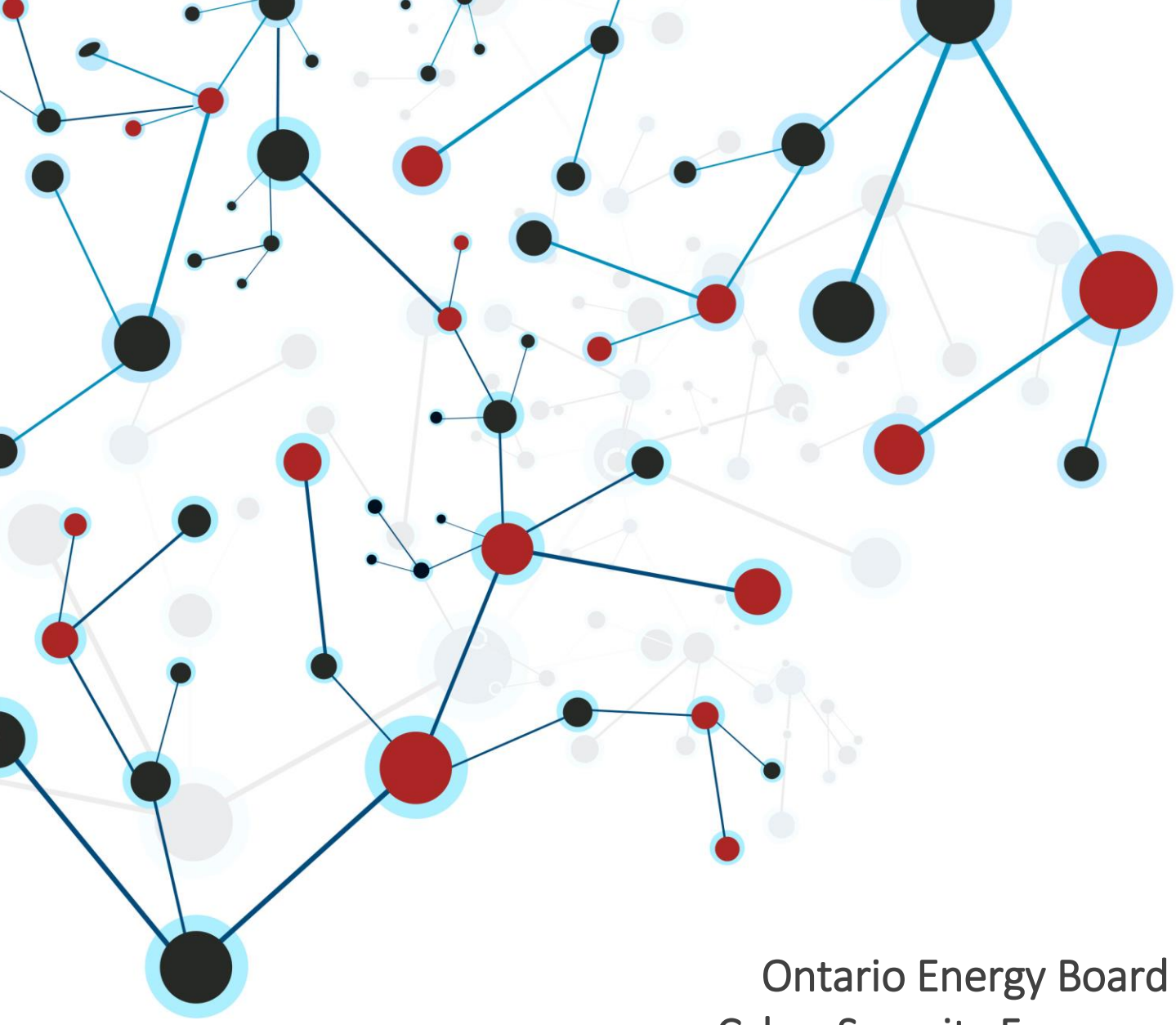

Ontario Energy Board
Cyber Security Framework

Accelerating compliance using Security-as-a-Service (SECaaS)

