OFFICE OF THE
AUDITOR GENERAL
MANITOBA

Web version

Manitoba Hydro

Managing Cyber Security Risk Related to Industrial Control Systems

Table of contents

Web version

Main points

What we found

Cyber security risk is defined as the potential for adverse events impacting organizational operations (including mission, functions, image and reputation), resources and other organizations due to unauthorized access, use, disclosure, disruption, modification, or destruction of information, information technology (IT) and/or operations technology (OT). (Source: *Electricity Subsector Cybersecurity Risk Management Process*, U.S. Department of Energy, May 2012)

Our objective was to determine whether Manitoba Hydro's risk management practices ensure the design of security controls over Industrial Control Systems (ICS) and related Information Technology (IT) reasonably mitigate identified cyber risks

We concluded that cyber security risks related to ICS systems are not identified, assessed and managed. Until Manitoba Hydro has assessed the risks to all ICS systems it cannot be certain that it has applied the appropriate level of controls to prevent unauthorized access, modification or damage to these vitally important systems.

We based our conclusion on the findings discussed in our report and summarized below.

Manitoba Hydro not aware of all significant ICS cyber security risks

Manitoba Hydro has not prioritized its ICS and related IT systems for criticality to its generating, transmitting and distributing processes. Manitoba Hydro's risk management process includes 52 risk profiles, but ICS cyber security risk has not been identified as a corporate risk profile and has not been assessed. And as such, has not been communicated to the Board. Without comprehensive and coordinated ICS cyber security risk assessments, Manitoba Hydro may not be able to design and implement effective security controls for its ICS systems. (**section 1**)

Manitoba Hydro must comply with the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards which include cyber security controls (see **Appendix A** for a description of NERC). Manitoba Hydro's NERC CIP compliance program, however, consistent with NERC requirements, focuses on assets critical to the bulk electric system and not risks to Manitoba Hydro operations. For NERC CIP compliance purposes, only 2 physical locations have been identified as housing critical ICS cyber systems which must be protected using NERC CIP standards. These systems do not necessarily represent the only ICS systems that are critical to Manitoba Hydro operations. NERC standards and related compliance efforts by Manitoba Hydro should not be interpreted as adequate corporate cyber security risk management.

> The **bulk electric system**, often referred to as the North American electric grid, includes electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment.

Many gaps in ICS security controls at sites we visited

The 6 locations we visited (4 generating stations, a modernized transmission substation, a high voltage direct current (HVDC) convertor station) make use of ICS systems and are critical to Manitoba Hydro operations. We compared cyber security practices in place at each location to Public Safety Canada's recommended best practices for industrial control systems as they represent the minimum standards that should be implemented by all industries that use ICS. While some ICS security controls are evident at each location, we identified serious weaknesses in cyber security controls. (**section 2**)

In **section 3**, we identify several factors that we believe led to this lack of attention to ICS cyber security risks:

- "Air-gap" and non-routable serial cables provide a false sense of security.
- Responsibility for corporate-wide cyber security has not been assigned to one executive.
- Comprehensive ICS cyber security policies not in place.
- Responsibility for physical security is fragmented.
- Lack of ICS security awareness program and training.
- Management only recently exploring benefits of IT/OT convergence. IT Security not yet involved.

Why it matters

To monitor and control the generation, transmission and distribution of electricity, as well as the distribution of natural gas, Manitoba Hydro uses many ICS systems. We chose to audit Manitoba Hydro's ICS systems because of the significant impact that a loss in the reliable flow of power and gas can have on public safety and on the provincial economy. ICS systems control and monitor actual physical devices that, if compromised, could result in unintentional and/or inappropriate commands that could lead to equipment malfunction, causing significant risk to the health and safety of Manitobans as well as the environment. It is essential that the risks to ICS systems are properly managed.

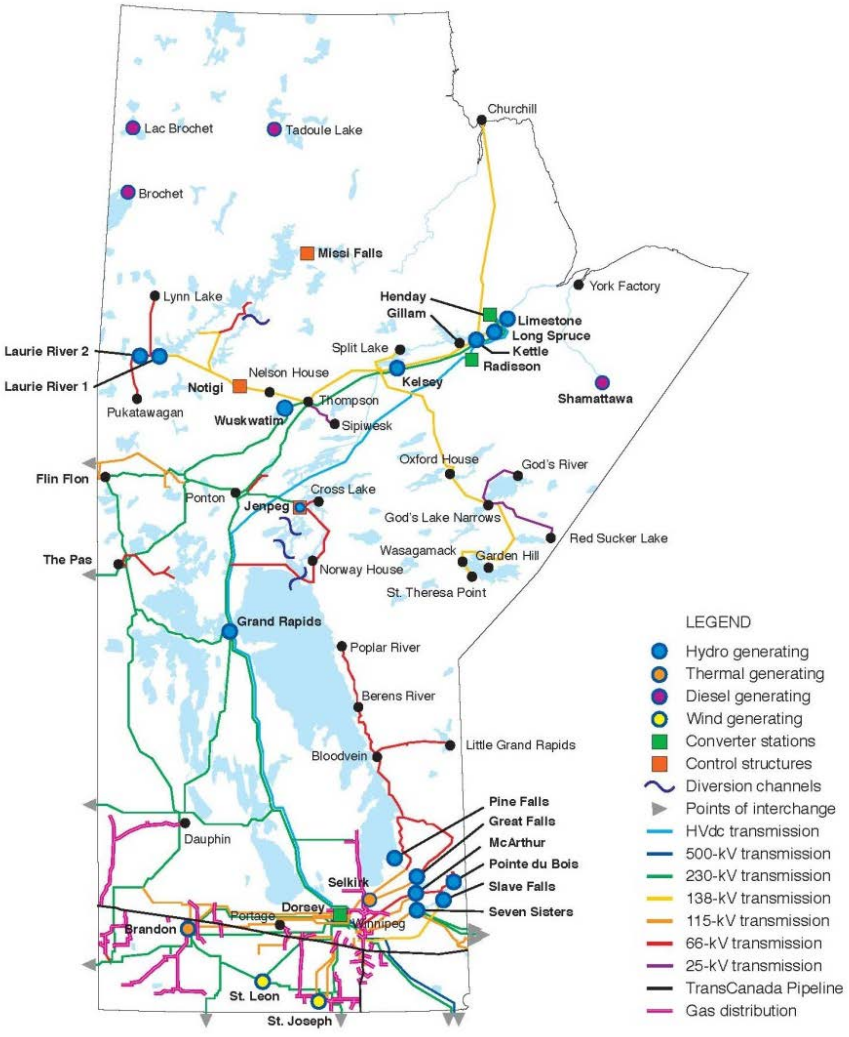
Background

About Manitoba Hydro

Providing reliable electricity is extremely difficult and technically complex. It involves real-time assessment, control and coordination of electricity production at generating stations, moving electricity across a network of transmission lines, and finally delivering the electricity to customers by means of a vast distribution network.

