Q. Please provide the following documents:

a) *Enterprise Risk Management Framework and Procedures, Risk & Insurance*, July 19, 2017;

b) *Enterprise Risk Management Policy*, Version 3.1, February 21, 2018; and

c) *Nalcor Energy: Risk Rating Guide*.

A. Please refer to the following attachments:

- PUB-NLH-036, Attachment 1: "Enterprise Risk Management Framework and Procedures, Risk & Insurance," July 18, 2017;
- PUB-NLH-036, Attachment 2: "ERM-01: Enterprise Risk Management Policy," Version 3.1, February 21, 2018; and
- PUB-NLH-036, Attachment 3: "Nalcor Energy: Risk Rating Guide."

Enterprise Risk Management Framework and Procedures

Risk & Insurance
Latest Version – July 18, 2017

DOCUMENT REVISION HISTORY

Version	Date	Revisions
1.0	July 8, 2013	Initial release
1.1-1.7	January 2015-October 2015	Required annual review and update Delineation of Corporate and line of business level processes Consideration given to alignment with COSO where possible Review with internal stakeholders
1.9-1.11	June 2015	Updated versions - Nalcor Executive review and sign off
2.0	November 2015	Final updated version approved by CEO
3.0	May 2017	Updated to accommodate revised organizational structure
4.0	July 2017	Final updates applied by ERM representatives

RELATED DOCUMENTS

Document name	Version/Date	Location
Financial Risk Management Policy Statement	March 28, 2012	Obtain from Corporate Treasurer
Financial Risk Management Strategy	December 2013	Obtain from Corporate Treasurer
Enterprise Risk Management Policy	April 2017	Obtain from Chief Risk Officer

DISTRIBUTION LIST

Name	Job Title
Sturge, Derrick	CFO/Vice President Finance
Warren, Auburn	General Manager, Commercial, Treasury & Risk
Jones, Greg	General Manager, Energy Marketing
Meaney, James	VP Finance Power Supply
Hayes, Angelina	Chief Risk Officer
Drummond, Jonathan	Manager, Bull Arm Operations
Coady, Laurie	Manager, Corporate Services & Commercial Advisor
Marsh, Darren	Manager, Operational Insurance & Risk
Borden, Jackie	Manager, Internal Audit
Burry, Oral	Manager, Long Term Planning & Asset Management
Costello, Kris	Asset Manager, Oil & Gas
Pelley, Scott	Corporate Treasurer
Natalie Templeman	GM, IT and CIO
Catherine Squire	Manager, Planning, Risk & Controls
Suzanne Kenny	Manager, Financial Risk & ERM
Lisa Hutchens	VP, Finance and CFO, NL Hydro

Contents

Preface 4
Purpose of Manual 4
General Structure of Manual 4
Manual Objectives 5
Guiding Principles 5
Scope of Manual 6
Assumptions 6
Who should use this Manual 6

1 ERM Framework 7
1.1 Background Information 7
a) Framework - Mandate and Commitment 7
b) Framework – Design 8
c) Framework - Implementation 8
d) Framework - Monitoring and Review 9
e) Framework - Continual Improvement 9
1.2 Risk Management Process 9
a) Step 1 – Establishing the Context 12
b) Step 2 - Risk Identification 14
c) Step 3 - Risk Analysis 16
d) Step 4 - Risk Evaluation 17
e) Step 5 - Risk Treatment 18
f) Step 6 - Monitoring and Review 20

2 Roles and Responsibilities 22
2.1 Chief Risk Officer 22
2.2 ERM Representatives 22
2.3 Role of Risk Owners 23
2.4 Role of Executive Owners 23
2.5 Role of Internal Audit 24
2.6 Role of Strategic and Business Planning 24

3 Risk Committees 25

4 Use of Risk & Insurance Plans 26
4.1 Line of Business and Risk & Insurance Plan 26

5 ATIPPA/Energy Corporation Act & ERM 26
5.1 ATIPPA & ERM 26
5.2 Energy Corporation Act & ERM 26
5.3 Implications 27

6 Required Frequency 27

7 Glossary of Key Terms 28

Appendix 1 – Enterprise Risk Management RACI Charts

Preface

Today, business decisions are informed by risk. This document is a framework to support furthering the continuity and effectiveness of Enterprise Risk Management ("ERM") principles and processes.

Our ERM Framework and Procedures document ("the Framework", "Framework") is aligned with the goals of Safety, Environment, Business Excellence, People and Community to ensure risks are well managed and monitored throughout the organization and in line with the risk management expectations of our stakeholders. Risks are assessed against divisional, line of business or departmental plans which are anchored back to these objectives and rating guides are structured to consider impacts against these goals.

The Framework provides a common and pragmatic process for discussing risk management within the company, embedding risk philosophy within our culture, and for clearly communicating our risk management capabilities to external and internal stakeholders. It should be read in concert with the *ERM Policy Statement* as well as established Risk & Insurance Plans.

The Chief Risk Officer ("CRO") is responsible for updating this document and for ensuring the Framework continues to be aligned with applicable standards. After consultation and review by ERM Representatives, changes to this document will be approved by the EVP, Finance & CFO.

Purpose of Manual

Building on the Board approved *ERM Policy*; this document intends to provide practical guidance in how to use the tools and templates available. It also defines a common framework for building consistent and reliable data for risk reporting and common language is used to rate and discuss risk across the organization. Documenting critical business risks and their treatment strategies also encourages knowledge transfer and sharing.

General Structure of Manual

This Framework and Procedures document is organized into 7 sections. A brief description of each section follows:

Section 1 - ERM Framework: Contains general information about core elements of our ERM Framework, including the principles, infrastructure and processes which underpin its design.

Section 2 - Roles and Responsibilities: Provides a high level view of accountabilities within the framework, as well as more specific roles for key roles and departments.

Section 3 – Risk Committees: Details the objectives and structure of the risk committees.

Section 4 – Risk and Insurance Plans: Details the objectives and process for creating and maintaining Risk and Insurance plans.

Section 5 - ATIPPA/Energy Corporation Act: Provides guidance related to sharing and publication of potentially sensitive information/documentation.

Section 6 - Required Frequency: Outlines the minimum frequency with which each key process must be executed to remain in compliance with the overall ERM program requirements.

For access to this document and the Risk Toolset please see the below path or reach out to the Corporate Risk and Insurance team:

H:\Corporate Risk and Insurance\2. ENTERPRISE RISK MANAGEMENT\1. ERM\1. Policy&Framework

Manual Objectives

The Framework and Procedures were developed:

- To provide guidance to facilitate the consistent application of the ERM Framework, supporting processes, and toolset;

- To educate key stakeholders with respect to ERM and risk management as general concepts, and to provide clarity with respect to how we intend to manage risk as an organization. This includes internal and external stakeholders or interested parties;

- To provide clear delineation of roles and responsibilities with respect to risk management. This document clearly articulates specific accountabilities for key individuals; and

- To provide a forward looking view pertaining to elements of the framework that are planned but not yet implemented. As implementation progresses, these elements will be added to this document in more detail and in accordance with timelines established in Risk & Insurance plans.

Guiding Principles

The ERM Framework is underpinned by general principles stating that effective risk management:

- Creates and protects value;
- Is an integral part of all organizational processes;
- Is part of decision making;
- Explicitly addresses uncertainty;
- Is systematic, structured and timely;
- Is based on the best available information;
- Is tailored;
- Takes human and cultural factors into account;
- Is transparent and inclusive; and
- Facilitates continual improvement of the organization.

Scope of Manual

The established Framework focuses on applying a structured and consistent approach to risk assessment and risk treatment. Essentially, risk assessments focus on the risks to achieving business plans and represent an important part of the strategic planning process. This does not replace the need for management to implement more detailed process level risk assessments and risk management practices as part of embedding appropriate internal controls and management systems within their operations.

This Framework applies to Nalcor and all of its subsidiaries. Accordingly, unless otherwise noted, all references to Nalcor within the remainder of this document are meant to include all of its subsidiaries, and any which may be formed before the next update to this document.

Assumptions

It is expected that, as the business evolves and Risk & Insurance Plans push the business towards greater maturity, this manual will require revisions to incorporate new or anticipated practices, procedures, or changes in best practice guidance.

As implementation progresses, additional elements will be introduced and implemented. This may include the use of risk metrics, establishment of a formal risk appetite framework including risk tolerances, development of Board and Executive dashboards and other reporting, the creation of monitoring processes over key risk treatment plans, and updates to governance and policy as required.

The information in this version is limited to the information available at the time of publication and it is to be used in conjunction with other policies and procedures. This document will exist a step behind the business given that the focus in the next several years is on implementation and raising the ERM maturity level overall, therefore procedures will potentially be added and enhanced with greater frequency than would be the case for a more mature process.

Given the recent restructure some terms are being used interchangeably throughout this document and may be more relevant and familiar dependant on the audience. Most notable;

- “Line of Business”, “Division” and “Subsidiary” are used somewhat interchangeably given the current structure of the organization
- “Vice President, VP”, “Executive Vice President, EVP” , “ President Hydro”
- “Strategic Plans”, “Strategic Business Plans” and “Business Plans”

We expect to have this will be updated as the corporate structure is finalized. Should you have any questions with respect to expectations based on the above please don’t hesitate to reach out to the CRO for clarity.

Who should use this Manual

This Manual is for the information and use of all stakeholders of the ERM Framework including the Board of Directors, Leadership Team, Risk Committee members, and any staff responsible for applying the principles and processes outlined herein.

1 ERM Framework

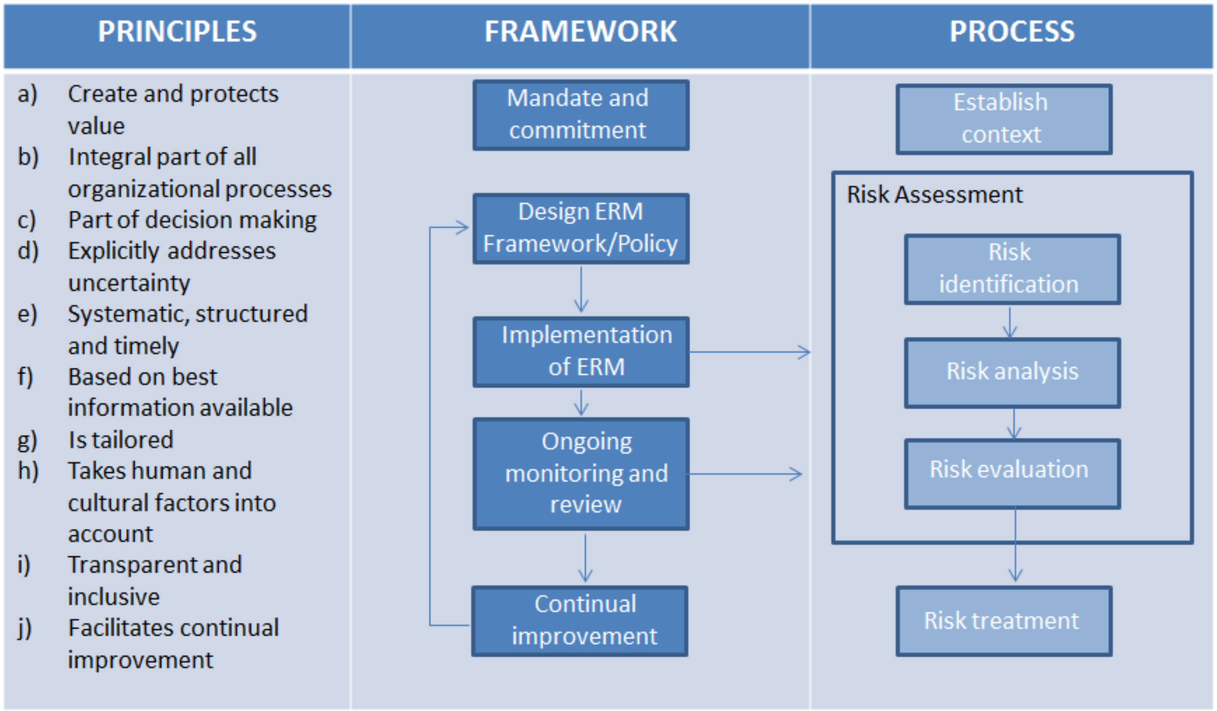
1.1 Background Information

A well designed framework ensures ERM is part of existing strategic and operational plans, internal control processes and day-to-day operations[1]. Additionally, it creates a common understanding of roles and responsibilities and promotes knowledge transfer across management

Some aspects of a fully integrated framework have not been implemented. The introduction of additional elements is outlined in Risk & Insurance Plans and will be incorporated into this document as they are embedded. This Framework & Procedures document should be read in concert with these documents.

