☑	C2M2 IR-3a: "Cybersecurity event and incident response personnel are identified and roles are assigned"	The Response Plan with thresholds, roles and responsibilities, and 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**, Sch 1, 4.7 ·**GAPP**, 1.2.7	☑	☑	☑	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 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	☑	☑		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, ICyber Security-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 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**, Sch 1, 4.7 ·**GAPP**, 1.2.7	☑	☑		C2M2 IR-3d (MIL2): "Cybersecurity event and incident response is performed according to defined procedures that	The Response Plan with thresholds, roles and responsibilities, and process is executed.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
							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 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	☑	☑	☑	C2M2 ISC-1a: "Information is collected from and provided to selected individuals and/or organizations"	The Response Plan with thresholds, roles and responsibilities, and 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	☑			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	☑			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	☑			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.,	Forensics are performed for impactful incidents and events, and adjustments are made to controls as appropriate.

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
							triage, handling, communication, coordination, and closure)"	
		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	☑			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 ·**GAPP**, 1.2.7	☑			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.
		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	☑			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	☑	☑		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	☑	☑	☑	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	☑	☑	☑	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	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	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
							at an organization-defined frequency"	
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	·**CCSCSC** 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	☑	☑	☑	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	☑	☑		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 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"	Subsequent to the execution of the Response Plan within 30 days lessons learned are identified and incorporated into the security controls and Response Plan.
		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	☑	☑	☑	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	**RC.CO-1:** Public relations are managed	·**COBIT 5** EDM03.02 ·**GAPP**, 1.2.7	☑	☑	☑	C2M2 RM-1c (MIL3): "Organizational risk criteria	Upon detection of a significant incident the appropriate

Function	Category	Subcategory	Informative References	High Risk	Med Risk	Low Risk Baseline	Initial Achievement Level (C2M2 is MIL1 unless otherwise specified)	Illustrative Examples
	activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other Cyber SIRTs, and vendors.						(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"	forms of public relations are engaged.
		RC.CO-2: Reputation after an event is repaired	·**COBIT 5** MEA03.02 ·**GAPP**, 1.2.7	☑	☑		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	☑	☑	☑	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 process is executed.