Stratejm

Office: 888.876.0504

Email: info@stratejm.com

Website: www.stratejm.com

About this Whitepaper

The Ontario Energy Board recently published a report entitled "*Cybersecurity Framework to Protect Access to Electronic Operating Devices and Business Information Systems within Ontario's Non-Bulk Power Assets."* As Ontario's independent energy regulator, this represents a significant step toward strengthening the industry focus on cyber security and privacy. The framework defines a process and provides tools to facilitate continuous improvement in organizations that are subject to OEB regulatory oversight.

This whitepaper introduces the OEB Cyber Security Framework, describes the basic steps in the process and assesses its impact on the Local Distribution Companies (LDCs). The benefits of leveraging Security-as-a-Service to meet the compliance requirements in a timely and more cost-efficient manner are also identified.

Contents

Introduction

The Ontario Energy Board (OEB) published its Cybersecurity Framework Staff Report and Whitepaper in June, 2017. The objective of their initiative is to increase security and privacy in Ontario's Local Distribution Companies (LDCs), with the overall goal of reducing cyber risk and improving service resilience.

The OEB Cyber Security Framework (OEB-CSF) is an extended version of the National Institute of Science and Technology (NIST) Framework. It also addresses confidentiality for the consumer information that is handled and stored by the electricity distribution sector.

The OEB initiative aims to increase the maturity of the security processes and ensure sector-wide consistency in the reporting of security and privacy status and incidents.

Critical infrastructure Security

The reliable delivery of electricity, natural gas and water is generally considered to be essential to modern living. The electricity, natural gas and water distribution infrastructures must, therefore, be protected from service disruption, system damage or component destruction. With cyber-physical systems, at least as much attention must be paid to protecting the software as is given to monitoring the physical assets.

LDC operational systems, usually referred to as Operations Technology (OT), are most often implemented using SCADA-based systems. But OT systems are now being treated as just one of the use cases in the rapidly expanding Internet of Things (IoT) portfolio, and "smart" SCADA systems are starting to evolve and adapt to the IoT standards.

SCADA has a lengthy history dating back to the 1960s that pre-dates most current Internet, Cloud and IoT systems.

Modernizing SCADA systems to use TCP/IP-based networks has significantly increased the cyber-attack threat surface. Enhancing cyber security and privacy has become fundamental for all types of critical infrastructure systems.

The demand for and benefits of increased integration of OT and IT is a recent development, basically derived from the increasing opportunities that can be derived from data analytics, open data, smart meters and customer self-service.

The potential for highly-visible disruption (i.e., the lights go off!) makes electricity, natural gas and water infrastructures attractive targets for terrorists and cyber warfare. With IoT-based systems, almost every "thing" can be a breach target, and there is no shortage of news stories to prove it[1].

Cyber security has become an "elephant in the room" for Ontario's LDCs, just as it is for most large enterprises. The OEB-CSF helps to minimize the impact of any security and privacy weaknesses that exist in the technologies and products that have been installed.

[1] For example, see this July 7th report from UK-based Independent news.