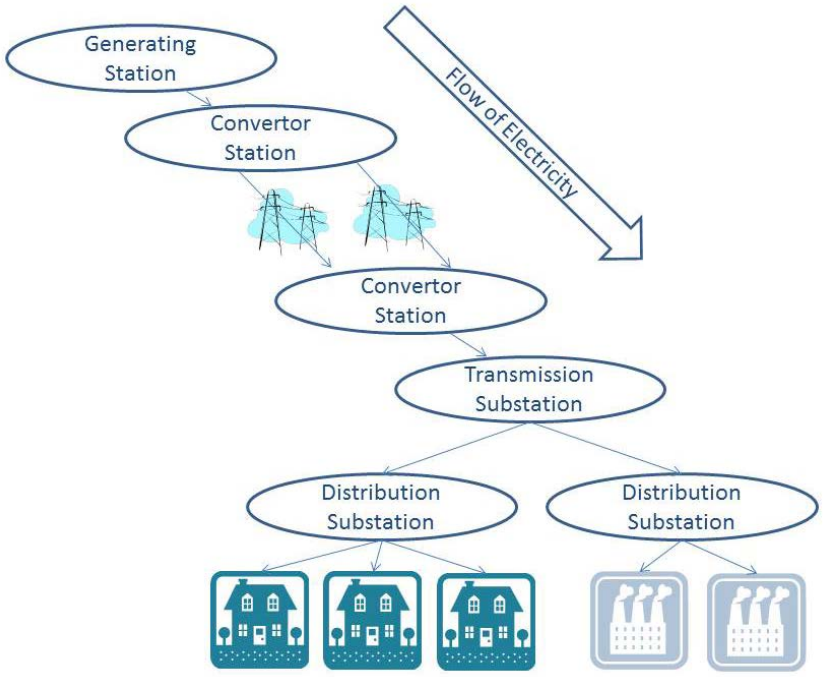
Manitoba Hydro provides electricity to more than 548,000 Manitoba customers. Approximately 96 percent of the electricity is generated at 15 hydroelectric generating stations located primarily in the northern and south-eastern region of the province. The remaining electricity comes from 2 thermal generating stations, 4 diesel generating stations and 2 wind farms (**Figure 1**).

Figure 1: Major electrical and gas facilities



In order to transmit most of the electricity from the northern generating stations to southern Manitoba it needs to be converted to high voltage direct current (HVDC). Upon reaching its destination, it is converted back to its original state for distribution to consumers. There are 3 HVDC convertor stations, and about 12,800 km of transmission lines, 78,000 km of distribution lines and more than 400 substations. **Figure 2** illustrates the infrastructure involved in the generation, transmission and distribution of electricity.

Figure 2: Electric utility infrastructure



Manitoba Hydro delivers natural gas to approximately 269,000 Manitoba consumers through a network of 9,000 km of pipeline and regulating stations that it operates and maintains. The majority of the natural gas consumed in Manitoba is sourced from Alberta and is transported to Manitoba on the TransCanada Pipelines.

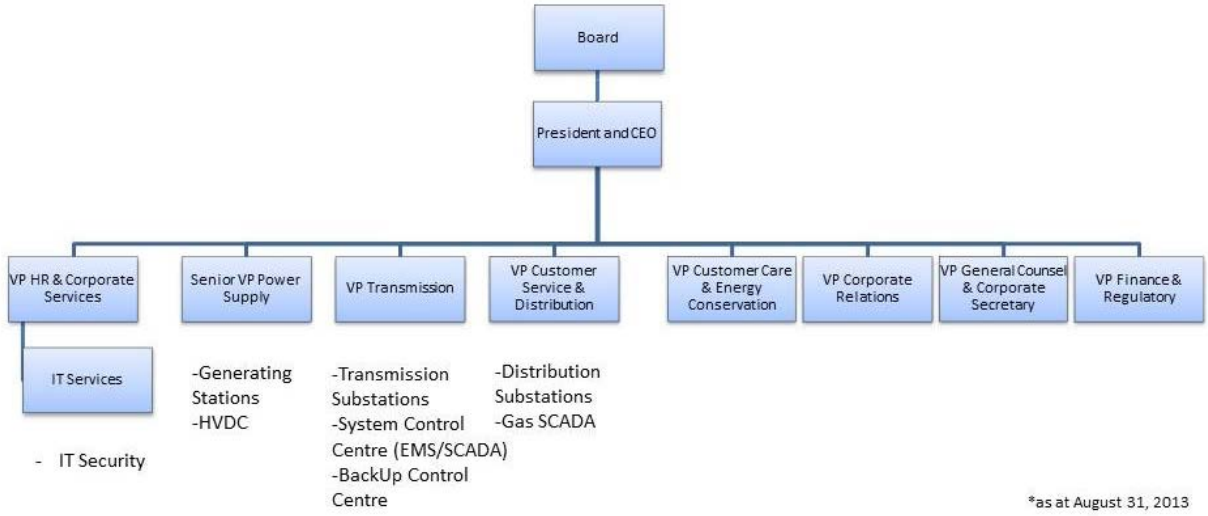
Figure 3 shows how Manitoba Hydro was organized as at August 31, 2013.

The Power Supply business unit plans, designs, builds and operates hydraulic and thermal generating stations.

Transmission designs, constructs and maintains transmission facilities. Transmission is also responsible for monitoring, controlling and regulating the flow of electricity into, out of, and throughout the province via the System Control Centre (SCC).

Customer Service and Distribution takes delivery of electricity from the transmission system, and natural gas from the Trans Canada Pipeline, and distributes that energy to Manitobans.

Figure 3: Manitoba Hydro organization chart



What are Industrial Control Systems?