This section includes a description of the elements of the ERM Framework, as well as the risk management process itself. A summary can be found in Figure 1.

Figure 1: Summary of ERM Principles, Framework and Risk Management Process


PRINCIPLES
FRAMEWORK
PROCESS
a) Create and protects value
b) Integral part of all organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on best information available
g) Is tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Facilitates continual improvement
Mandate and commitment
Design ERM Framework/Policy
Implementation of ERM
Ongoing monitoring and review
Continual improvement
Establish context
Risk Assessment
Risk identification
Risk analysis
Risk evaluation
Risk treatment

a) Framework - Mandate and Commitment

The ongoing effectiveness of a risk management framework depends on strong overall commitment by management and the Board of Directors. Senior leaders and the Board demonstrate this commitment by approving the *ERM Policy,* assigning resources to risk management initiatives and efforts, developing and utilizing risk related reporting and metrics, and ensuring risk is an integral part of strategic and business planning.

[1] Adopted from CAN/CSA-ISO31000-10

b) Framework – Design

Designing an ERM framework and supporting policy involves:

- Understanding the organization and its context and environment;
- Establishing a risk management policy framework;
- Clarifying roles and accountabilities for risk management;
- Integrating the risk management process into key organizational processes;
- Assigning appropriate resources to support the program; and
- Establishing internal and external communication and reporting mechanisms.

c) Framework - Implementation

In implementing a framework for managing risk, the organization must define the appropriate timing, resource and strategy. Risk management policies and processes should be integrated wherever possible into existing organizational processes and procedures and must impact decision making to be seen as effective. Implementation includes consultation and communications, information and training sessions, and feedback.

Risk & Insurance Plans are updated annually for each line of business and for the Risk & Insurance team. Updates, feedback, and templates developed through this process will be shared with the Risk Committees primarily so that the line of business leads and senior leadership have an opportunity to provide input. Figure 2 below provides a summary of the high level “building blocks” that are being progressed as well as the roles and responsibilities

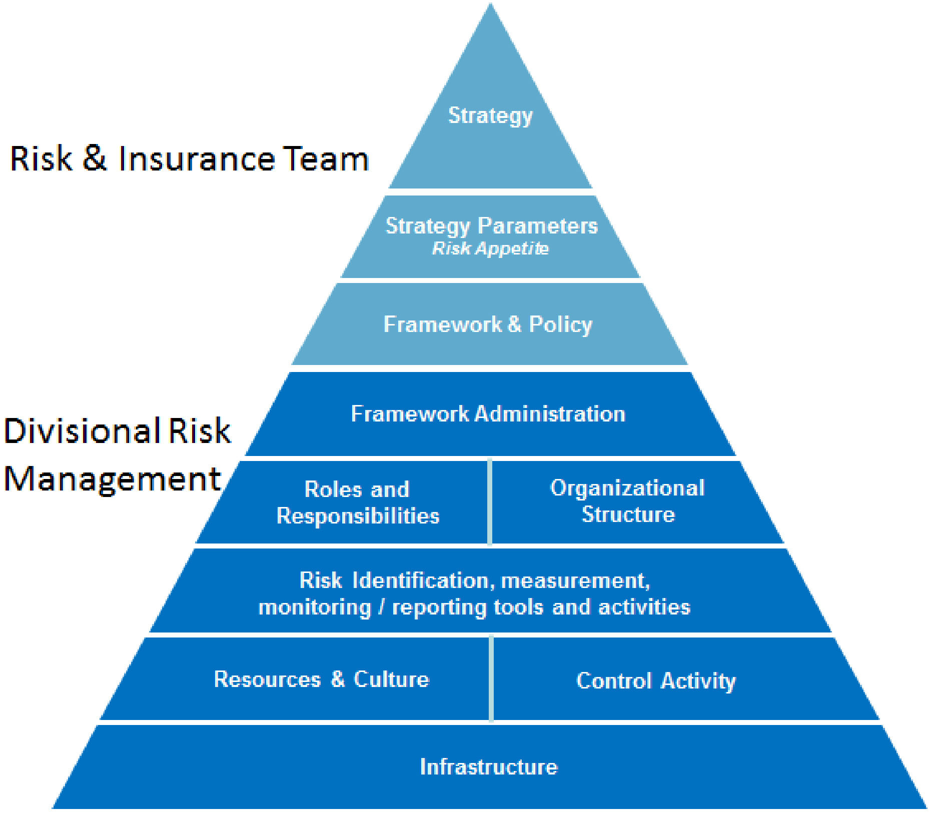


Figure 2: Risk Management Framework

d) Framework - Monitoring and Review

Progress against risk management plans will be measured and reported to divisional Risk Committees

Reporting on compliance with the *ERM Policy Statement* as well as the processes outlined herein may also form part of monitoring, as may periodic reviews of the effectiveness of the risk management framework overall by external parties.

Maturity assessments will be completed periodically to assess progress improving risk management maturity across the business.

e) Framework - Continual Improvement

Communication and consultation is a dialogue between an organization and its stakeholders. This dialogue is continual and iterative. It is a process that involves sharing and receiving information about the management of risk.

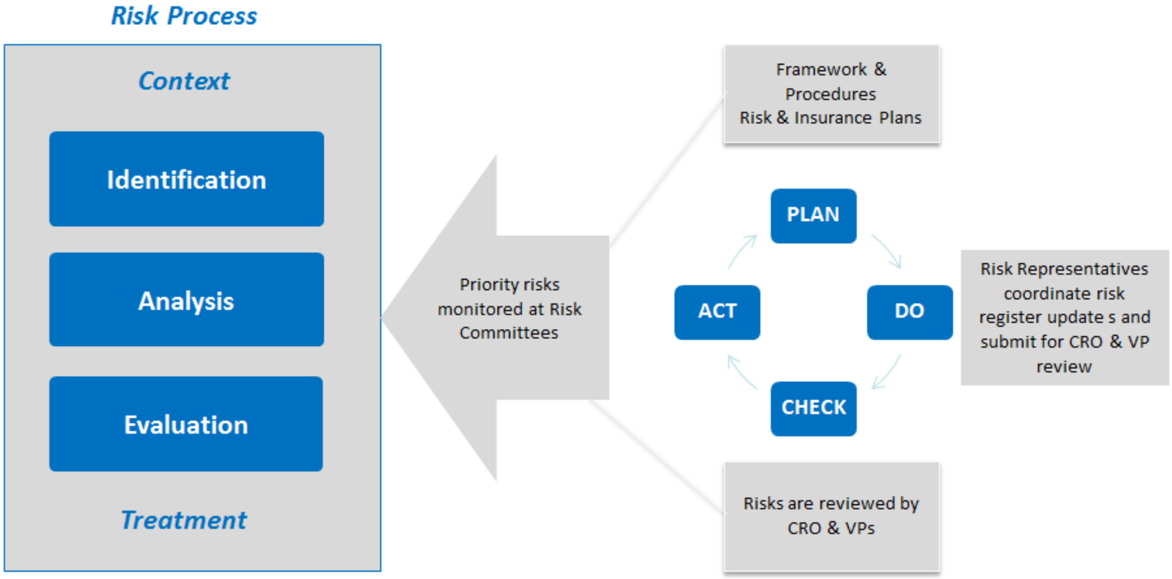
Discussions could be about the existence of risks, their nature, form, likelihood, and significance, as well as whether or not risks are acceptable or should be treated, and what treatment options should be considered.

It should also ensure that all stakeholders are involved and consulted as changes to the Framework are considered and that they are given an opportunity to give feedback on the benefits or challenges of implementation. This is accomplished primarily through the establishment and regular meetings of Risk Committees and by close engagement with ERM representatives.

1.2 Risk Management Process

The risk management process is the core of the Framework and can be applied to any area of the business that requires risk assessment. This process is summarized in Figure 3 below.

Figure 3: The Risk Management Process

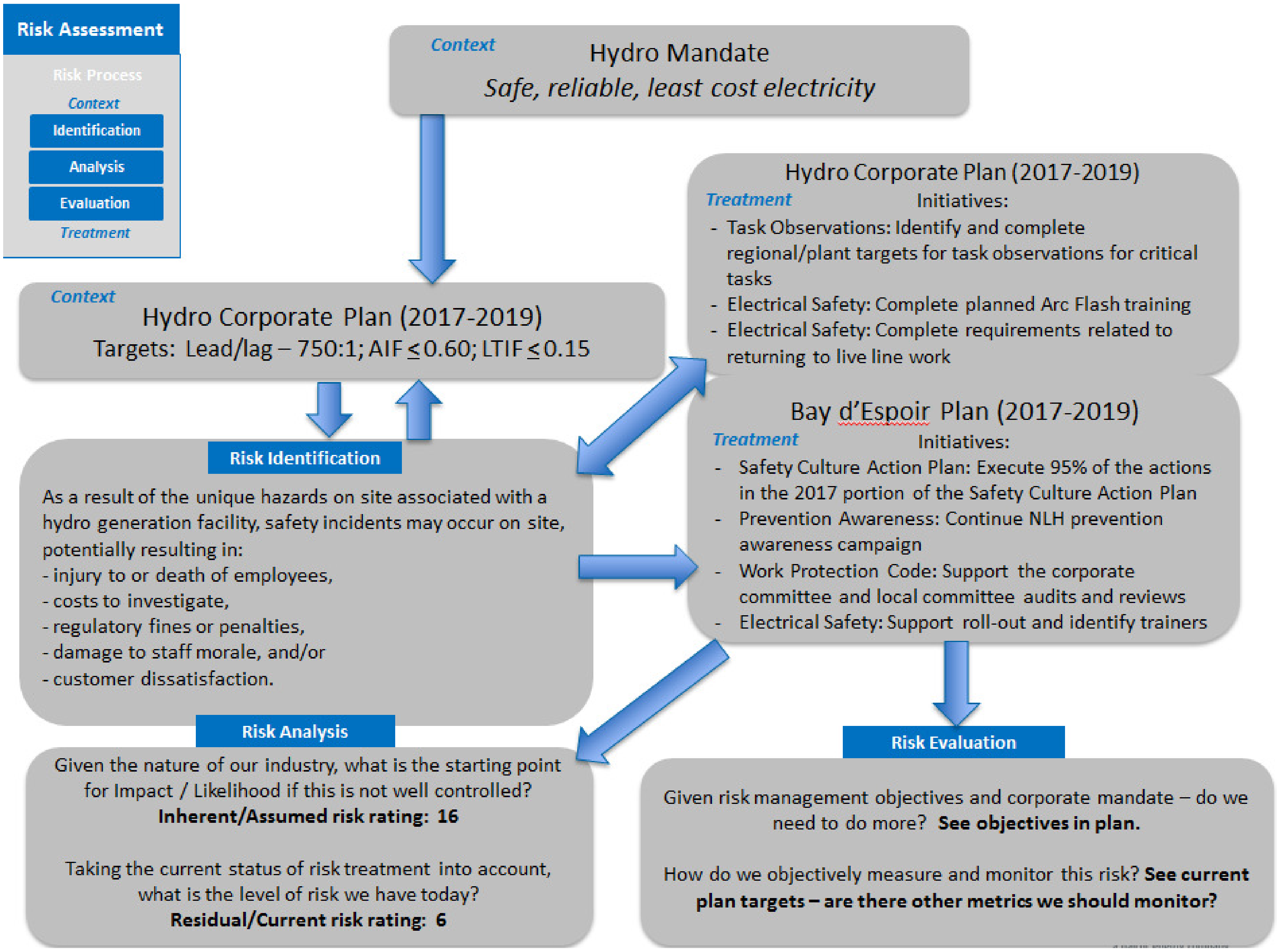

Risk Process
Context
Identification
Analysis
Evaluation
Treatment
Priority risks monitored at Risk Committees
Framework & Procedures Risk & Insurance Plans
PLAN
DO
CHECK
ACT
Risk Representatives coordinate risk register update s and submit for CRO & VP review
Risks are reviewed by CRO & VPs

Risk assessments can be done at different levels of the organization, including:

- Consolidated or subsidiary registers;
- Entity, divisional or departmental level risk assessments (lines of business);
- Process level risk assessments;
- Project risk assessments;
- Risk assessments for new products, markets or other opportunities; etc.