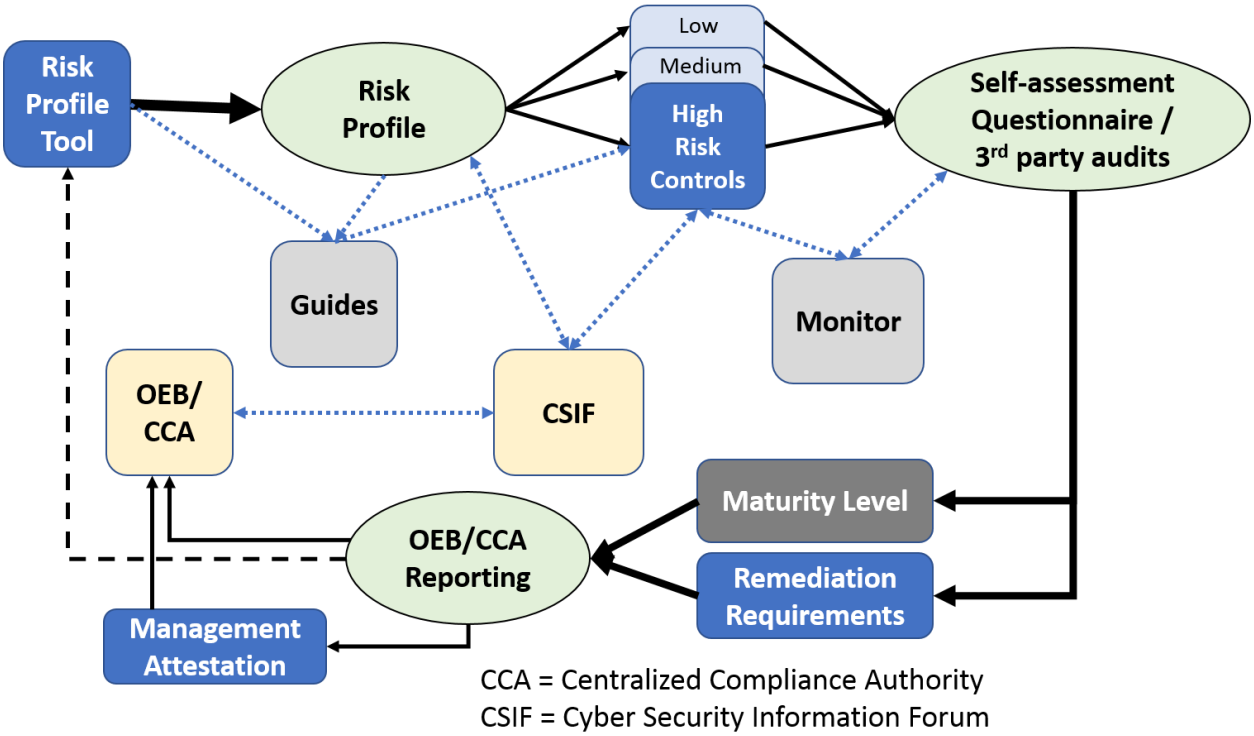

Figure 1: The OEB Cyber Security Framework process

The OEB Cyber Security Framework

In February 2016, the OEB initiated a comprehensive review of cyber security for the non-bulk electrical grid and its associated business systems. Given the critical importance of electricity distribution and the business benefits of IT/OT integration, it is not surprising that awareness of security and privacy issues is growing and that industry cooperation is starting to happen.

The result of the review was the publication of the draft OEB-CSF and its supporting documents and tools.

The LDCs will implement the controls and standards and will execute the processes defined in the OEB-CSF annually. **Figure 1** illustrates the macro steps involved (based on the June draft report).

1. The risk profile questionnaire

The first step is to establish a risk profile to serve as a baseline for future planning. The result is an organizational ranking of High, Medium or Low risk.

The risk profile is determined by answering the 46 questions that are included in the OEB whitepaper. All LDCs use the same set of questions to assess their inherent risks. Standardizing the tool helps to preserve consistency and objectivity across all LDCs and allows the OEB to aggregate and compare the data.

The OEB also uses the risk profile to confirm that the LDC has examined its risks, has established its cyber security gaps and objectives, and has assessed its current capabilities relative to the objectives.

The profile questions are both technical and business-oriented and are sector-specific.

Example questions include *"Does your entity process credit card transactions or pre-authorized bank payments?" "Does your entity have ICCP connections with the IESO or your transmission provider?"* and *"Does your entity serve any critical infrastructure installations?"*

Implications for the LDC:

LDCs must complete the questionnaire within three (3) months of the final approval of the OEB-CSF. ***CEO sign-off (attestation) is required.***

The risk profile leads directly to a security gap analysis and prioritization is needed for any security mitigation projects.