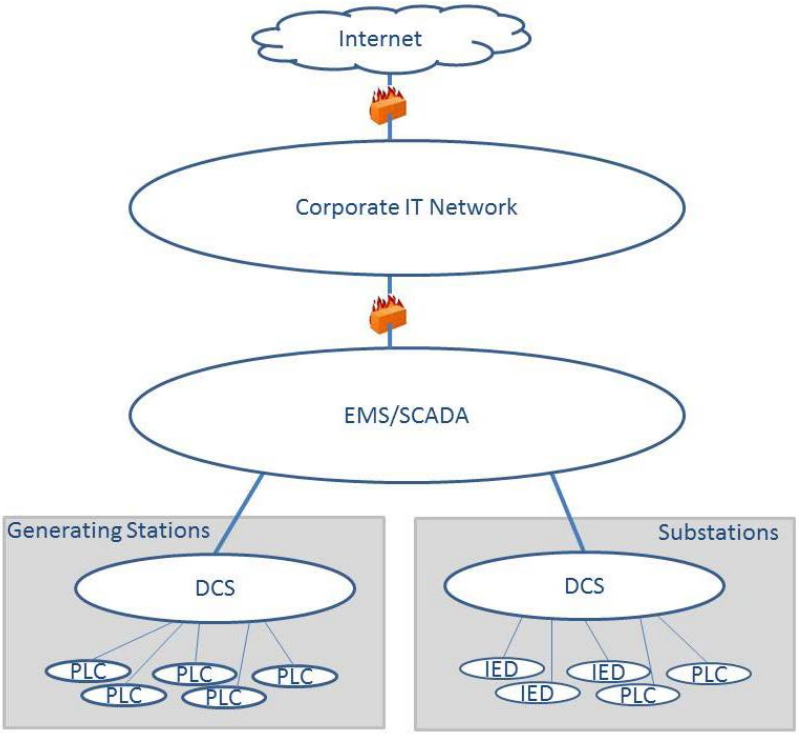
Industrial Control Systems (ICS) are used extensively in many industries including utilities, natural gas, water treatment plants, and manufacturing plants. Modern ICS systems use computers and software to collect and analyze data from sensors and then send instructions to physical devices such as valves and pumps.

ICS is a general term used to describe several types of control systems (Source: NIST 800-82):

- Supervisory Control and Data Acquisition (SCADA) systems enable the centralized control and data collection for monitoring and controlling remote assets (including Distributed Control Systems and Programmable Logic Controllers) over long distances.
- Distributed Control Systems (DCS) are generally used to control and regulate local industrial processes (e.g. electric power generation).
- Programmable Logic Controllers (PLC) are typically small industrial computers that have been designed to perform logic functions. They are used for discrete control of specific applications.
- Intelligent Electronic Devices (IED) are sensor/actuators that contain intelligence required to perform local processing and control.

Numerous industrial control systems are necessary to monitor and control all of the complex processes involved in the generation, transmission and distribution of electricity. (**Figure 4**)

Figure 4: Conceptual Industrial Control Systems configuration



How does Manitoba Hydro use Industrial Control Systems?

To generate and transmit electricity within Manitoba, Manitoba Hydro uses many Industrial Control Systems. PLCs are used within the majority of generating stations to monitor and control specific processes (i.e. one turbine). Distributed Control Systems, at these sites, manage power generation processes (all PLCs). The Energy Management System (EMS) and SCADA work together to monitor, coordinate and control the generation and transmission of electricity.

What are ICS cyber security risks?

Cyber security risk is defined as the potential for adverse events impacting organizational operations (including mission, functions, image and reputation), resources and other organizations due to unauthorized access, use, disclosure, disruption, modification, or destruction of information, information technology (IT) and/or operations technology (OT). (Source: *Electricity Subsector Cybersecurity Risk Management Process*, U.S. Department of Energy, May 2012)

The National Institute of Standards and Technology (NIST) *Guide to Industrial Control System (ICS) Security (800-82)* lists potential adverse events an ICS may face including:

- Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation.
- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life.

- Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects.
- ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects.
- Interference with the operation of safety systems, which could endanger human life.

Risks can occur when there are threats and existing vulnerabilities. Threats to control systems can come from both deliberate and accidental sources (**Figure 5**). These threats are often downplayed. Organizations need to assume that an adversary has the skills and intent to attack these systems. The probability of a successful attack will therefore depend on the level of protection provided to the system.

Figure 5: Threats to Industrial Control Systems

Deliberate	Accidental
Hostile governments	Natural disasters
Terrorist groups	Human error
Hackers	Equipment failure
Hacktivists	
Criminal groups	
Disgruntled insider	

Industrial control systems were initially not connected to corporate networks and relied heavily upon their own unique communication protocols. To improve information sharing, ICS systems have been modernized and are increasingly connected to the business corporate networks and external agencies. While this has certainly increased organizational efficiency, ICS systems have inherited many of the more widespread and traditional cyber security vulnerabilities of IT networks (i.e. viruses, denial of service attacks).

Recently many vulnerabilities have been discovered in ICS equipment. In 2010, the malicious code Stuxnet specifically targeted industrial control systems. Stuxnet would alter the control network to change key parameters and thereby physically damage critical ICS equipment. The code was designed to only attack very specific control systems in limited locations. However, now that it has been reverse engineered, security experts warn that it can be used as blueprint for an attack that could cause catastrophic damage.

> Cyber security starts by developing an understanding of the risks an organization faces, and those it may expose its clients and other stakeholders to. Given some of the applications of ICS, these risks can extend beyond financial and business risks and include loss of life and injury. It is therefore imperative that organizations consider their exposure to cyber threats, assess the resulting risks, and implement safeguards accordingly.
>
> *Risk Management Guide for Critical Infrastructure Sectors*, Public Safety Canada July 2010

Given the constantly changing nature of cyber vulnerabilities and threats, an "all-hazards" approach must be taken to risk identification and management, including careful consideration of high-impact but low frequency events (i.e. coordinated cyber-attacks).

In May, 2012 NERC Cyber Attack Task Force stated (see **Appendix A** for a description of NERC):

> A highly coordinated and structured cyber, physical, or blended attack on the bulk power system, could result in long-term, difficult to repair damage to key system components in multiple simultaneous or near-simultaneous strikes. Unlike "traditional," probabilistic threats (i.e. severe weather, human error, and equipment failure), a coordinated attack would involve an intelligent adversary with the capability to quickly bring the system outside the protection provided by current planning and operating practices. An outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods.

How are corporate risks managed at Manitoba Hydro?

In 2004, Manitoba Hydro issued its *Risk Management Policy*. The policy outlined the requirements for risk identification, impact analysis, risk treatment, and residual risk assessment. It requires that systems be implemented to monitor key risks, and that information provided by these systems be used to facilitate management actions. Further it requires that stakeholders be appropriately informed and that risks be managed within the Corporation's approved risk tolerances.

In 2012 Manitoba Hydro identified 52 risk profiles organized in 11 risk categories (Market, Financial, Environmental, Infrastructure, Human, Business Operational, Reputation, Governance-Regulatory-Legal, Aboriginal, Emerging Technologies, and Strategic). Each risk profile was assigned to a responsible business unit.