The level of detail may vary depending on the assessment being undertaken, however, the principles will remain the same in all instances. The descriptions that follow assume that risk is being assessed at either a consolidated or divisional level. Process, project, and other more detailed risk assessments are the responsibility of management and part of the company's internal control systems. They will focus on the objectives of the project and/or supporting processes, and will generally be more granular and detailed than those which are filed and retained as part of the ERM program. Examples include use of safety hazard registers, identification of environmental aspects, information systems vulnerability assessments, etc. They are important feeds to the program, however, and provide key insights into the right rating for consolidated level risks. See Figure 4 for an example of how safety (as a risk) ties to the Hydro Plan and Mandate.

Figure 4: Example- Linking Safety to Mandate, Plan & Risk



Risk Assessment

Risk Process

Context

Identification

Analysis

Evaluation

Treatment

Context Hydro Mandate

Safe, reliable, least cost electricity

Context Hydro Corporate Plan (2017-2019)

Targets: Lead/lag – 750:1; AIF ≤ 0.60; LTIF ≤ 0.15

Risk Identification

As a result of the unique hazards on site associated with a hydro generation facility, safety incidents may occur on site, potentially resulting in:

- injury to or death of employees,
- costs to investigate,
- regulatory fines or penalties,
- damage to staff morale, and/or
- customer dissatisfaction.

Hydro Corporate Plan (2017-2019)

Treatment Initiatives:

- Task Observations: Identify and complete regional/plant targets for task observations for critical tasks
- Electrical Safety: Complete planned Arc Flash training
- Electrical Safety: Complete requirements related to returning to live line work

Bay d'Espoir Plan (2017-2019)

Treatment Initiatives:

- Safety Culture Action Plan: Execute 95% of the actions in the 2017 portion of the Safety Culture Action Plan
- Prevention Awareness: Continue NLH prevention awareness campaign
- Work Protection Code: Support the corporate committee and local committee audits and reviews
- Electrical Safety: Support roll-out and identify trainers

Risk Analysis

Given the nature of our industry, what is the starting point for Impact / Likelihood if this is not well controlled?
Inherent/Assumed risk rating: 16

Taking the current status of risk treatment into account, what is the level of risk we have today?
Residual/Current risk rating: 6

Risk Evaluation

Given risk management objectives and corporate mandate – do we need to do more? **See objectives in plan.**

How do we objectively measure and monitor this risk? **See current plan targets – are there other metrics we should monitor?**

a) Step 1 – Establishing the Context

As outlined in Figure 4 under Process, context must be established before risk assessment and the treatment of risk can be documented. Establishing the context requires consideration of:

i. External Context / Environment

- Includes factors considered in a typical analysis of Strengths, Weaknesses, Opportunities and Threats ("SWOT"), which forms part of the strategic and business planning process.
- Examples include stakeholder expectations, cultural considerations, the business operating environment, the regulatory environment, financial markets, technological changes and the political landscape.

ii. Internal Environment

- Encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- Includes factors considered in typical SWOT analysis carried out in formulating the annual business plan and the 5-year strategic plan.
- Examples include information technology resources, the organizational culture and human resources (turnover, succession, training needs, etc.).

iii. Objective Setting

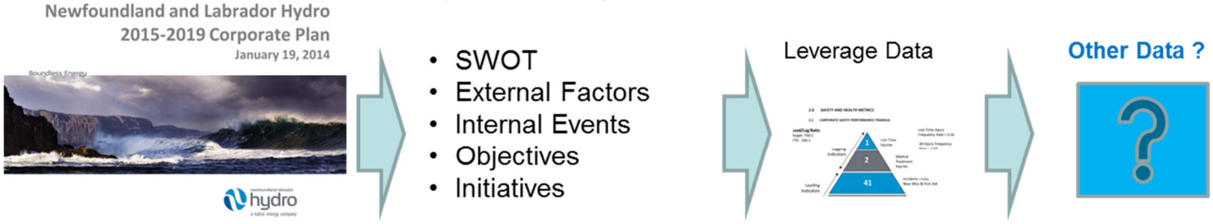
- Business goals are clearly articulated and link back to Safety, Environment, Business Excellence, People and Community.
- A business goal is a high-level statement what the company wants to achieve and typically does not change unless the vision or direction of the company changes
- Objectives are what the company will achieve during the planning period (specific, measurable, achievable, relevant and time-bound)
- Objectives are achieved through the initiatives that are included in the strategic, departmental, risk and insurance plans and other plans.
- Objectives must exist before identifying potential events affecting their achievement. If it is not very clear what the specific priority objectives are, time should be spent determining goals and objectives before the risk assessment begins.
- A target is a specific part, or interim step, of an objective to be achieved in the year
- An initiative is an activity or action to be completed in order to achieve anobjective or target

iv. Event Identification

- Historical and other known internal and external events can also be identified and reviewed as inputs.

Risks identified should be considered and evaluated in the context of the potential impact on our goals, objectives and initiatives. These factors are already considered through the business planning cycle, and therefore do not require a separate effort. There should be a clear and demonstrable linkage between what is contained in business plans and the risks identified. Risk assessment is an important part of business planning.

Figure 5: Setting Context

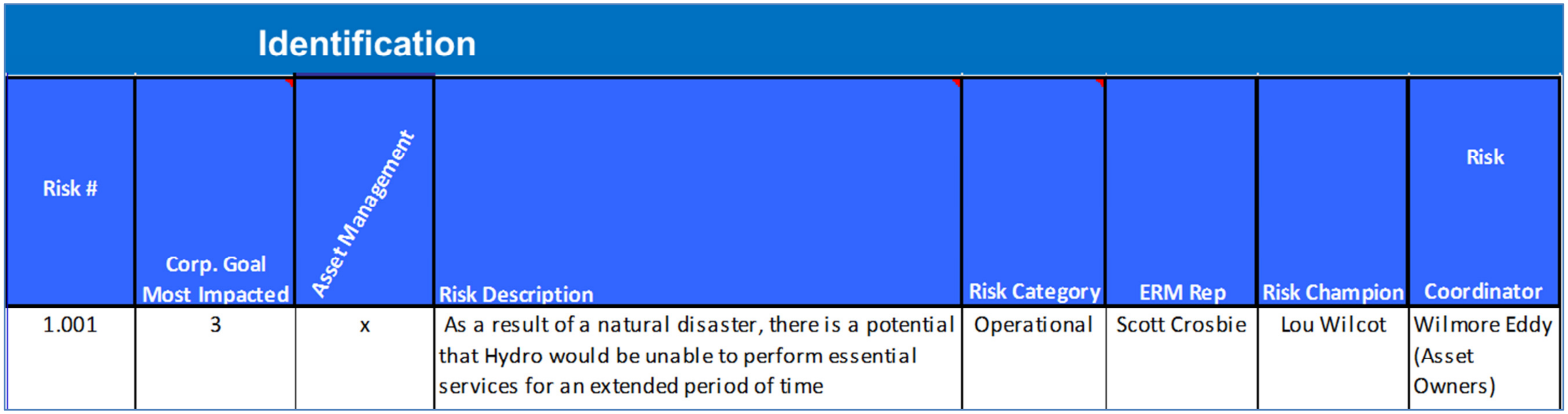


The risk assessment should inform the planning process, and may lead to the identification of additional objectives that were not reflected in the strategic plan but that arose out of the context setting exercise.

As shown in Figure 5, once the context is established, the risk assessment steps can begin. The purpose of a risk assessment is to accurately assess the risks that are assumed by the organization, as a result of operating a line of business, taking on a particular project, or introducing a critical business process.

There are two 'sides' to a risk assessment. The first is considering the "inherent risk" (i.e. assumed risk level). This is the level of risk the organization assumes just by operating in the chosen industry, for example. It does not consider any management intervention or risk treatment. The second is "residual risk" (i.e. current risk level). Once all management actions are documented and assessed for effectiveness, this represents the level of risk exposure the organization is living with today, taking management interventions and actions into account. The rating scales used are part of the *ERM Toolset*. Risks are documented in risk registers. Excerpts of the *risk register* used are shown throughout, see Figure 6-8. A separate template is generally used for corporate service functions, such as Environment and Information Technology. This is referred to as a '*Detailed Risk Treatment Plan'*.

Figure 6: Risk Identification



Identification

Risk #	Corp. Goal Most Impacted	Asset Management	Risk Description	Risk Category	ERM Rep	Risk Champion	Risk Coordinator
1.001	3	x	As a result of a natural disaster, there is a potential that Hydro would be unable to perform essential services for an extended period of time	Operational	Scott Crosbie	Lou Wilcot	Wilmore Eddy (Asset Owners)

b) Step 2 - Risk Identification

The framework broadly defines risk as the effect of uncertainty on objectives. Hence, it is important to remember that risk identification is always performed in the context of related objectives.

Risks should be stated in the following format:

> "As a result of a **Definite Cause** an **Uncertain Event** may occur, resulting in a **Negative** or **Positive Impact**."
>
> **Definite Cause**: Clearly state the root cause/(s) and risk event trigger/(s)
> **Uncertain Event**: Clearly state nature of the risk event triggered by the cause
> **Negative Impact**: Clearly state the nature of the loss that would be prompted by the uncertain event
> **Positive impact**: Clearly state nature of the opportunity prompted by the uncertain event

An alternative statement format is the use of 'IF… THEN…' statements, as follows: **IF**…As a result of competition from other provinces and/or new projects in NL **THEN**….the Project may have challenges recruiting and retaining skilled, experienced trades, resulting in poor productivity, cost growth and schedule slippage.

Either option gives cause and effect, the first is advantageous in that it provides more detail on possible impacts.

Once objectives and their related risks are identified, it is necessary to categorize them as either (1) Operational, (2) Strategic, (3) Financial and/or (4) Compliance risks. Users should refer to the *ERM Risk Category – Subcategory Catalog*, which can be found in the *ERM Toolset*. The *Financial Risk Management Policy* is also a useful reference with respect to the various categories of financial risk.

Categorization of risks will allow for the eventual aggregation of line of business risks at a consolidated level, creating a consistent data source for future risk reporting, and providing a common language for discussing risk across the organization.

Once identified, key priority risks to each line of business level should be inventoried using a *Risk Register*. A sample is included in the *ERM Toolset*. In order to be aligned with best practice with respect to identifying risks, in addition to the considerations given in Section 1.2, risk owners should consider the following:

- It is imperative to consider the “other side” of all opportunities – that is, the risks associated with not pursuing an opportunity should always be considered;
- Identification should include risks impacting line of business goal achievement vs objective irrespective of whether their source is under control of the particular line of business. Involve subject matter experts from Finance, Information Security, etc.;
- For each risk identified, so-called “knock-on” or “spin-off” impacts should be considered.

Once risks have been identified and inventoried in the registers, the line of business ERM Representative(s) are responsible for identifying a risk owner for each risk, which should be the individual with the required expertise to manage and assess the particular risk. ERM Representatives are also responsible for ensuring that the owners understand their role as described in Section 2.2, and for assisting risk owners in completing required documentation.