The LDC needs to re-evaluate its risk profile periodically or in response to changes in business, regulatory or technical circumstances.

Some LDCs will find it difficult to complete a self-assessment objectively. A knowledgeable cyber security partner can provide a valuable perspective at this stage.

2. OEB-CSF Security Controls

The OEB-CSF provides guidance as to which security and privacy controls are appropriate for each risk level. The controls are based on the NIST Framework and the Privacy by Design principles (which are described in more detail below).

The self-assessment identifies gaps in people, processes and technologies that need to be corrected. When the security control gaps are known, the LDC can take steps to implement the specific guidance that enables the security objectives to be met.

The real objective, however, is to get better at managing security risks and protecting against privacy breaches. Each LDC must determine how and when to implement the various controls and when to update any controls they may already have in place.

As an example, using the sample row in **Figure 2**, a software asset management capability would be required: *"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 or as sophisticated as an automated, Cloud-based asset discovery, management and tracking system.

Implications for the LDC:

LDCs will need to demonstrate increasing levels of maturity over time according to their individual security plans and needs.

Some controls are primarily internal procedures while others will involve technology upgrades or new systems (such as asset management).

LDCs can also use external partners to kick-start their plans and projects to expand upon existing security capabilities.

An asset management system, for example, could be implemented by a qualified Service Provider as part of, or separate from, Security-as-a-Service.

3. OEB Reporting

Reporting is an important component of the OEB-CSF process and will be mandatory when implemented. The reports will explicitly monitor LDC progress towards their targets and allow an industry-wide overview of the status and progress.

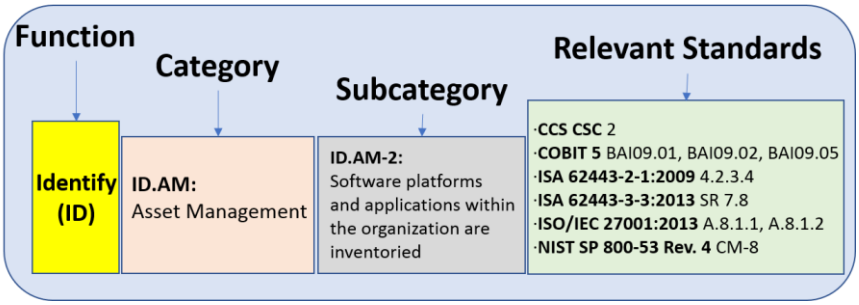

Figure 2: Sample framework row

Initial self-assessment report

To ensure that the OEB-CSF is being worked on, each LDC must provide an initial report within three (3) months after the final OEB-CSF report is issued, acknowledging that it:

- has reviewed and understood the OEB-CSF;
- has taken steps to plan and implement compliance;
- has assigned a team to assess risk and evaluate their current ability to implement the framework objectives to achieve such compliance; and
- confirms they will furnish an annual certification of compliance.

Annual reporting (beginning in 2018)

Reporting is to be implemented in two stages – the Initial Report, and Annual Reports.

Stage 1:

Within 12 months, the LDCs are expected to:

- Determine their risk profile;
- Understand their cyber security control requirements;
- Assess their current cyber readiness;
- Assess the effectiveness of their existing controls;
- Develop and implement action plans to remove deficiencies;
- Establish cyber security monitoring capabilities; and
- Provide the OEB with a certification confirming the above.

The initial target is to attain a Maturity Indicator Level of 1 (MIL1) which means that security processes are ad hoc or better. A specified time will be allocated for the LDCs to attain this level.

Over time, increases in maturity will be required (i.e., from MIL1 to MIL2/3) if appropriate.