These risks are analyzed for potential impact (Financial, System Reliability, Safety, Environment, and Customer Value) and likelihood. Corporate risk tolerances for each risk are determined and used to guide the extent of mitigating actions considered necessary. Individual risk profile managers are responsible for ensuring that risk treatments are effectively implemented.

Manitoba Hydro's corporate risk management department is responsible for producing its annual *Risk Management Report*. The report provides stakeholders with information on the status of identified major risks facing the Corporation. The report describes each identified risk, and the activities used to mitigate the risks, and provides estimates of the likelihood and impact of any residual risks.

As part of the annual risk report preparation, the Corporate Risk Management department requests that responsible business units update their risk documentation for changes to identified risks, emerging issues, and mitigation efforts.

Why is it important that ICS cyber security risks be understood and managed?

A survey of more than 500 of the world's most senior business leaders ranks cyber security as the 3rd highest corporate risk that organizations face today. *(Lloyd's Risk Index, 2013)*

Over the past decade a host of organizations including the Canadian government, NERC, ICS-CERT, and the Midwest Reliability Organization (MRO) have highlighted the increased cyber security risks to ICS. In the 2006 *Government Operations Centre: Cyber Environment Risk Assessment*, the Canadian government stated that the cyber risk for electrical energy utilities is rated as high impact and medium probability with an **overall rating as high**. It also noted increasing incidents of cyber-related vulnerabilities which supported the overall risk rating of **high**.

> The cyber threat to critical infrastructure continues to grow and represent one of the most serious national security challenges we must confront.
>
> *US Presidential Executive Order* 2-14-35, Feb 12, 2013

Audit approach

Our objective was to determine whether Manitoba Hydro's risk management practices ensure the design of security controls over Industrial Control Systems (ICS) and related Information Technology (IT) reasonably mitigate identified cyber risks.

Our audit criteria are based on the standards included in the IT *Risk Management Audit/Assurance Program* developed by the Information Systems Audit and Control Association (ISACA). The criteria were discussed with management prior to commencing our fieldwork.

To understand security controls in place, we conducted 6 site visits. We compared cyber security practices in place at each location to Public Safety Canada's best practices for industrial control systems.

The audit examined practices in place up to August 31st, 2013. Our examination was substantially conducted between July and November 2013.

We did not assess the overall management of Manitoba Hydro's risk management program or the NERC reliability compliance program.

Our examination was performed in accordance with the value-for-money auditing standards recommended by the Canadian Institute of Chartered Accountants, and accordingly, included such tests and other procedures as we considered necessary.

Findings and recommendations

We concluded that cyber security risks related to ICS systems are not identified, assessed and managed. Until Manitoba Hydro has assessed the risks to all ICS systems it cannot be certain that it has applied the appropriate level of controls to prevent unauthorized access, modification or damage to these vitally important systems.

1. Manitoba Hydro not aware of all significant ICS cyber security risks

Effective ICS risk management begins by identifying and prioritizing all ICS systems necessary to support operations and business processes. An inventory of all associated hardware and software would then be created and maintained. All potential risks to ICS systems would be evaluated for likelihood and impact, and based on these risk assessments, appropriate cyber security controls would be applied. Any residual risks should be accepted by management, and a risk registry should be updated regularly.

1.1 ICS systems critical to operations not identified

Manitoba Hydro has not identified and prioritized all ICS and related IT systems that are used to support its generating, transmitting and distributing processes. Nor has it created a related inventory of all ICS hardware and software. An accurate inventory of all ICS systems is a necessary component of IT management and is necessary to understanding exposures to vulnerabilities and various threats.

1.2 Cyber security risks to critical ICS assets have not been identified

Manitoba Hydro's risk management process includes 52 risk profiles. These are summarized in an annual risk management report. ICS cyber security, or more broadly cyber security, is not one of the risk profiles. We identified 7 of Manitoba Hydro's risk profiles that could include industrial control systems risks.

For each of these profiles, we examined the supporting documentation (what officials referred to as the "Longform"). These documents do not identify or discuss ICS cyber security risks. We also examined risk management reports prepared by Transmission Systems Operations (2010) and Customer Service & Distribution (2013). These reports focused primarily on the risks of component failures due to, for example, wear and tear, equipment flaws, and physical vandalism. These documents also do not identify and discuss any ICS cyber security risks. Risk reports were not produced by divisions within Power Supply and IT Services.

In examining the divisional risk reports, we noted that there was no clear mapping between these reports and the corporate "Longforms". For example, the corporate "Longform" for **Infrastructure - Prolonged loss of system supply** includes a risk treatment of "implementing cyber security upgrades". After reviewing the Cyber Security Upgrade project documentation, we noted that these upgrades were primarily focussed on NERC critical cyber assets (see **section 1.4**). We could not find mention of cyber security risks or their corresponding risk treatments in any divisional risk reports.

Without comprehensive and coordinated cyber security risk assessments, Manitoba Hydro may not be able to design and implement effective security controls for its ICS systems.

Implementing an effective cyber security risk management process for ICS systems presents unique challenges. There are a variety of existing cyber security standards and tools available to assist organizations that use and maintain ICS systems (i.e. ISA/IEC 62443, NIST 800-82). In May 2012, the US Department of Energy, in conjunction with NERC, NIST and the Canadian federal government (Natural Resources Canada), created a Risk Management Process (RMP) to assist utilities in understanding and managing cyber security risks with respect to ICS systems. This document outlines a risk management model that can be tailored to any size utility. It is designed to integrate with existing corporate risk management efforts. We encourage Manitoba Hydro to take advantage of the guidance outlined in these standards and the RMP document.

Conducting ICS cyber security risk assessments requires an expertise in both cyber security and control systems engineering. Given the lack of focus on cyber security risk assessments to date, Manitoba Hydro will need to ensure that sufficient qualified staff are available to effectively conduct ICS risk assessments.

> **Recommendation 1:** We recommend that Manitoba Hydro identify, assess and mitigate all ICS cyber security risks and that this be performed on a priority basis for assets critical to operations.

1.3 ICS cyber security risks not communicated to the Board

Manitoba Hydro's annual *Corporate Risk Management Reports* from 2004 to 2012 discuss the risk profiles and include an overall summary. The reports are provided to the Board annually for their review and information. Because ICS cyber security risks are not identified (**section 1.2**), the reports do not discuss ICS cyber security risks. As a result, ICS cyber security risks have not been communicated to the Board or other stakeholders.