Designated risk owners must use the rating tools provided in the *ERM Toolset* to determine a risk rating for each risk for which they have ownership, on the basis of Impact and Likelihood, as well as other rationale of these ratings. They also must document and capture risk treatment plans, either planned or implemented.

c) Step 3 - Risk Analysis

Once risks associated with objectives are appropriately identified and categorized, the risk assessment process continues with risk analysis. This involves considering the Impact & Likelihood ratings for each risk on both an inherent (“assumed”) and residual (“current”) basis.

The outcome of this analysis are ratings for each risk (Low, Medium, High), based on the likelihood of occurrence (i.e. probability) and the potential impact. Tools for risk analysis include the *Risk Rating Matrix, Impact Measurement Tool* and the *Financial Impact Matrix,* which are included in the *ERM Toolset*. (These tools should be consulted in conjunction with this document)

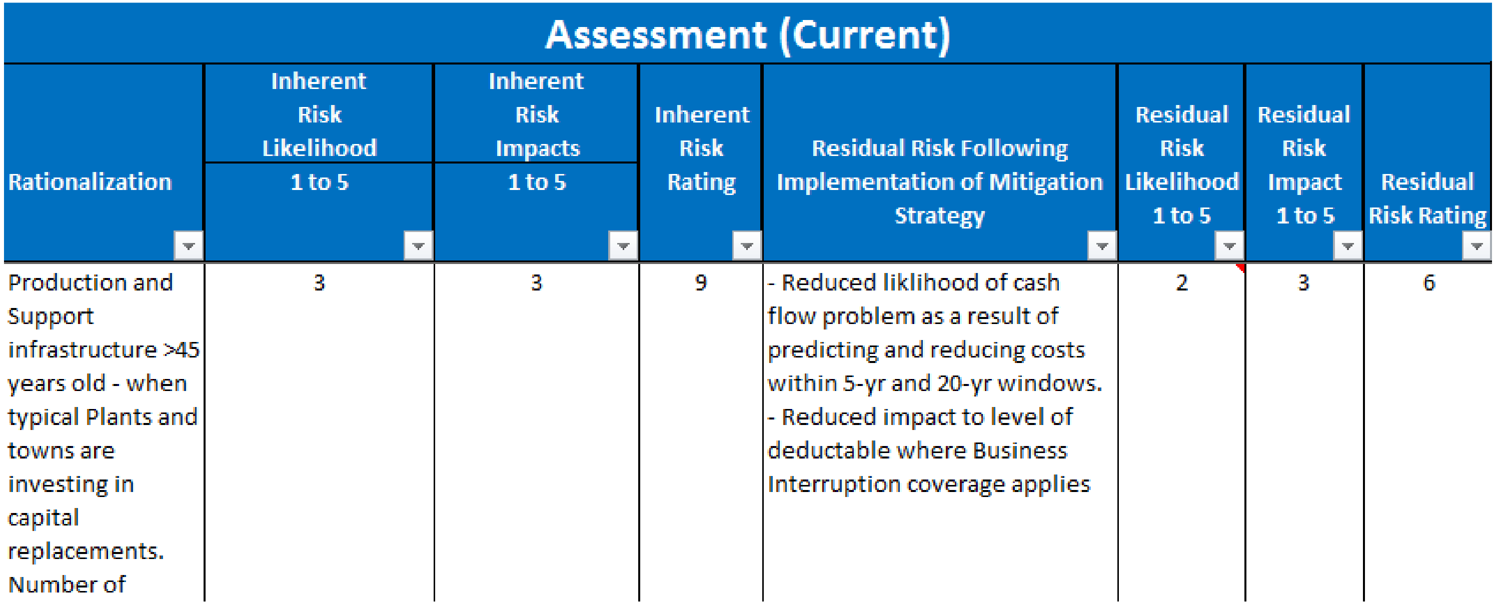
The impact and likelihood ratings assigned should be supported by adequate rationale such that a third party could understand why a particular rating was selected.

Completing this exercise allows for risks to be sorted on the assumed and/or current ratings they were given to identify key areas of focus which would require further evaluation, as detailed in the next section. See Figure 7 below.

Important notes: *It is important to note that current risk ratings should reflect only the impact of management actions that are known to be effective at the time of assessment, and do not consider future planned actions. Key controls should be monitored to give management assurance that they are working as expected.*

If a long list of risks is identified, it is recommended that an initial ranking be taken to prioritize documentation efforts or identify priority risks for focus on treatment and documentation. Software is available through Risk and Insurance to facilitate this process.

Figure 7: Risk Analysis



Assessment (Current)							
Rationalization	Inherent Risk Likelihood 1 to 5	Inherent Risk Impacts 1 to 5	Inherent Risk Rating	Residual Risk Following Implementation of Mitigation Strategy	Residual Risk Likelihood 1 to 5	Residual Risk Impact 1 to 5	Residual Risk Rating
Production and Support infrastructure >45 years old - when typical Plants and towns are investing in capital replacements. Number of	3	3	9	- Reduced liklihood of cash flow problem as a result of predicting and reducing costs within 5-yr and 20-yr windows. - Reduced impact to level of deductable where Business Interruption coverage applies	2	3	6

d) Step 4 - Risk Evaluation

Risk evaluation involves tying the risks identified to other aspects. This includes considering what feedback management receives regarding the effectiveness or quality of a particular management action, such as the results of any audits or regulatory reviews completed. Risk owners should escalate to Management where key controls and processes are in place but where monitoring reviews are not established to give them regular feedback that they are working as intended. Resources (people, systems, etc.) may need to be re-allocated to provide this feedback, which is a critical component of effective control.

Recommendations should also be made where controls or processes are not in place, or are not working to address the risk.

For priority risks, these recommendations are a critical input to annual planning and budgeting process, and the corresponding actions should be actively managed.

e) Step 5 - Risk Treatment

This step in the process will differentiate the various risk treatment strategies that are available to management to reduce risk exposure. The risk owner can choose to (1) avoid, (2) mitigate, (3) transfer, and/or (4) accept the risk.

Risk Avoidance – Risk avoidance can be as simple as avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk. Instead of avoiding the risk, the owner can transfer it to another party, through the use of insurance, outsourcing, or specific contractual terms (where applicable, and with their own set of related risks).

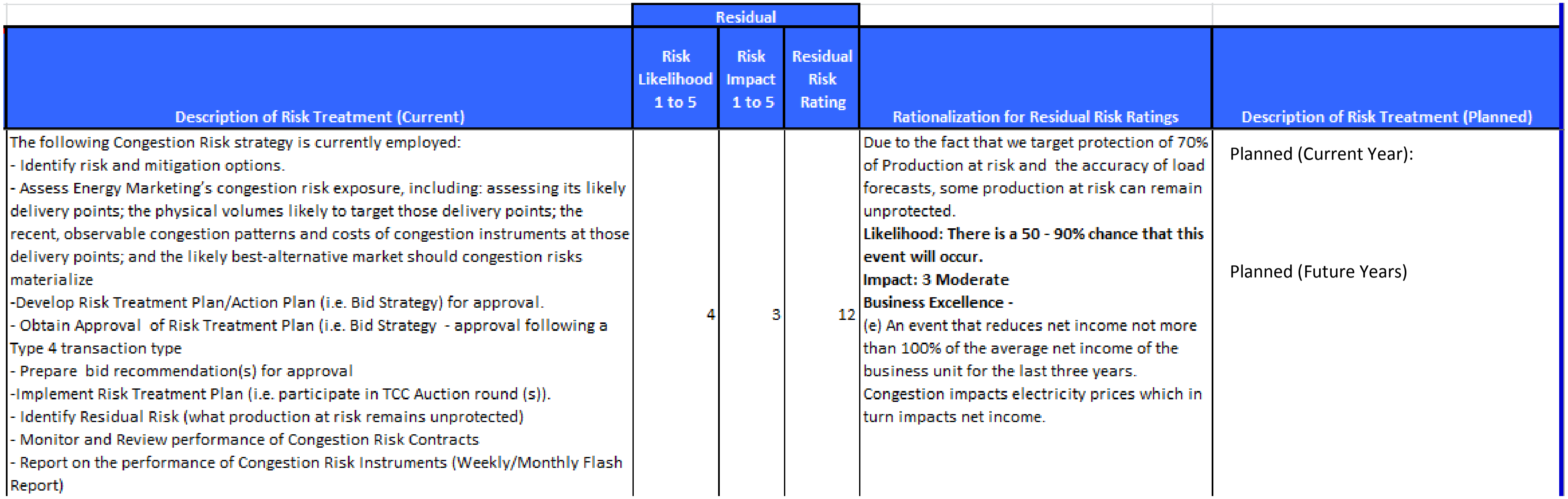
Risk Mitigation – Mitigation can be equated with adjusting the internal controls in place to manage the risk by adding, modifying, or even removing controls to better suit the risk being managed. For example, installing fire suppression systems where none were installed before to protect critical operational assets.

Risk Transfer – Alternatively, the owner may attempt to reduce likelihood of occurrence by implementing a risk transfer strategy. Examples include the use of derivative financial instruments to address foreign exchange rate or commodity price exposure, or the purchase of insurance policies.

Risk Acceptance – In contrast, with risk acceptance the risk owner can make the informed decision to take no further action and retain the risk in pursuit of a commensurate return. Analysis may also show that the cost of implementing further risk reduction measures does not provide enough benefit to make this a viable or prudent option.

At the line of business level, Risk Treatment Plans are currently captured in the *Risk Register.* See Figure 8 below.

Figure 8: Documentation of Risk Treatment Strategies



	Residual				
Description of Risk Treatment (Current)	Risk Likelihood 1 to 5	Risk Impact 1 to 5	Residual Risk Rating	Rationalization for Residual Risk Ratings	Description of Risk Treatment (Planned)
The following Congestion Risk strategy is currently employed: - Identify risk and mitigation options. - Assess Energy Marketing's congestion risk exposure, including: assessing its likely delivery points; the physical volumes likely to target those delivery points; the recent, observable congestion patterns and costs of congestion instruments at those delivery points; and the likely best-alternative market should congestion risks materialize -Develop Risk Treatment Plan/Action Plan (i.e. Bid Strategy) for approval. - Obtain Approval of Risk Treatment Plan (i.e. Bid Strategy - approval following a Type 4 transaction type - Prepare bid recommendation(s) for approval -Implement Risk Treatment Plan (i.e. participate in TCC Auction round (s)). - Identify Residual Risk (what production at risk remains unprotected) - Monitor and Review performance of Congestion Risk Contracts - Report on the performance of Congestion Risk Instruments (Weekly/Monthly Flash Report)	4	3	12	Due to the fact that we target protection of 70% of Production at risk and the accuracy of load forecasts, some production at risk can remain unprotected. **Likelihood: There is a 50 - 90% chance that this event will occur.** **Impact: 3 Moderate** **Business Excellence -** (e) An event that reduces net income not more than 100% of the average net income of the business unit for the last three years. Congestion impacts electricity prices which in turn impacts net income.	Planned (Current Year): Planned (Future Years)

f) Step 6 - Monitoring and Review

An ERM Framework requires monitoring on several levels. This includes

g) Review of the Framework itself
h) Compliance with the ERM policy
i) Compliance with the Divisional and/or Lines of Business plans developed
j) Risk Register Review - Management are expected to monitor the controls they identify to control priority risks as part of implementing appropriate management and internal control systems. See figure 9 below that outlines the Risk Register review process.