The LDCs will self-certify their risk assessment, cyber security objectives and capability assessments. Each sub-category of the OEB-CSF table must be evaluated using the implementation response choices as indicated in the table:

Response	Definition
Yes	The expected testing has been performed and all elements of the requirement have been met.
Yes, with CCW	The expected testing has been performed and the requirement has been met with the assistance of a compensating control. (CCW = compensating control worksheet)
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 known 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.

Stage 2:

As the OEB-CSF evolves and LDC cyber maturity increases, the reporting and audit assurance processes will be expanded.

Stage 2 will involve a more rigorous assessment of the LDC control environment as it relates to cyber security policies, processes and resources.

As part of Stage 2, a Centralized Compliance Authority (CCA) will be established to serve as the sponsor for risk-based and rotational testing. This is expected to consist of:

- Self-assessments that allow the LDCs to report in a flexible and meaningful way, and could include a combination of the Self-Assessment Questionnaire and a set of Key Risk Indicators (KRIs);
- Desktop audits to look at policies and procedures, conducted internally by employees or by an external party; and
- On-site tests by the CCA or other independent accredited third parties.

KRIs linked to the risk profiles would serve as standard measurement metrics. They can also assist the OEB to identify areas of risk across the industry as well as within individual LDCs.

Implications for the LDC:

The LDCs will be required to develop governance policies and practices, implement tools to monitor progress based on metrics, and provide reports based on the OEB-CSF sub-categories and their related KRIs.

LDCs will need to perform self-assessments and ensure funding for improvements when needed.

Periodic auditing will also be required and must be supported by continuous data collection and business analytics.

A qualified cyber security partner could provide significant support both for collecting the required data and in preparing the reports. Shared tools also reduce costs and would leverage the service provider's experience.

4. Industry working groups

The OEB-CSF is expected to be supported by new industry working groups that will consult with both third-party stakeholders and the regulated entities.

LDCs are expected to participate in a mandatory Cyber Security Information Sharing Forum (CSISF) as is shown in **Figure 1**.

Shared sector ownership of the OEB-CSF will allow it to evolve and improve over time and will increase the sharing of experiences and enable more industry collaboration.

Implications for the LDC:

The LDCs will be expected to prepare for and participate in the various activities of the committees.

This would involve developing submissions, reviewing deliverables and assigning responsibilities to internal experts.