Although subsequent to our audit period, we note that the 2013 *Risk Management Report* that was submitted to the Board in November 2013, identified Cyber Security as one of the "Significant and Emerging Risks". The report states, "Countermeasures and management controls and processes are in place to mitigate this risk…" However, as discussed in **section 1.2**, cyber security risks to critical ICS assets have not been identified. In our view, the report should have discussed this significant limitation. If left uncorrected, the corporate risk management report may provide the Board with unwarranted assurance on the adequacy of security measures over ICS assets.

Recommendation 2: Once ICS cyber security risks have been assessed, we recommend that Manitoba Hydro include cyber security as a corporate risk profile in the annual risk management report that is presented to the Board.

1.4 NERC CIP standards apply only to assets critical to the bulk electric system and not all assets critical to Manitoba Hydro operations.

Manitoba Hydro must comply with the NERC CIP standards (see **Appendix A**), which include cyber security controls. NERC standards are focused on the management of assets critical to the flow of electricity through the North American electric grid.

NERC has developed criteria for the identification of critical assets (critical assets can include locations such as generating stations, transmission substations, control centres and key equipment such as transformers and transmission lines). For example, NERC standards generally apply to facilities 100kV and above. Using these criteria, Manitoba Hydro has identified 18 critical assets (8 physical locations) (**Figure 6**). These assets represent a relatively small percentage of Manitoba Hydro's total bulk electric system assets (455). For each critical asset, NERC requires that critical cyber assets be identified, again using a set of NERC criteria. Manitoba Hydro has determined that only 2 of the 18 critical assets (2 specific locations) house critical cyber assets. As a result, these 2 locations must be protected using NERC CIP requirements. Because of the blanket application of the CIP requirements, NERC does not require a cyber risk assessment.

Figure 6: Determining NERC critical cyber assets

NERC requirements	At Manitoba Hydro
Identify all assets relevant to the bulk electric system	**455 assets**
⇩	
Using NERC Critical Asset Criteria, identify the NERC critical assets	**18 assets**
⇩	
Using the NERC Critical Cyber Asset Criteria, identify NERC critical cyber assets	
⇩	**2 assets**
Apply NERC CIP controls to the NERC critical cyber assets	

All remaining Manitoba Hydro assets (including all generation stations, transmission substations, control structures, HVDC stations, and distribution assets) do not need to comply with NERC CIP requirements. It is important to note that assets assessed as critical for NERC purposes do not necessarily represent the only assets that are critical to Manitoba Hydro operations.

> Our shared responsibility to cyber security goes beyond compliance. Being compliant with security regulations does not equal good security; rather, compliance is a component (the result) of a good security program.
> Midwest Reliability Organization President Nov/Dec 2011

An ICS cyber security risk management program, that identifies risks to all ICS systems, would assist Manitoba Hydro in accomplishing its NERC compliance goals. NERC standards and related compliance efforts by Manitoba Hydro should not be interpreted as adequate corporate cyber security risk management.

2. Many gaps in ICS security controls at sites we visited

To assess whether the lack of ICS cyber security risk assessments had a significant impact on the decisions made by Manitoba Hydro when securing cyber assets critical to its operations, we visited 4 generating stations, a modernized transmission substation, and a HVDC converter station. These locations make use of ICS systems and we believe are critical to Manitoba Hydro operations. It is important to note that the sites selected were identified as not having NERC critical cyber assets. We compared cyber security practices in place at each location to Public Safety Canada's recommended best practices for industrial control systems (TR12-002) as they represent the **minimum** standards that should be implemented by all industries that use ICS.

At each of the sites we visited, some ICS security controls were evident (for example perimeter physical security, password controls, and computer room environmental controls) but we identified serious weaknesses in the following areas:

- Network segmentation.
- Patch management.
- Access controls.
- System hardening.
- Intrusion detection.
- Physical security.
- Malware protection and detection.
- Change controls and configuration management.
- Incident planning and response.

In addition to the minimum cyber security controls, comprehensive ICS risk assessments could identify additional ICS security measures to properly mitigate the risks. As with all ICS security controls, careful evaluation and testing in the applicable network environment is necessary prior to implementation.

Full implementation of Recommendation 1 should resolve these security gaps.

3. Several factors led to lack of attention to ICS cyber security risks

Manitoba Hydro's regulatory compliance focus when dealing with ICS cyber security risks is not unique. A 2011 Government Accountability Office (GAO) audit of the NERC reliability standards in the United States noted the following:

> **Utilities focusing on regulatory compliance instead of comprehensive security.**
> The existing federal and state regulatory environment creates a culture within the utility industry of focusing on compliance with cybersecurity requirements, instead of a culture focused on achieving comprehensive and effective cybersecurity... (NERC CIP) security requirements are inherently incomplete, and having a culture that views the security problem as being solved once those requirements are met will leave an organization vulnerable to cyber-attack. Consequently, without a comprehensive approach to security, utilities leave themselves open to unnecessary risk. (Source: *Electricity Grid Modernization*, GAO, January 2011)

3.1 "Air-gap" and non-routable serial cables provide false sense of security

Prior to 2009, 12 generating and HVDC stations had industrial control systems (DCS) that connected to Manitoba Hydro's corporate IT network. In addition, these stations were connected to the System Control Centre (SCC) using non-routable serial cables. In 2009, the majority of these stations were disconnected from the corporate IT network. This "air-gap" network segmentation was implemented to reduce NERC compliance requirements rather than as part of a comprehensive security architecture. Consequently, controls needed to enhance the effectiveness of the "air-gap" were not implemented.

Non-routable serial cables do not transmit internet communication (Internet Protocol (IP)).

Systems that are physically isolated from other networks are still vulnerable to security breaches. For example, well-intentioned operations and engineering staff could connect an infected laptop or USB storage device to a generating station's control network (DCS). There are operational reasons why Manitoba Hydro staff connect devices and share information between the corporate and ICS networks. Such connections would allow malicious software to attack the "air-gapped" system, potentially impacting both operations and safety of site personnel.

While an "air-gap" reduces the risk of malware spreading from a generation station to the SCC and vice versa, it has fostered a false sense of security within Manitoba Hydro. This configuration is used at all of the facilities we visited. In today's cyber threat environment, an "air-gap" between two networks should not be seen as an all-encompassing security control. Additional layers of controls are essential to reducing overall cyber risks.

The Computer Emergency Readiness Team (ICS-CERT), a division of the U.S. Department of Homeland Security, announced in their 2012 *Year In Review* that the control networks of two generation facilities had been attacked by connecting infected USB devices. As well, USB storage devices were a primary attack vector of the Stuxnet malware.