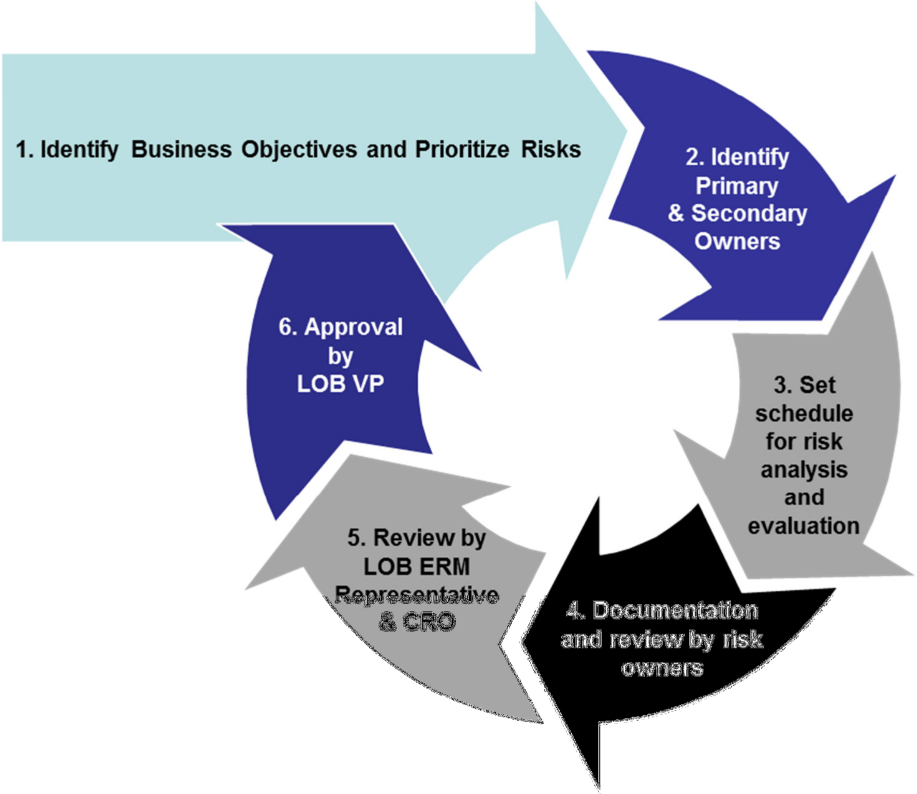
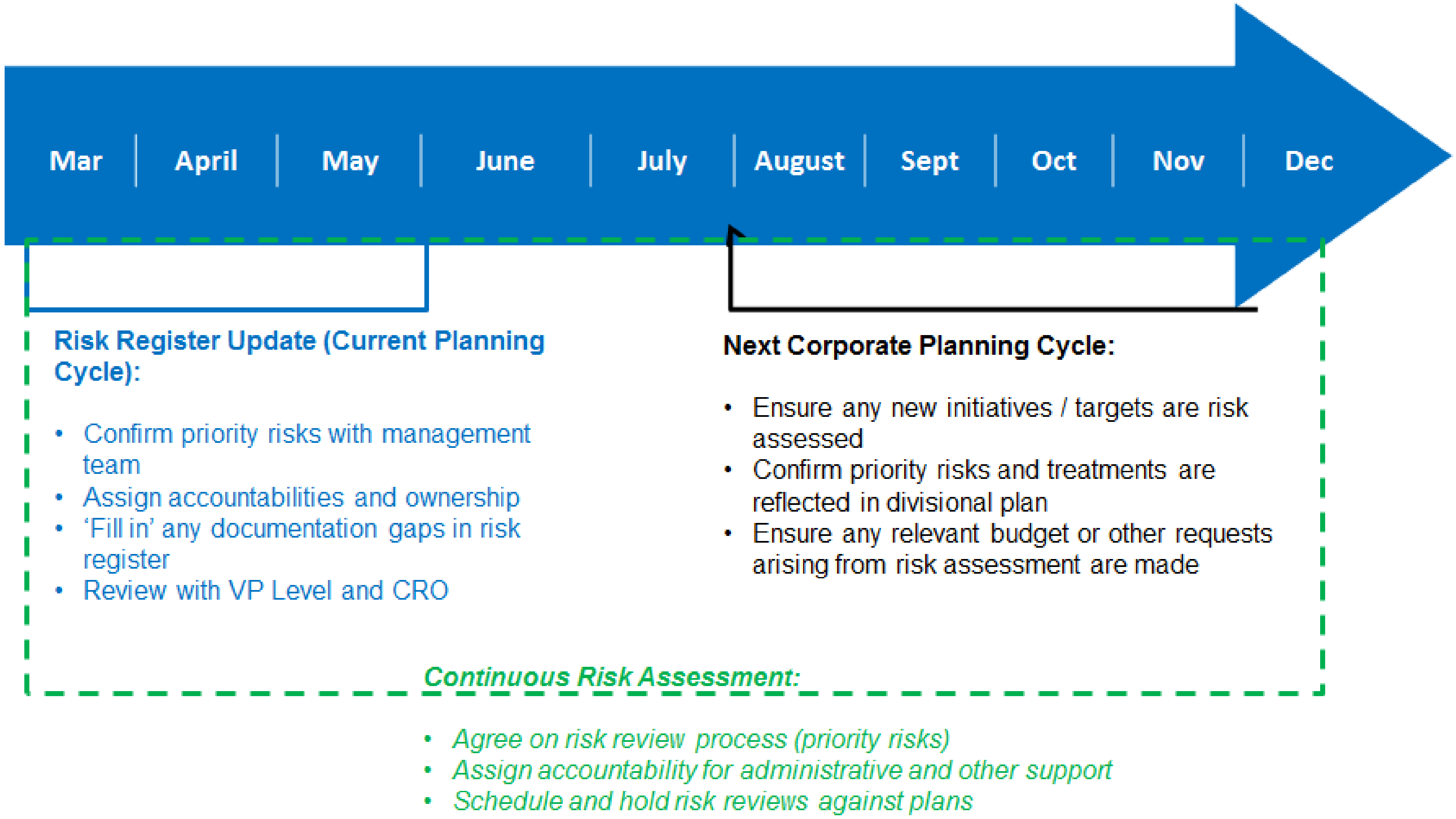

1. Identify Business Objectives and Prioritize Risks
2. Identify Primary & Secondary Owners
3. Set schedule for risk analysis and evaluation
4. Documentation and review by risk owners
5. Review by LOB ERM Representative & CRO
6. Approval by LOB VP

Figure 9: Risk Register Review cycle

The annual review process and risk register review cycle is outlined below in Figure 10. This risk register review process and cycle aligns with planning and budget cycle.

Figure 10: Annual Risk Assessment Process



Risk Register Update (Current Planning Cycle):

- Confirm priority risks with management team
- Assign accountabilities and ownership
- 'Fill in' any documentation gaps in risk register
- Review with VP Level and CRO

Next Corporate Planning Cycle:

- Ensure any new initiatives / targets are risk assessed
- Confirm priority risks and treatments are reflected in divisional plan
- Ensure any relevant budget or other requests arising from risk assessment are made

Continuous Risk Assessment:

- *Agree on risk review process (priority risks)*
- *Assign accountability for administrative and other support*
- *Schedule and hold risk reviews against plans*

2 Roles and Responsibilities

The objective of the risk management program is to ensure that risks are managed and monitored in a structured and consistent manner throughout the organization and in line with the expectations of our stakeholders.

The **Boards of Directors** are responsible to ensure management has processes in place to effectively identify and control risk, and that these processes can be demonstrated.

Senior management is responsible to identify, analyze, treat, monitor and report on risks that threaten the achievement of their business objectives.

All staff have a responsibility to appropriately balance risk and reward within the activities that they operate, and to raise concerns where they are unsure this balance has been struck. Employees must understand their role with respect to processing transactions and are the ones who bring risk mitigation (i.e. internal controls) to life.

The internal control system is an important source of risk data and insights. For example, strong internal control requires that management understand the key risks facing their business, which identifies critical business processes, i.e. those processes which exist to manage those priority risks.

2.1 Chief Risk Officer

The high-level role of the Chief Risk Officer's Risk and Insurance team is to support the Risk Management Program and the ERM framework and supporting policies. Some activities that fall under the Risk Management Program are as follows:

- Ensure Risk and Insurance plans are kept up to date, in consultations with divisions, lines of business and departments
- Consult with lines of business in creation of new guidance or update of existing guidance
- Facilitate and oversee annual risk assessment process company-wide
- Develop and maintain ERM Corporate five year plan
- Coordinate and review risk reporting
- Provide dedicated compliance oversight to Energy Marketing with respect to financial and operational risks
- Coordinate and facilitate annual portfolio risk assessment
- Ensure periodic reviews of Framework and process effectiveness

2.2 ERM Representatives

Each line of business will have an ERM representative whose responsibilities will include:

- Ensure the identification of priority business risks and the assignment of accountabilities
- Ensure the delivery of actions agreed upon in Risk & Insurance Plans. This may include the development of risk reporting and/or risk profiles

- Secure appropriate consulting and other expertise and resources to deliver line of business Risk and Insurance plans
- Identify any training needs for the line of business/division

2.3 Role of Risk Owners

Each risk in a *Risk Register* will have a Primary and Secondary Risk Owner. As outlined above, designated risk owners are responsible for ensuring the use of the *ERM Toolset* to assess each risk for which they have ownership. The risk owners are also accountable and responsible for implementing any budgeted treatment strategies.

Primary Risk Owner: One line of business contact will be identified as a primary owner of each priority risk; their responsibilities include:

- Coordinating necessary meetings with secondary risk owners or otherwise keeping advised of the status of actions against priority risks
- Ensuring that the information presented on the risk in the *Risk Register* is current and complete;
- Ensuring the documentation of risk treatment plans within the *Risk Register*; and
- Considering whether appropriate monitoring and reporting exists where critical processes and controls are identified as part of the risk register review cycle
- Implementing any new mitigation strategies, and ensuring that these find their way into the planning cycles and budgets where required.
- Known previously as "*Risk Champion*"

Secondary Risk Owner(s): Depending on the risk, there may be numerous functions and departments, either within or outside of the line of business, that will need to take action(s) as part of the treatment plan for that risk; their responsibilities include:

- Providing input regarding risk treatment, if outside the control of the line of business or division
- Providing updates on risk treatment plan status to the Primary Risk Owner in advance of Risk Committees and other meetings as required
- Advising the Primary Risk Owner immediately if priority actions are trending off plan or if a critical business process or control does not operate as expected.

2.4 Role of Executive Owners

Executive Risk Owner(s): Executives have primary ownership of consolidated or divisional level risks. Their responsibilities include:

- Coordinating necessary meetings with action plan owners to keep advised of status;
- Preparing and submitting reports regarding key risks to the Risk Committee(s), in accordance with an agreed scheduled and using approved templates as they are developed and approved by the Committees;
- Working with CRO and ERM representative to ensure that the use of ERM tools and templates is aligned with corporate methodology;

- Ensuring the documentation of risk treatment plans; and
- Providing a consolidated view of risk exposure across all entities.

Executives may decide to delegate these responsibilities, but remain accountable for ensuring they are fulfilled.

2.5 Role of Internal Audit

There are a number of key roles that the internal audit function plays in the ERM Framework, both during the implementation and on an ongoing basis thereafter such as:

- Leveraging the consolidated and divisional risk profiles to facilitate audit planning;
- Providing assurance on the risk management process (risk identification, risk analysis and risk evaluation);
- Evaluating the Framework and risk management process outlined in Figures 1 & 2; and

Also, as the implementation of the Framework progresses, Internal Audit may commence regular reporting to the Board on its audits of the Framework.

However, to ensure appropriate segregation of duties, Internal Audit will not[3]:

- Have any accountability for the ERM Framework;
- Have any involvement in the process of formulating risk appetite;
- Make any decisions with respect to the treatment of risks; or
- Implement any risk mitigation or other treatment of risks on behalf of management.

2.6 Role of Strategic and Business Planning

There is a recognized importance of a clear linkage with the strategic and business planning processes. It is for this reason that updates to the *Risk Register* are made at the same time that business plans are being updated. The risk assessments done as part of the ERM program are to link directly to the objectives, targets and initiatives detailed in strategic plans, which are created around our corporate goals.