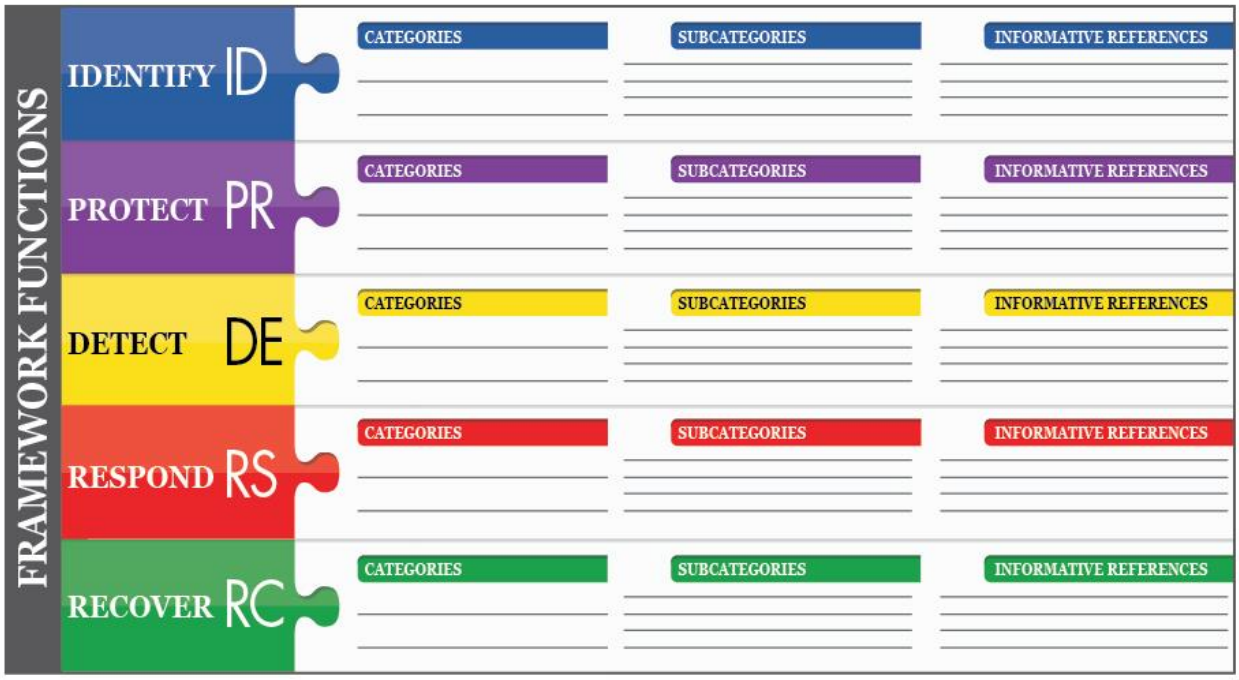

Figure 3: NIST framework elements

The Underpinnings for the OEB-CSF

The OEB-CSF was based on the NIST Framework Core for controls, the Cybersecurity Capability Maturity Model (C2M2) for measurements, and controls derived from the principles of Privacy by Design.

(a) The NIST Framework Core

The NIST Framework Core is a key part of the popular Framework for Improving Critical Infrastructure Cybersecurity published by the NIST in 2014 and updated on January 10, 2017 (released as Draft Version 1.1 for public review).

The Framework Core consists of a categorized set of cybersecurity activities and references, organized around particular outcomes. The Framework Core defines four major sub-divisions - ***Functions***, ***Categories***, **Subcategories** and ***Informative References***. **Figure 3** (above) is the NIST diagram showing the relationships among the elements.

The five functions could be viewed as a *"cyber security supply chain"* – they form a life cycle for processes associated with managing cyber security risk. The definitions for the functions are provided in the box.

Functions are divided into categories (e.g., ID.AM = Asset Management) and subcategories (e.g., ID.AM-1 – Physical devices and systems within the organization are inventoried), with each sub-category supported by informative references.

The references are to specific sections of standards, guidelines or practices that are common across critical infrastructure sectors. They illustrate a method for achieving the outcomes associated with each sub-category.

These various references are common across all the critical infrastructure sectors.

A sample row was shown earlier in **Figure 2**.

Identify: Develop the organizational understanding to manage cyber security risk to systems, assets, data and capabilities.

Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. This supports the ability to limit or contain the impact of a potential cyber security event.

Detect: Develop and implement the appropriate activities to identify the occurrence of a cyber security event. The Detect Function enables timely discovery of cyber security events.

Respond: Develop and implement the appropriate activities to take action regarding a detected cyber security event. The Respond Function supports the ability to contain the impact of a potential cyber security event.

Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event. The Recover Function supports timely recovery to normal operations to reduce the impact of a cyber security event.

The NIST Framework is a called a *"principle-based framework"* but it is not prescriptive. It allows cyber security risk management to be integrated into an organization's overall risk management process to:

- Address the interactions of multiple risks;
- Encompass the entire organization including both IT and OT;
- Ensure that decision-making includes a process of continuous improvement; and
- Refer to standards that can support risk management activities.

The OEB adaptation of the NIST Framework table is included in the whitepaper and is also available separately as a spreadsheet. The spreadsheet also includes risk ratings, C2M2 baseline levels and examples.

(b) The U.S. Department of Energy C2M2 Maturity Model

The U.S. Department of Energy developed the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). ES-C2M2 was designed to improve energy sector cyber security and to help organizations evaluate, prioritize, and improve their cyber security capabilities. It includes a maturity model, an evaluation tool, and DOE-facilitated self-evaluations.