Use of non-routable serial cables between ICS assets is often thought of as a "secure" solution that does not require additional protection. This misconception is strengthened by the current NERC CIP requirements that exclude serial protocols as a potential threat vector. However, any communication medium (cables, protocols) can be used for a cyber-attack. Security researchers have recently discovered critical security vulnerabilities that take advantage of serial connectivity. The risk of attack using serial protocol should not be overlooked.

Implementation of Recommendation 1 should resolve these concerns.

> While the implementation of an antivirus solution presents some challenges in a control system environment, it could have been effective in identifying both the common and the sophisticated malware discovered on the USB drive and the engineering workstations."
>
> *2012 Year in Review,* ICS-CERT

3.2 Responsibility for corporate-wide ICS cyber security not assigned to one executive

On August 14, 2003, eastern Canada and the US experienced a cascading electric power blackout. The outage affected an estimated 50 million people. The following day, the Prime Minister and the US President directed that a joint task force be established to investigate the causes of the blackout and recommend ways to reduce the possibility of future outages. The Task Force published a report on November 19, 2003.

While the Task Force concluded that a malicious cyber attack was not the direct or indirect cause of the power outage, it did identify a number of areas of concern with respect to cyber security within the electricity sector. One of the recommendations was that organizations establish clear authority and ownership for cyber security. They further noted that the owner should have the ability to influence corporate decision-making and be able to make cyber security related decisions for both IT and OT systems throughout the enterprise.

At Manitoba Hydro, there is no corporate-wide oversight on the quality and adequacy of cyber security measures in place. Each business unit and department is responsible for managing their ICS systems and risks, potentially understating corporate-wide risks. These business units include:

- Transmission.
- Power Supply.
- Customer Service and Distribution.

Fragmented control can result in inconsistent practices/controls.

Recommendation 3: We recommend that Manitoba Hydro assign responsibility for corporate-wide cyber security to one executive.

3.3 Comprehensive ICS cyber security policies not in place

An organization's IT policy instruments are essential components of its information security program because many IT policy instruments are developed in response to an identified risk. IT policy instruments include policies, standards, guidelines, directives, and procedures.

Manitoba Hydro has established cyber security policies for all NERC critical cyber assets. These policies include:

- Roles and responsibilities.
- Personnel security.
- Electronic security.
- Physical security.
- Information protection and disposal.

These policies currently only apply to the systems located at 2 physical locations (NERC critical assets, see **section 1.1**).

In addition Manitoba Hydro has an Information Technology security policy. This policy defines roles and responsibilities and governing principles for corporate IT Security. It also includes guidelines and the following security procedures:

- System and software security.
- Communication security.
- Data security.
- Physical security.
- Change control.
- Security Administration.

Because of potential operational and safety concerns, the corporate IT policies do not apply to ICS systems. No other policies are in place to guide operating divisions in managing and securing their ICS systems.

Corporate cyber security policies should also guide the design and procurement of all control systems (software, systems, and networks) and should be included in the procurement requirements. For example, Manitoba Hydro's Smart Grid initiatives, including Distribution Automation and Advanced Metering Infrastructure (AMI), should include risk-reducing privacy and cyber security requirements throughout the project lifecycle. Without clear corporate-wide ICS cyber security policies, procedures and standards, Manitoba Hydro cannot ensure new ICS systems are securely designed, procured and implemented.

When developing ICS policy instruments, in addition to the results of risk assessments, several cyber security maturity models (i.e. ES-C2M2, ICS-CERT CSET) are available to help in identifying strengths and weaknesses compared to industry standards/best practices.

Recommendation 4: We recommend that Manitoba Hydro develop and implement ICS cyber security policy instruments and make them applicable to all ICS systems.

3.4 Responsibility for physical security is fragmented

Physical access to computers, network equipment, and network cables should be restricted to only those persons who have a requirement to use and maintain those devices. Unauthorized access to essential ICS systems could result in damage to operational systems and processes.

Manitoba Hydro has a Corporate Security Department. In 2012, Corporate Security updated its physical security policy. This policy requires the categorization of site facilities into 1 of 5 Asset Protection categories. For each category the policy includes physical security standards. However, these standards are limited to the exterior of each facility. Given the criticality of ICS systems, we would expect to find physical security policy instruments that outline specific requirements to protect those key systems from unauthorized access. Such policies are not in place.

A NERC security policy is in place that details the physical security requirements for NERC assets and associated critical cyber assets. As previously noted, the majority of Manitoba Hydro facilities, that house ICS systems, fall outside of this policy.

The Corporate Security Department told us that they provide consultative assistance to business units on physical security matters as requested and investigate any physical security breaches that may occur. But that they do not have overall responsibility for physical security of all Manitoba Hydro assets and buildings.

Current ownership of physical security functions at Manitoba Hydro resides with each business unit and department. Site/facility managers are responsible for ensuring their own security. When conducting our site visits we noted that each site had some physical security controls restricting public access but controls were inconsistently applied increasing the risk of unauthorized access to ICS systems. The rationale for the varying physical security measures at each site could not be provided.

In February 2013, a Physical Security Working Group, comprised of key internal corporate stakeholders, was formed with the goal of creating a corporate standard for physical security technology (one aspect of physical security). While some progress has been made, the corporate standard has not been completed.

Recommendation 5: We recommend that Manitoba Hydro assign responsibility for corporate-wide physical security to one executive.

Recommendation 6: We recommend that Manitoba Hydro develop and implement physical security policy instruments to control physical access to ICS systems.

3.5 Lack of ICS security awareness program and training

Engineering staff and operators are normally not cyber security specialists and are understandably more concerned about reliability and safety than cyber security and malicious attacks.

An ICS security awareness and training program has not been developed. Many of the operational and engineering staff, at the sites we visited, had previously attended in-house cyber security training for NERC assets. However, as these sites are no longer classified as NERC CIP critical (see **section 3.1**), the staff at these sites are no longer required to complete the training.

We examined the NERC cyber security awareness training provided by Manitoba Hydro. The training does not sufficiently cover ICS threats and vulnerabilities. In addition, corporate security awareness communications do not deal with ICS cyber security risks.

> **Recommendation 7:** We recommend that Manitoba Hydro develop and deliver a comprehensive ICS cyber security training and awareness program for all staff responsible for the operation, maintenance and security of ICS systems.

3.6 Management only recently exploring benefits of IT/OT convergence, IT Security not yet involved

Information Technology (IT) services departments typically focus on delivering enterprise information systems to support business objectives (e.g. SAP, e-mail, web services). Operational Technology (OT) is a term used to describe technical systems that monitor and control physical operating equipment (e.g. field devices). They are systems dedicated to the actual physical equipment used to perform real-time operations. These differences have led to organizations developing separate and distinct organizational structures for IT and OT departments.