[3] Internal Auditing's Role in Risk Management (IIARF White Paper – March, 2011)

3 Risk Committees

The Risk Committees are established to meet the following high level objective:

To confirm that risks are being managed within the parameters established by the Board of Directors as referenced in the Enterprise Risk Management ("ERM") Policy, ERM-01

These Committees are responsible to articulate and monitor priority risk for their division. This Information is submitted to the Risk & Insurance team quarterly, and will be used as an input to developing a consolidated risk profile for the organization.

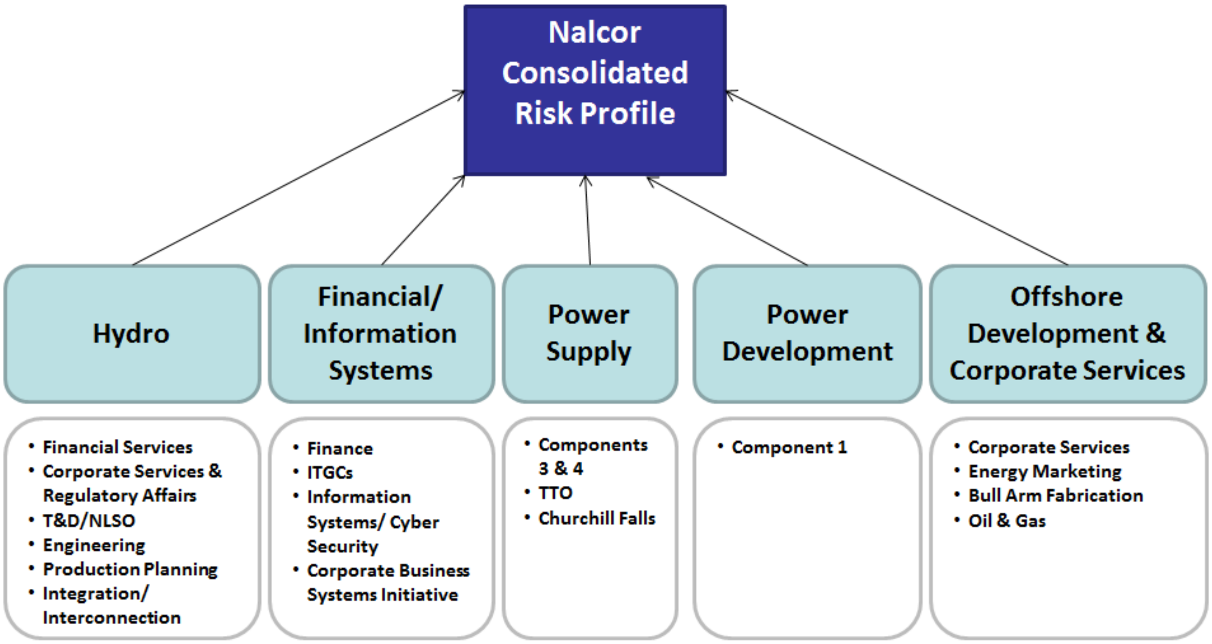
Progress and timelines identified in Risk & Insurance Plans are also overseen by the Risk Committees, which are made up of senior managers and risk representatives.

Risk Committee Membership

Risk Committee members are appointed by each EVP, and the President, Hydro in consultation with the Chief Risk Officer. Each committee shall approve a Terms of Reference document governing their activities. This is to be reviewed annually.

Several planned enhancements are underway at a consolidated level. Largely, these enhancements are focused on creating routine risk reports at a line of business and divisional level, as well as a consolidated Risk Profile.

Figure 11 – Consolidation of Risk Reporting


Nalcor Consolidated Risk Profile
Hydro
Financial/ Information Systems
Power Supply
Power Development
Offshore Development & Corporate Services
• Financial Services
• Corporate Services & Regulatory Affairs
• T&D/NLSO
• Engineering
• Production Planning
• Integration/ Interconnection
• Finance
• ITGCs
• Information Systems/ Cyber Security
• Corporate Business Systems Initiative
• Components 3 & 4
• TTO
• Churchill Falls
• Component 1
• Corporate Services
• Energy Marketing
• Bull Arm Fabrication
• Oil & Gas

4 Use of Risk & Insurance Plans

4.1 Line of Business and Risk & Insurance Plan

Risk & Insurance plans are developed for both the line of business and consolidated levels. These documents set out risk management initiatives for the year ahead and with a 5 year view (3-year at Hydro), detailing a set of realistic goals and objectives along with proposed timelines for completion. They inform strategic plans with respect to the resources required to move ERM implementation forward.

The basis for a Risk & Insurance Plan is to close a known gap or to increase the effectiveness of risk management for the Line of Business, thereby moving the level of maturity and sophistication forward. Risk & Insurance Plans are tailored for each line of business based on maturity and current state. A template has been provided to support the development of these plans.

All plans will be reviewed and approved by the CRO and ERM Representative. The line of business VP is ultimately accountable for the Risk & Insurance Plan and supporting risk activities, and the ERM Representative is responsible for ensuring adequate consultation and engagement at this level.

5 ATIPPA/Energy Corporation Act & ERM

5.1 ATIPPA & ERM

Some of the information captured in our risk registers is considered commercially sensitive and would not normally be released in response to a request for information

- Risk registers contain recommendations, plans or proposals in many cases to establish new programs or to change a program that have not been implemented
- The relevant sections here are the ones relating to treatment of risks as well as the ratings that drove the recommendations, plans or proposals

5.2 Energy Corporation Act & ERM

The risk assessments done as part of the ERM program are done at the level of each entity and in the context of their strategic plans

- The workshop approach recommended for all lines of business ensures this linkage is properly captured and can be demonstrated
- One of the main objectives of these assessments is to determine whether or not recommendations are to be put forward each year regarding how we manage risks within the organization

These documents form part of the strategic plan and the focus of this program is to create a consolidated view of risk.

- The risk registers are subject to the exclusions in the Energy Corporation Act since much of the information contained would be considered commercially sensitive as part of Nalcor's strategic business plans

5.3 Implications

- More often than not, risk descriptions would be subject to release as they represent risks typical to an organization operating in our various industries (eg. risks inherent to a utility or energy marketing operation)
- There will be some exceptions to this where the risk descriptions themselves contain information or content deemed commercially sensitive, as such no information should be released without review by CRO, Legal Counsel, the relevant EVP, or President, Hydro, CFO & VP Finance and Manager, Corporate Communications.
- As part of the ERM review, disclosure notes have been added to the Risk Registers in the near term on the advice of Legal Counsel, and care should be taken to mark 'DRAFT' on all working copies
- There is no reason not to communicate by email, but these documents should be treated as confidential and sensitive at all times

6 Required Frequency

The following table outlines current standards with respect to frequency for key processes within the ERM Framework. This table will expand as the Framework is implemented.

Frequency of Key Processes

ERM Framework	Frequency or deadline
1. Review ERM Policy Statement and Framework & Procedures document, and update if required	Annually
2. Review/update Departmental Risk & Insurance Plan	Annually
3. Review/update Divisional/Line of Business Risk & Insurance Plans	Annually
4. Compliance reviews – ERM Policy and Framework	Annually
5. Complete and monitor Maturity Assessment by division	Periodically
6. Independent assessment of ERM effectiveness	Periodically
7. Deliver and/or source Board level ERM training	On request
Line of Business/Divisional Level Risk Management Processes	**Frequency or deadline**
8. Divisional Risk Committee meetings	Quarterly
9. Complete line of business level risk assessment	Annually
10. Review/update Risk and Insurance Plans	Annually
11. Deliver and/or source ERM training	As required
12. Secure appropriate consulting and other expertise	As required
Consolidated Risk Management Processes	**Frequency or deadline**
13. Update consolidated corporate risk assessment	Annually
14. Deliver and/or source ERM training	On request
15. Secure appropriate consulting and other expertise	As required

7 Glossary of Key Terms

The following definitions are adapted from a number of sources: (1) Committee of Sponsoring Organizations of the Treadway Commission (COSO), (2) Deloitte and Touche LLP and CAN/CSA-ISO 31000-10 as published by the National Standard of Canada.

Assumed (inherent) risk – the risk without considering any risk treatment (i.e. the risk assumed by participating in a given industry, selling a certain product, etc.).

Current (residual) risk – the risk remaining after considering the effectiveness of chosen risk treatment (i.e. post-mitigation).

Enterprise risk management – a group of coordinated activities, affected by the organization's board of directors, management and other personnel in strategy setting and across the enterprise, designed to identify potential events that may affect the organization, and manage risk to be within the organization's risk appetite.

ERM framework – set of components that provide the foundations (policy, objectives, mandate and leadership commitment) and organizational arrangements (accountabilities, processes, responsibilities and resources) for designing, implementing, monitoring, reviewing and continually improving risk management throughout an organization.

ERM toolset – the collection of tools and templates developed and maintained by the Risk and Insurance department for use by employees in implementing the ERM Framework.

ERM policy – statement of overall intentions and direction of an organization related to ERM.

External context – external environment in which the organization seeks to achieve its objectives including key drivers and trends having an impact on the objectives of an organization and the cultural, social, political, legal, regulatory, financial, economic, natural and competitive environments in which it operates.

Impact – The relative significance of a particular risk to an entity if that risk event came to pass. The magnitude of the impact is assessed with respect to the effect on achieving the corporate goals of Safety, Environment, Business Excellence, People and Community.

Internal context – internal environment in which the organization seeks to achieve its objectives, which encompasses consideration of the organization's governance framework, organizational structure, objectives, capabilities, culture, policies and information systems.

Internal control – a process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

Likelihood – the probability that a particular risk will occur within a given time period. In assessing the probability of occurrence for the purpose of risk assessment, it is important to define the time period over which the likelihood of occurrence is being assessed.

Risk – the effect of uncertainty on objectives, or anything that could prevent the organization from achieving its objectives if it came to pass (sometimes referred to as a “risk event”).

Risk appetite – the nature and amount of risk an organization is willing to take on in pursuing its goals. Forms the bounds within which management must operate the business. It is often supported by more granular tolerance limits against agreed key risk indicators (i.e. metrics).

Risk analysis – process undertaken to comprehend the nature of risk and to determine the level of risk.

Risk assessment – the overall process of risk identification, risk analysis and risk evaluation.

Risk capacity – a key consideration in formulating risk appetite, it refers to the organization’s ability to assume the impact of an adverse event as well as its degree of sophistication with respect to effecting risk management processes.

Risk categories – Financial, Strategic, Operational or Compliance.

Risk evaluation – process of comparing the results of the risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk identification – process of finding, recognizing and describing risks.