ES-C2M2 maps to the NIST functions and categories. It groups cyber security practices into ten domains arranged according to maturity level. The four Maturity Indicator Levels (MILs) can be used both during normal operations and at times of crisis.

MIL0: Not Performed
MIL1: Initiated, but may be ad hoc
MIL2: Repeatable
MIL3: Managed/Adaptive

The OEB-CSF assigns a maturity level to each sub-category row. This ensures a more consistent benchmarking of LDC cyber security capabilities, facilitates sharing of knowledge and best practices, and can even guide cyber security investments.

(c) Privacy by Design Principles

Because the original NIST Framework did not fully address privacy, the OEB included sub-categories that reflect the Privacy by Design (PbD) principles that were originally developed by a former Information and Privacy Commissioner of Ontario.

PbD recommends inserting privacy and data protection functions into information technologies, organizational processes, networked architectures and entire systems of governance and oversight.

Privacy requirements and controls have been included at all risk levels in the OEB-CSF.

The seven foundational principles of PbD are listed in the box.

1. **Proactive, not Reactive; Preventative not Remedial:** Prevent privacy breaches from occurring by thinking about privacy before-the-fact.
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 is an essential component of the core design and architecture of systems and business practices.
4. **Full Functionality - Positive Sum, not Zero-Sum:** Accommodate all legitimate interests without the need to sacrifice functionality or security in the name of privacy.
5. **End-to-End Security - Full Lifecycle Protection:** Strong security is essential to privacy throughout the entire information management lifecycle.
6. **Visibility and Transparency - Keep it Open:** Trust but verify and ensure that business practices and technologies are operating according to stated promises and objectives.
7. **Respect for User Privacy - Keep it User-centric:** Protect the interests of the individual.

Benefits for the LDCs

The OEB believes its framework will increase awareness and commitment within the LDCs, will ensure consistency across the LDCs and will support improved electricity reliability, security and privacy across Ontario. The OEB-CSF will support the LDCs in assessing their risks, designing their controls, addressing identified gaps and implementing appropriate governance – all of which need to be done anyway for the LDCs to meet their regulatory requirements.

The OEB-CSF is also expected to reduce costs through increased sharing and collaboration among the LDCs, thereby encouraging collaboration for continuous improvement.

An industry-wide approach to security increases confidence in the solutions and provides the OEB with assurance that the appropriate level of cyber maturity can and will be achieved.

Since the OEB-CSF leverages existing standards, it can also provide guidelines and coordination with OEB legal and audit requirements. The policy and reporting requirements demonstrate that Ontario's LDCs are addressing cyber security risks and have common criteria to meet their reliability, security and privacy obligations.

As a side benefit, the OEB Staff Report also suggests that the proposed OEB-CSF can be adopted by other electricity transmitters and natural gas distributors to provide similar assurances to the OEB.

Security-as-a-Service (SECaaS)

LDCs will need assistance to comply with the OEB requirements in a timely manner. This is due to a variety of reasons including the complexity of issues, the lack of knowledge and experience in the technical aspects, or even just the shortage of staff for the effort involved, especially during the initial ramp-up.

Adopting a cyber Security-as-a-Service (SECaaS) as an approach is an appealing option for kick-starting the implementation of the OEB-CSF, especially when funding and expertise are scarce.

A SECaaS provider can be an invaluable partner if they know the existing LDC ecosystem, understand the various security standards and best practices, and have local Ontario-based expertise and experience. It can be very advantageous to use industry experts who know the needs of the LDCs and have experience with the NIST standards.

Many of the OEB-CSF sub-categories can be satisfied through *"as a service"* solutions that are available today.

The following table offers a more detailed mapping of typical SECaaS services to the requirements of the OEB-CSF.