Over time, operational technology systems have been updated and replaced so that the underlying networking, hardware, and software have become more like traditional IT systems (e.g. Windows workstations and servers, databases, IP networking). This has led to common technical requirements between the IT and OT functions.

At Manitoba Hydro, each business unit is responsible for the management and operation of their own OT systems. Corporate IT Services told us they are not responsible for managing, maintaining and securing any of these systems.

Leveraging the systems, resources and personnel between IT and OT makes good business sense. Since 2011, officials at Manitoba Hydro have been discussing the potential benefits of centrally managing these systems. Given the increased risk that OT systems now face as they are modernized, cyber security needs to be an important topic in any IT/OT convergence discussions. As at the end of our fieldwork, convergence discussions had not dealt with security matters.

> **Recommendation 8:** We recommend that Manitoba Hydro develop a strategy to converge IT and OT management, including IT security.

Summary of recommendations

We recommend that Manitoba Hydro:

1. identify, assess and mitigate all ICS cyber security risks and that this be performed on a priority basis for assets critical to operations.
2. once ICS cyber security risks have been identified, include cyber security as a corporate risk profile in the annual risk management report that is presented to the board.
3. assign responsibility for corporate-wide cyber security to one executive.
4. develop and implement ICS cyber security policy instruments and make them applicable to all ICS systems.
5. assign responsibility for corporate-wide physical security to one executive.
6. develop and implement physical security policy instruments to control physical access to ICS systems.
7. develop and deliver a comprehensive ICS cyber security training and awareness program for all staff responsible for the operation, maintenance and security of ICS systems.
8. develop a strategy to converge IT and OT management, including IT security.

Response of officials

General comments

We have considered the recommendations and are pleased to provide you with Manitoba Hydro's response. For the most part, Manitoba Hydro embraces the recommendations flowing from the audit and recognizes the importance of ensuring proper protocols are implemented to protect and mitigate the risk of both cyber and physical security attacks on Manitoba Hydro's key industrial control systems.

Below you will find Manitoba Hydro's response to each of the recommendations.

Response to recommendations

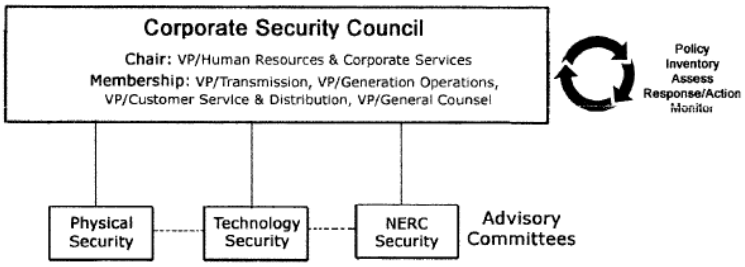
Recommendations 3 and 5:

3. Assign responsibility for corporate wide cyber security to one executive.
5. Assign responsibility for corporate wide physical security to one executive.

Manitoba Hydro's Response:

Effective April 1, 2014, the Vice-President Human Resources and Corporate Services will be assigned responsibility for both corporate-wide cyber and physical security. Organizational restructuring is underway to effect the change to a single accountability model for corporate-wide cyber and physical security.

Given both cyber and physical security spans several business units across the organization, a Corporate Security Council , comprising of Vice-Presidents and Chaired by the Vice-President, Human Resources and Corporate Services, has been constituted as illustrated below.



Terms of reference are presently under development. However, the Corporate Security Council will be the vehicle for providing executive oversight relating to all corporate security functions, developing and executing strategy, setting priorities relating to the implementation of the Auditor General's recommendations and governance relating to changes in security policy. The Corporate Security Council will also provide oversight and direction to the three advisory committees.

Recommendations 1, 4, 6 and 7:

1. Identify, assess and mitigate all ICS cyber security risks and that this be performed on a priority basis for assets critical to operations.
4. Develop and implement ICS cyber security policy instruments and make them applicable to all ICS systems.
6. Develop and implement physical security policy instruments to control physical access to ICS systems.
7. Develop and deliver a comprehensive ICS cyber security training and awareness program for all staff responsible for the operation, maintenance and security of ICS systems.

Manitoba Hydro's Response:

Manitoba Hydro endorses and supports audit recommendations 1, 4, 6 and 7. The Corporate Security Council is seized with developing and executing a strategy to satisfy each of these recommendations.

Recommendation 2:

2. Once cyber security risks have been identified, Include cyber security as a corporate risk profile in the annual risk management report that is presented to the board.

Manitoba Hydro's Response:

As noted in the Audit Report, cyber security has been identified by Manitoba Hydro as a 'Significant and Emerging Risk' in the annual Corporate Risk Management Report that was submitted to the Board in November 2013. We anticipate that in future reports, cyber security will be incorporated as a corporate risk profile, to be assessed and managed under the auspices of the Corporate Security Council.

Recommendation 8:

8. Develop a strategy to converge IT and OT management, including IT security.

Manitoba Hydro's Response:

Manitoba Hydro has been exploring the benefits and efficiencies of leveraging existing IT expertise and management practices to our OT systems and networks, including IT security. As noted in the Audit Report, a working group has been struck to review current practices and recommend opportunities for improvement where appropriate. Enhanced guidance and oversight through the corporate security governance framework will ensure that actionable items are identified and executed in a timely manner.

Appendix A – North American Electric Reliability Corporation (NERC)

The North American Electric Reliability Corporation (NERC) is an international regulatory authority established to reduce the risks to the reliability of the bulk electric system in North America. NERC develops and enforces reliability standards; annually assesses seasonal and long-term reliability; monitors the system; and educates, trains and certifies industry personnel.

NERC develops and enforces 100 reliability standards in 14 categories. Manitoba Hydro must comply with all but the nuclear standards.

Reliability standards categories
Resource and Demand Balancing
Communications
Critical Infrastructure Protection (CIP)
Emergency Preparedness and Operations
Facilities Design, Connections and Maintenance
Interchange Schedule and Coordination
Interconnection Reliability Operations and Coordination
Modeling, Data, and Analysis
Nuclear
Personnel Performance, Training and Qualifications
Protection and Control
Transmission Operations
Transmission Planning
Voltage and Reactive

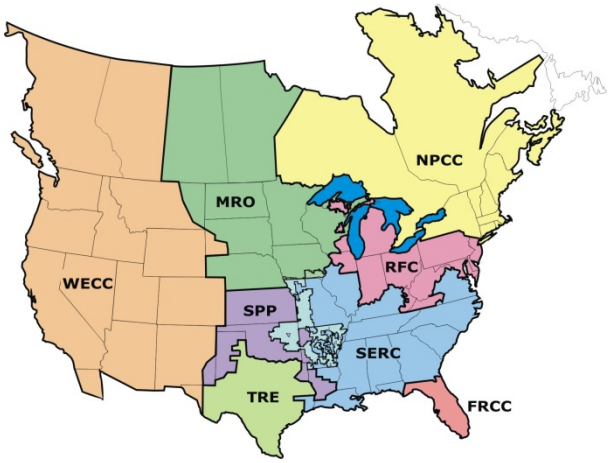
Why does Manitoba Hydro need to comply with NERC?