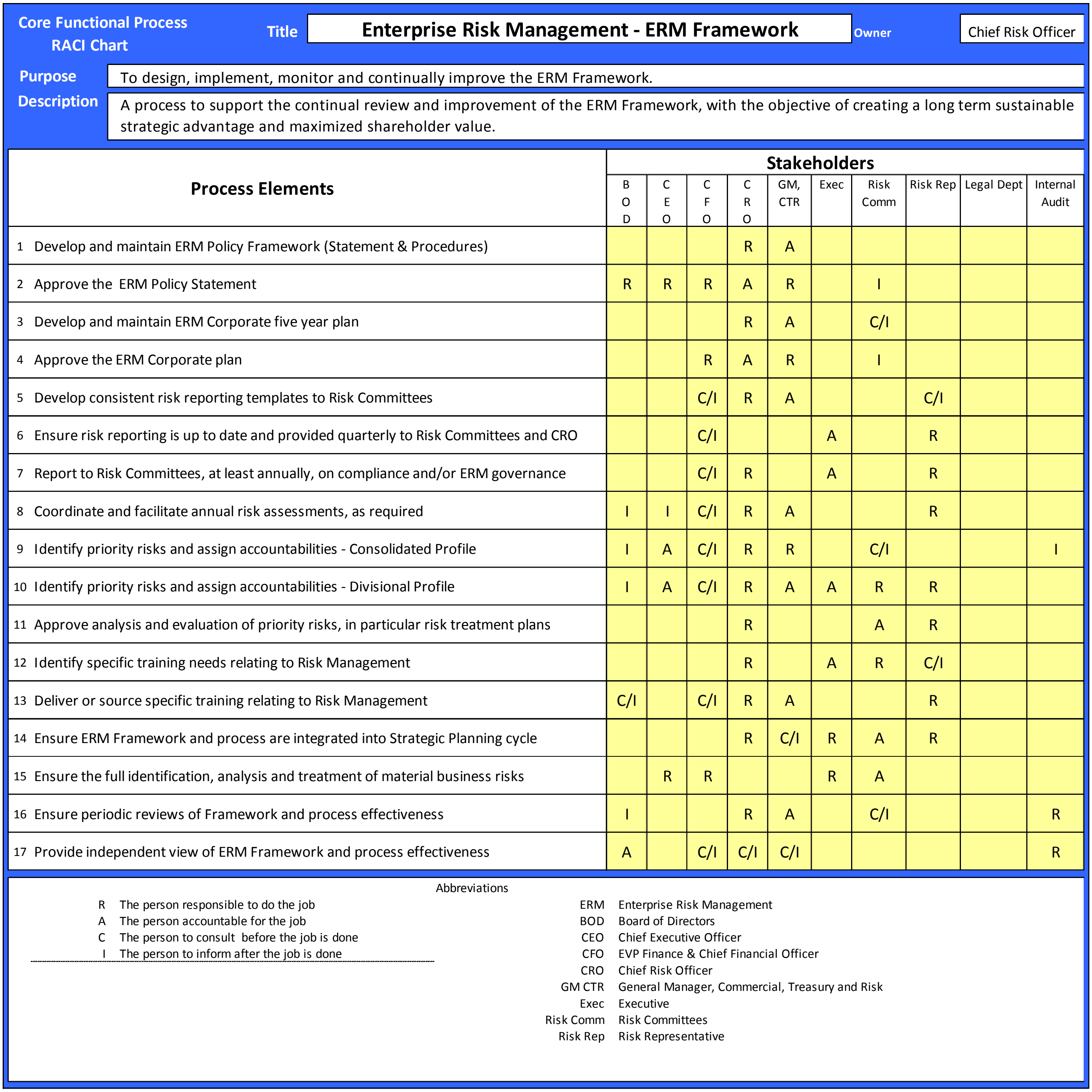
Risk owner – person or entity with the accountability and authority to manage a risk or delegate.

Risk philosophy – see risk appetite.

Risk source – element, which alone or in combination, has the intrinsic potential to give rise to uncertainty.

Risk treatment – often referred to as risk mitigation, it describes a process undertaken to modify a risk which can include avoiding the risk, accepting the risk to pursue opportunity, removing the risk source, changing the likelihood, changing the consequences, sharing or transferring the risk or retaining the risk by informed decision.

Appendix 1 – Enterprise Risk Management RACI Charts



Core Functional Process RACI Chart	Title: **Enterprise Risk Management - ERM Framework**	Owner	Chief Risk Officer
Purpose	To design, implement, monitor and continually improve the ERM Framework.		
Description	A process to support the continual review and improvement of the ERM Framework, with the objective of creating a long term sustainable strategic advantage and maximized shareholder value.		

	Process Elements	Stakeholders									
		BOD	CEO	CFO	CRO	GM, CTR	Exec	Risk Comm	Risk Rep	Legal Dept	Internal Audit
1	Develop and maintain ERM Policy Framework (Statement & Procedures)				R	A					
2	Approve the ERM Policy Statement	R	R	R	A	R		I			
3	Develop and maintain ERM Corporate five year plan				R	A		C/I			
4	Approve the ERM Corporate plan			R	A	R		I			
5	Develop consistent risk reporting templates to Risk Committees			C/I	R	A			C/I		
6	Ensure risk reporting is up to date and provided quarterly to Risk Committees and CRO			C/I			A		R		
7	Report to Risk Committees, at least annually, on compliance and/or ERM governance			C/I	R		A		R		
8	Coordinate and facilitate annual risk assessments, as required	I	I	C/I	R	A			R		
9	Identify priority risks and assign accountabilities - Consolidated Profile	I	A	C/I	R	R		C/I			I
10	Identify priority risks and assign accountabilities - Divisional Profile	I	A	C/I	R	A	A	R	R		
11	Approve analysis and evaluation of priority risks, in particular risk treatment plans				R			A	R		
12	Identify specific training needs relating to Risk Management				R		A	R	C/I		
13	Deliver or source specific training relating to Risk Management	C/I		C/I	R	A			R		
14	Ensure ERM Framework and process are integrated into Strategic Planning cycle				R	C/I	R	A	R		
15	Ensure the full identification, analysis and treatment of material business risks		R	R			R	A			
16	Ensure periodic reviews of Framework and process effectiveness	I			R	A		C/I			R
17	Provide independent view of ERM Framework and process effectiveness	A		C/I	C/I	C/I					R

Abbreviations

R	The person responsible to do the job
A	The person accountable for the job
C	The person to consult before the job is done
I	The person to inform after the job is done

ERM	Enterprise Risk Management
BOD	Board of Directors
CEO	Chief Executive Officer
CFO	EVP Finance & Chief Financial Officer
CRO	Chief Risk Officer
GM CTR	General Manager, Commercial, Treasury and Risk
Exec	Executive
Risk Comm	Risk Committees
Risk Rep	Risk Representative

Policy Title	**Enterprise Risk Management Policy**
Policy Group	ERM
Policy Number	ERM-01
Accountable Division	Risk & Insurance
Policy Owner	Chief Risk Officer

1. Policy Statement

Recognizing that the management of risk is critical to achieving corporate objectives and implementing internal control systems, Nalcor Energy ("Nalcor") has implemented an Enterprise Risk Management ("ERM") Framework to ensure that a timely, structured and systematic approach is used to manage key business risks.

2. Purpose

The purpose of this Policy is to outline the key components of Nalcor's ERM Framework ("the Framework"), including the infrastructure required to complete risk assessments, and to develop and document risk treatment plans. The Framework requires ongoing communication and consultation with key stakeholders, as well as monitoring and reviews of effectiveness, both of the Framework itself and also key management actions to manage priority risks.

3. Guiding Principles

Nalcor's Framework is underpinned by principles stating that risk management:

1. Creates and protects value
2. Is an integral part of all organizational processes
3. Is part of decision making
4. Explicitly addresses uncertainty
5. Is systematic, structured and timely
6. Is based on the best available information
7. Is tailored
8. Takes human and cultural factors into account
9. Is transparent and inclusive; and
10. Facilitates continual improvement of the organization.

4. Definitions and Terms[1]

Enterprise Risk Management ("ERM") – a group of coordinated activities designed to identify potential events that may affect the organization's objectives, and to manage related risks to be within the organization's risk appetite and tolerances.

ERM framework – set of components that provide the foundations for designing, implementing, monitoring, reviewing and continually improving risk management throughout an organization.

Risk – the effect of uncertainty on objectives.

[1] *The following definitions are adapted from a number of sources: (1) Committee of Sponsoring Organizations of the Treadway Commission (COSO), (2) Deloitte and Touche LLP and CAN/CSA-ISO 31000-10 as published by the National Standards of Canada.*

Risk appetite – the nature and amount of risk an organization is willing to take on in pursuing its goals. Forms the bounds within which management must operate the business.

Risk assessment – the overall process of risk identification, risk analysis and risk evaluation.

Risk management - the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate event(s) or to maximize the realization of opportunities.

Risk treatment – often referred to as risk mitigation, it describes a process undertaken to modify a risk which can include avoiding the risk, accepting the risk to pursue opportunity, removing the risk source, changing the likelihood, changing the consequences, sharing or transferring the risk or retaining the risk by informed decision.

5. Scope of Application

This policy applies to all divisions and lines of business within Nalcor Energy. With respect to the implementation of the framework, direction is set through Policy, and subsidiary companies and divisions submit annual risk & insurance plans to the Nalcor Energy Chief Risk Officer, who is responsible for monitoring compliance with the framework and assessing risk maturity.

6. Process/Procedure[2]

Subsidiary Companies and Divisions

The Risk & Insurance team maintains and administers the frameworks that focus on developing a consolidated view of risk, the individual divisions and lines of business are required to complete entity level risk assessments as part of the annual strategic planning process. This is captured in a template referred to as the Risk Register, and using the guidelines outlined in the ERM Toolset and Procedures. There will often be several component risks at a subsidiary or divisional level which are shown as a theme, or enterprise level risk when consolidated.

Subsidiary companies and divisions are expected to:

- Complete an annual risk assessment as part of completing annual plans
- Determine which risks linked to current operational, departmental and strategic plans are considered priority, and monitor the status of these risks at a divisional level on a quarterly basis
- Ensure that the management of critical business processes (i.e. those that manage a priority risk) include formal consideration of risk
- Ensure that review and monitoring activities are embedded in critical business processes, and that they embody a spirit of continuous improvement
- Support the implementation of ERM initiatives that are part of the framework implementation and are designed to improve risk management maturity. These activities are agreed upon in Risk & Insurance Plans annually
- Review ERM Policy, Framework and Procedures document and Toolset and provide feedback on opportunities for improvement as requested

The activities above are overseen by Risk Committees, which are established for

[2] *Adopted from CAN/CSA-ISO31000-10*

Newfoundland and Labrador Hydro and each division of Nalcor Energy. Membership is to be comprised of senior managers as agreed between the Committee Chair and Nalcor Energy Chief Risk Officer. Terms of Reference for each Committee to be reviewed and approved annually. The activities above are driven largely by Risk Representatives assigned by the President, Hydro and Nalcor Energy Executive Vice Presidents, in consultation with the Nalcor Energy Risk & Insurance team as required. Additional detail regarding the execution of these activities, the use of the Risk Register and other tools and templates can be found in the more detailed ERM Framework and Procedures document.

Consolidated Nalcor Energy Risk Management Activities

A risk framework provides another lens to assist management in allocating resources, prioritizing efforts, and aligning focus. Senior management in each subsidiary company or division apply the framework to manage the risks affecting their plans and initiatives. At a consolidated level Nalcor Energy includes multiple entities, divisions and lines of business with varied operations and activities. Providing direction on the consistent application of certain risk management principles and practices is necessary in order to create consolidated risk reporting, and includes the responsibility to:

- Review and approve Risk & Insurance plans, policies, procedures, templates and Toolsets
- Oversee the completion of annual risk assessments, and the establishment of risk appetite statements and tolerances
- Develop risk reporting templates to the Risk Committees and Boards of Directors, as required
- Oversee the implementation and consistent application of the framework within subsidiaries and divisions
- Monitor the status of risk treatment plans for priority risks at a consolidated Nalcor Energy level
- Ensure that review and monitoring activities take place within the framework as required, and that they embody a spirit of continuous improvement

The activities above are driven largely by the Risk & Insurance team in consultation with the Executive Vice President, Finance and CFO and other Executive as required. Additional detail regarding the execution of these activities and the use of the Risk Profile and Detailed Risk Treatment Plan templates can be found in the ERM Framework and Procedures document.

7. Responsibilities

High level roles and responsibilities

There are three broad stakeholder groups who must fulfill their roles in order for the ERM framework to be effective; front line staff and management, the Risk & Insurance department and independent overseers (i.e. Auditors and the Boards of Directors).

Front line staff and management

All staff have a responsibility to appropriately balance risk and opportunity within the activities that they operate, and to raise concerns where they are unsure this balance has been struck. Employees must understand their role with respect to processing transactions and are the ones who bring risk treatment (i.e. internal controls) to life. For additional guidance on management's role with respect to ensuring appropriate internal control systems within their entity or department, the Management Control Policy should be referenced.