NIST Categories	Security-as-a-Service Support
Identify	
• Asset management • Business Environment • Governance • Risk Assessment	A SECaaS provider can: • Develop resource inventories with extensions to include both IT and OT assets and component relationships; • Establish an information inventory including purposes for collecting data; • Map and maintain external links and supplier dependencies; • Provide assistance with asset and object prioritization; • Supply consultative services for organizational, policy, governance and risk management functions; and • Provide assistance in reviewing legal and regulatory requirements.
Protect	
• Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology	A SECaaS provider can: • Consult on access control policies and Identity Access Management processes; • Monitor adherence to policies for provisioning, changing or terminating access rights; • Assist with developing security and privacy training policies and practices; • Offer custom training services and awareness campaigns;

	• Assist with developing and disseminating policies and practices relating to the management of personal information; • Assist or provide change management processes and tools for full life cycle management of assets; • Provide assistance and consultation for DR/BC planning, testing and execution; • Provide or support a vulnerability management program; • Provide and support a Threat Intelligence System; • Collect threat intelligence and information concerning vulnerabilities from multiple sources including ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings, internal assessments.
Detect	
• Anomalies and Events • Security Continuous Monitoring • Detection Processes	A SECaaS provider can: • Monitor critical systems and review logs on an ongoing basis; • Analyze event information and review against threat advisory services: • Assist with the development and deployment of incident response plans; • Monitor physical and logical access points for unauthorized personnel; • Perform vulnerability scans for critical system environments; and • Review and test detection processes.
Respond	
• Response Planning • Communications • Analysis • Mitigation • Improvements	A SECaaS provider can: • Assist with response plan development and execution; • Provide notifications and help with investigating the highest priority notifications; • Assist with analyzing potential business and operational impacts; • Perform or assist with forensic analyses and recommend adjustments to controls as appropriate; • Help to address and mitigate high priority vulnerabilities as defined by threat advisory services and/or vendors; and • Identify lessons learned and incorporate them into the security controls and the response plan.
Recover	
• Response Planning • Improvements • Communications	A SECaaS provider can: • Maintain the recovery plan and assist with managing its use during recovery from an incident; • Facilitate de-briefings, capturing lessons learned and making changes to security controls and response plans

Next Steps

The LDCs can move forward with several priority activities to kick-start their participation in the OEB cyber security initiative. Some possible actions that do not need to wait for the finalization of the OEB-CSF are:

1. Complete a response to the Risk Profile Tool (as provided in the OEB whitepaper) to determine your initial profile ranking (which would be a High, Medium or Low risk).
2. Determine your current compliance status by completing the Self-Assessment Questionnaire for your risk profile. Determine which areas require further effort to achieve MIL1. Add any additional risk management functions that are specific to your LDC.
3. To the extent possible, prepare the initial report to the OEB (due 3 months after final approval of the OEB-CSF), acknowledging that you:
    - have reviewed and understood the OEB-CSF and its related documents;
    - have taken steps to plan and implement compliance;
    - have assigned a team to assess your risks and your current ability to implement the framework objectives to achieve such compliance; and
    - confirm you will furnish an annual certification of compliance.
4. Develop a roadmap of actions and/or projects that will be required over the first year of the process.

About the Author

Don Sheppard P.Eng. is a Senior Consultant with ConCon Management Services of Toronto, Ontario. He has been a consultant and advisor to IT managers for more than thirty years. Don has participated in the development of various ISO standards including the OSI Security Architecture and, more recently, the Cloud Computing Reference Architecture. Don developed service descriptions and facilitated threat risk analyses for a large government project. Don is also an active blogger.

About Stratejm Inc.

Stratejm has developed Canada's first cloud-based Cyber Security-as-a-Service offering, enabling enterprise customers to solve security problems in a secure, intuitive and cost-effective manner. Time-to-value is optimized and the enterprise is under no obligation to purchase new hardware or software. Stratejm's security platform is backed by a state-of-the-art Threat Intelligence Centre that is staffed by security professionals. Call 1-888-876-0504 or email to info@stratejm.com for further information.