Manitoba Hydro voluntarily began working towards complying with NERC standards in 2003.

In 2004, a Manitoba Order in Council authorized Manitoba Hydro to join the Midwest Reliability Organization (MRO) and formally adopt NERC's Reliability Standards. The MRO is one of eight regional entities responsible for:

- assessing compliance with reliability standards.
- providing seasonal and long-term assessments of the bulk power system.
- conducting technical analyses of matters impacting bulk power system reliability.

An interim agreement between NERC, MRO, and Manitoba Hydro operated until 2012. It set out comprehensive arrangements for monitoring and enforcing compliance to NERC standards.



On June 11, 2009 the *Manitoba Hydro Amendment and Public Utilities Board Amendment Act* received royal assent. The Act and implementing regulations came into force on April 1, 2012 and set the basis for the adoption of mandatory and enforceable NERC reliability standards in Manitoba. The legislation gives the Public Utilities Board authority to make determinations of non-compliance with NERC reliability standards and to impose sanctions. Sanction recommendations resulting from a violation are based on the level of risk and severity associated with the violation. These sanctions can include significant monetary penalties (up to $1 million dollars per day). The MRO audited Manitoba Hydro in 2012 and is scheduled to perform compliance audits on a 3 year cycle. The MRO can perform "spot check" or "event driven" audits at their discretion.

How does Manitoba Hydro ensure compliance with NERC standards?

Complying with NERC standards is a sizable endeavour. A corporate NERC Reliability Compliance Program was established in 2006 to manage Manitoba Hydro's responsibilities for compliance to these standards. The purpose of the program is to assess the risks of non-compliance, inform management of its compliance obligations, develop expertise in industry compliance issues, and help line departments integrate the requirements of mandatory reliability standards into the day-to-day activities of the corporation. The program includes three key components:

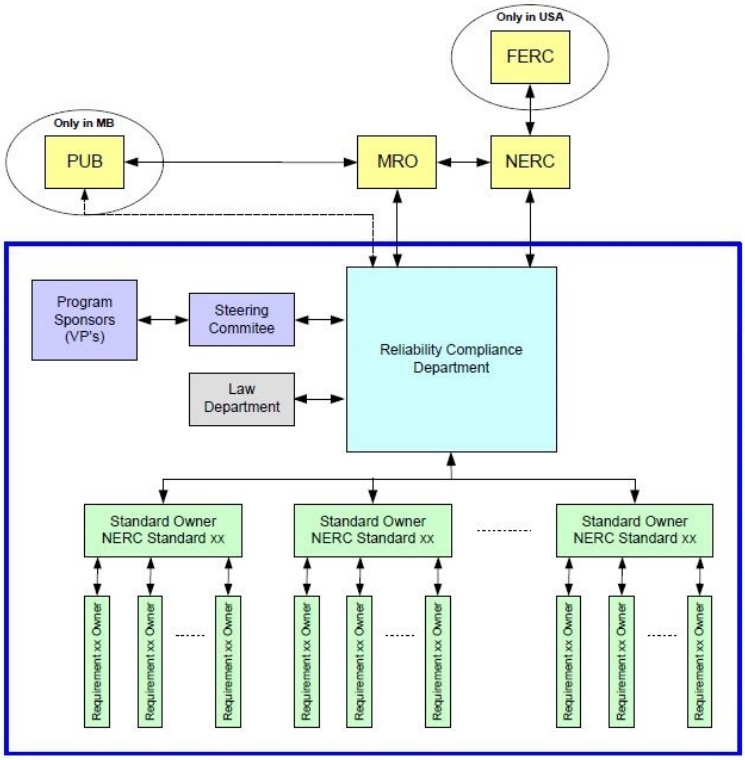
- Standards development.
- On-going compliance.
- Monitoring and enforcement.

Responsibility for each standard has been assigned to subject matter experts who are responsible for developing compliance and mitigation plans. The program has defined roles and responsibilities for standard owners and stakeholders.

The Reliability Compliance department manages the risks (reliability, financial, and reputational risks) associated with non-compliance. A corporate policy, *"Mandatory Compliance with North American Electric Reliability Corporation (NERC) and Midwest Reliability Organization (MRO) Standards"*, was created. It delegates compliance responsibilities and outlines violations and sanctions.

A Reliability Compliance Steering Committee has been established to monitor and review the program status and provide valuable oversight of the program deliverables. The committee membership is comprised of division managers and other internal stakeholders. The committee reports a group of vice presidents (Transmission, Power Supply, Customer Care and Marketing, Finance and Administration).

Manitoba Hydro corporate NERC reliability compliance program



How do NERC standards deal with ICS cyber security?

The Critical Infrastructure Protection (CIP) standards are 1 of 14 categories of reliability standards. It is made up of 9 different standards to protect cyber assets. Each standard has a set of specific requirements that must be met.

Standard	Title
CIP-001	Sabotage Reporting
CIP-002	Critical Cyber Asset Identification
CIP-003	Security Management Controls
CIP-004	Personnel and training
CIP-005	Electronic Security Perimeter
CIP-006	Physical Security of Critical Cyber Assets
CIP-007	Systems Security Management
CIP-008	Incident Reporting and Response Planning
CIP-009	Recovery Plans for Critical Cyber Assets

Appendix B – Glossary of acronyms used in this report

CIP	Critical Infrastructure Protection
CSET	Cyber Security Evaluation Tool
DCS	Distributed Control System
EMS	Energy Management System
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
GAO	Government Accountability Office (US)
HVDC	High Voltage Direct Current
ICS	Industrial Control System(s)
ICS-CERT	Industrial Control System – Cyber Emergency Response Team
IED	Intelligent Electronic Device
IP	Internet Protocol
ISA/IEC	International Society for Automation / International Electrotechnical Commission
IT	Information Technology
MRO	Midwest Reliability Organization
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OT	Operations Technology
PLC	Programmable Logic Controller
RMP	Risk Management Process
SCADA	Supervisory Control and Data Acquisition
SCC	System Control Centre
USB	Universal Serial Bus