Senior management has a responsibility to ensure the framework is embedded within each division. Newfoundland and Labrador Hydro and each Nalcor Energy division has a Risk Committee chaired by President, Hydro and divisional Executive Vice President, respectively. These Committees are supported by the Nalcor Energy Risk & Insurance department, Risk Representatives for each division and by members appointed to the Committee Chair in its Terms of Reference. The Risk Committees are established to monitor compliance with the requirements outlined in this Policy and to oversee the management of priority risks for each subsidiary or division.

Risk & Insurance department

The CRO and their department are responsible to:

- Oversee the annual risk assessment process for Nalcor Energy, in coordination with Strategic Planning, and review the risk assessments done across subsidiaries and divisions for conformance with procedures, standards and other requirements
- Provide a bi-annual consolidated Risk Report to the Nalcor Energy Board of Directors, via the Governance Committee
- Act as a resource to coach and educate staff impacted by implementation regarding the framework and its application, and provide training as required or requested
- Ensure Risk Committee meetings take place at least quarterly and that there is adequate representation and expertise present
- Review Policy and other guidance at least annually and consult with subsidiary and divisional Risk Committees where updates are recommended
- Facilitate risk assessment workshops as required or requested
- Monitor adherence to the ERM framework in subsidiaries and divisions
- Monitor risk treatment plans for Nalcor Energy priority risks
- Review and update Risk & Insurance Plans at least annually
- Monitor and report progress against Risk & Insurance plans as required

The Risk & Insurance department is positioned to provide independent validation of compliance with ERM Policy and plans, as well as to monitor objectively the status of priority risk treatment plans.

Boards of Directors

The respective Boards are charged with ensuring that executive management is effectively governing and managing the enterprise's risk environment. Additionally, they are responsible for ensuring that management has a process for identifying the principal risks of the Corporation's business and ensuring the implementation of appropriate systems to effectively monitor and manage such risks with a view to the long-term viability of the Corporation. This includes oversight of internal control, management information systems, and regulatory compliance processes.

Auditors

Internal auditors are responsible to report independently to the Board regarding the effectiveness of activities taken by management, as well as priority risk treatment plans and ERM framework and process.

Note regarding conflicting interests

The roles as outlined above support independent and objective quality assurance over the ERM framework and process application within the organization, and also with respect to the effectiveness of priority risk treatment plans.

As a general principle, independence and/or objectivity can be impaired where a function or individual is responsible for assessing the quality of their own work. It is important that the Risk & Insurance department is recognized as a source of assurance over the activities of front line staff and management. It is not appropriate for members of this department to make management decisions regarding risk appetite, tolerance or treatment, but they will often serve as advisors where these elements require development.

Similarly, internal auditors or external service providers give management and the Board assurance over the quality of the work done by the Risk & Insurance department.

It is important this design and these principles are upheld in order to not compromise the quality assurance which is built into the framework.

Nalcor Energy:
Risk Rating Guide

Operational Impact Matrix Defined in Terms of Company Goals							
			Business Excellence				
Impact	Safety	Environment	Financial[1]	Operational	Compliance	People	Community
Very High (5)	- Fatality or injury causing permanent disability	- Regulatory non-compliance resulting in shut down of all operations for extended period - Major impact of extended duration requiring full scale response - Damage will be evident for more than 10 years - Observed effect observed beyond 10 km radius from Nalcor property	- Very high financial impact	Reliability: Reliability generation up-time <83% - Deficient in reserves. Power Emergency – Notice provided to stakeholders of an Alert level 4. Customers requested to conserve electricity. Rotating outages in effect. Customer: A whole region is impacted (eg. Avalon Peninsula NP Customers) - An incident that occurs between December - February in NL or October - April in Labrador - Restoration time expected to exceed 36 hours, or rotating outages - A Loss of 2 units for >3 months during GWAC (CFLCo) Project/Work Execution: Deterioration in project/work execution schedule, scope or quality which affects numerous Nalcor goals and divisions and requires extraordinary effort and use of unplanned resources to manage Business/Service Continuity: Business or service interruption of key infrastructure/critical assets (including IT/OT) at multiple critical sites concurrently, or a suspension of all operations for any amount of time Business Process/Control: No ownership assigned/no plan in place to address a lack of enterprise level/process level capabilities to address a priority risk	- Charges laid resulting in fines/penalties > $100,000 or imprisonment - Shut down of all operations for extended period	Recruitment/Retention: Unable to recruit/retain critical leadership or other positions at critical locations Training & Development: Regulatory training requirements for critical positions are not met	Public Relations: National and international media coverage - Serious damage to public property that results in widespread hardship Stakeholder Management: An irreparable loss in stakeholder trust/commitment
High (4)	- Involving a lost time injury	- Regulatory non-compliance with stop work orders issued - Extended clean-up effort required - Damage will be evident for next 5-10 years - Observed effect within 10 km radius from Nalcor property	- High financial impact	Reliability: Reliability generation up-time of 83-87% - Available reserves 0 to 85 MW. Power Warning - Notice provided to stakeholders of an Alert level 3. Customers requested to conserve electricity. Rotating outages are likely. Customer: A remote island community or other NP urban area (Grand Falls, Gander, Corner Brook) is impacted - An incident that occurs between April - November in NL or May - September in Labrador - Restoration time expected to exceed 24 hours or rotating outages - A Loss of 1 unit for several months during GWAC (CFLCo) Project/Work Execution: Deterioration in project/work execution schedule, scope or quality which affects a single business unit/division and requires extraordinary effort and use of unplanned resources to manage Business/Service Continuity: Business or service interruption of key infrastructure/critical assets (including IT/OT) at a single critical location, for an extended time period or an incident that forces a suspension of certain operations for an extended period of time Business Process/Control: Low level of enterprise level/process level capabilities to address a priority risk, responses partially implemented or not achieving control objectives	- Formal investigation by external regulator with multiple directives received and/or penalties/fines > $50,000 - Stop work orders issued impacting multiple sites	Recruitment/Retention: Unable to recruit/retain management positions at multiple locations Training & Development: Competency requirements for critical positions/management are not met	Public Relations: Local and possibly national media coverage - Significant damage to public property that entails hardship in a localized area Stakeholder Management: A loss in stakeholder trust/commitment that is doubtful whether it can be rebuilt
Moderate (3)	- Injury leading to a medical treatment incident	- Regulatory non-compliance Identified by government inspector resulting in administrative penalty - Reportable with some clean-up measures - Temporary damage - Observed effect on/directly adjacent to Nalcor property (within 500m radius)	- Moderate financial impact	Reliability: Reliability generation up-time of 87-91% - Available reserves 85 to 170 MW. Power Watch - Notice provided to stakeholders of an Alert level 2. Customer request to conserve electricity is likely. Customer: An isolated Labrador community is impacted - An incident that occurs between November - March in NL or September - April in Labrador - Restoration time expected within 12-24 hours - A Loss of use of a unit for ~6 weeks during GWAC (CFLCo) Project/Work Execution: Deterioration in project/work execution schedule, scope or quality which affects a single business unit/division and requires significant effort to manage, including redeployment of existing resources Business/Service Continuity: Business or service interruption of infrastructure/assets (including IT/OT) at multiple non-critical locations or at a single critical location that causes a disruption in performance levels without suspending operations Business Process/Control: Moderate level of enterprise level/process level capabilities to address a priority risk, responses implemented and achieving objectives most of the time	- Formal investigation by external regulator with multiple directives received and/or penalties/fines > $25,000 - Stop work orders issued impacting single site	Recruitment/Retention: Unable to recruit/retain or retain employee positions at multiple locations Training & Development: No capacity for training or development across multiple lines of business	Public Relations: Local media coverage only - Damage to public property that causes inconvenience in a localized area Stakeholder Management: Some loss in stakeholder trust/commitment that will require a committed effort to rebuild
Low (2)	- Minor injury requiring first aid treatment	- Regulatory non-compliance addressed by internal improvement initiatives - Reportable with limited clean-up measures - Non-permanent damage - Observed effect on Nalcor property only	- Low financial impact	Reliability: Reliability generation up-time of 91-95% - Available reserves 170 to 240 MW. Power Advisory - Advance notice provided to Newfoundland Power of an Alert Level 1. Customer: An incident that occurs between May - October in NL or June - August in Labrador - Restoration time expected to occur within 8 hours - A Corrective maintenance requiring outages of a week or more during GWAC (CFLCo) Project/Work Execution: Deterioration in project/work execution schedule, scope or quality which affects a single business unit/division and can be managed with minor adjustments to existing resourcing and other plans Business/Service Continuity: Business or service interruption of non-critical infrastructure/assets or of critical infrastructure/assets which is restorable in a short period of time without disruption to performance levels Business Process/Control: Medium to high level of enterprise level/process level capabilities to address the risk, responses implemented and achieving objectives except in extreme conditions	- Externally identified non-compliance that requires action but has no associated financial fines or penalties - Regulatory non-compliance identified internally and requires disclosure to external regulator	Recruitment/Retention: Unable to recruit/retain or retain employee positions at a single geographic location Training & Development: No capacity for training or development across a single line of business	Public Relations: Some Unfavourable media attention - Some damage to public property that does not inconvenience the public Stakeholder Management: Some loss in stakeholder trust/commitment that is easily rebuilt
Very Low (1)	- Negligible injury, no absence from work	- No regulatory compliance concern - Not reportable with no clean-up measures - No observed effect on Nalcor property or adjacent properties	- Very low financial impact	Reliability: Reliability generation up-time of 95-100% - Available reserves are greater than 240 MW Customer: An incident that occurs between June - September in NL or July - August in Labrador - Restoration time expected to occur in under 4 hours - Operational events with no impact on GWAC (CFLCo) Project/Work Execution: Impact can be absorbed through normal activity Business/Service Continuity: Business or service interruption which is not noticed outside of operational area which monitors the system impacted (eg. IT Security/ECC) Business Process/Control: High enterprise/process level capabilities to address the risk, redundant response mechanisms in place and regularly tested for critical risks	- Regulatory non-compliance identified internally and does not require disclosure to external regulator - Non-compliance addressed by internal improvement initiatives	Recruitment/Retention: Vacancies at a non-critical location Training & Development: Capacity for training is limited across organization	Public Relations: Slight media attention. Little stakeholder impact - Insignificant damage to public property Stakeholder Management: Little or no loss in stakeholder trust/commitment

[1]Financial Impact Matrix

In $ millions	1 - Very Low		2 - Low		3 - Moderate		4 - High		5 - Very High	
	Lo	Hi	Lo	Hi	Lo	Hi	Lo	Hi	Lo	Hi
Nalcor Energy	0.0	1.0	1.0	10.0	10.0	40.0	40.0	70.0	70.0	Unlimited
Power Supply/Power Development	0.0	1.0	1.0	10.0	10.0	40.0	40.0	70.0	70.0	Unlimited
Newfoundland and Labrador Hydro - Regulated	0.0	0.3	0.3	3.0	3.0	10.0	10.0	20.0	20.0	Unlimited
Churchill Falls (Labrador) Corporation Ltd	0.0	0.3	0.3	3.0	3.0	8.0	8.0	13.0	13.0	Unlimited
Energy Marketing	0.0	0.1	0.1	1.0	1.0	1.5	1.5	2.5	2.5	Unlimited

	Low		Medium		High
Impact	Risk Score = (Impact Rating) x (Likelihood Rating)				
Very High (5)	5	10	15	20	25
High (4)	4	8	12	16	20
Moderate (3)	3	6	9	12	15
Low (2)	2	4	6	8	10
Very Low (1)	1	2	3	4	5

Likelihood				
Rare (1)	Low (2)	Possible (3)	Likely (4)	Almost Certain (5)
0.5-5%	5-20%	20-50%	50-90%	>90%
1 in 200 years	1 in 20 years	1 in 5 years	1 in 2 years	Will happen this year/is happening now
A freak occurrence of factors would be required for the impacts to result	A rare combination of factors would be required in order for the impacts to materialize	Could happen when additional factors are present, otherwise, unlikely to occur	Not certain, but an additional factor could result in the impacts detailed	Almost inevitable that risk will cause the impacts detailed