ONTARIO POWER GENERATION

Internal Use Only		
Document Number: OPG-PROG-0004		Revision R005
Usage Classification: Information	Sheet Number: N/A	Page: 1 of 12

Program

TITLE
ENTERPRISE RISK MANAGEMENT

AUTHORIZATION	
DOCUMENT OWNER:	A. Chiarandini Director, Enterprise Risk Management
AUTHORIZATION AUTHORITY:	L. Kim VP, Chief Risk and Audit Executive

DOCUMENT RELATIONSHIP	
Applicability:	Assurance & Enterprise Risk Management
Receives Authority from:	OPG-POL-0004, Enterprise Risk Management Policy

Document is Related to Pressure Boundary ☐	Document Requires CNSC Notification ☐

PURPOSE
The purpose of this program document is to define the requirements for risk management at OPG.

DATES (YYYY-MM-DD)	
PDF Creation Date:	2020-07-16
Compliance Date:	January 1, 2021

EXCEPTIONS

© Ontario Power Generation Inc., 2020. This document has been produced and distributed for Ontario Power Generation Inc. purposes only. No part of this document may be reproduced, published, converted, or stored in any data retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without the prior written permission of Ontario Power Generation Inc.

TABLE OF CONTENTS

Page

1.0 DIRECTION 3
1.1.1 Role of Enterprise Risk Management 3
1.1.2 Risk Appetite and Tolerance 3
1.1.3 Alignment with Corporate Objectives 3
1.1.4 Opportunities 4
1.2 Risk Management Process 4
1.2.1 Organizational Levels For Risk Management 5
1.2.2 Risk Identification 5
1.2.3 Risk Treatment 6
1.2.4 Risk Registers 6
1.2.5 Project Risk Management 6
1.3 Risk Oversight 6

2.0 ROLES AND ACCOUNTABILITIES 6
2.1 Management Committees 6
2.2 Executive Risk Committee 7
2.3 Management (including Risk Owners) 7
2.4 Enterprise Risk Management Team 8

3.0 DEFINITIONS AND ACRONYMS 8
3.1 Definitions 8
3.2 Abbreviations and Acronyms 9

4.0 BASES, RECORDS AND REFERENCES 9
4.1 Bases 9
4.2 References 10
4.2.1 Performance References 10
4.2.2 Developmental References 10

5.0 REVISION SUMMARY 10
Appendix A: Enterprise Risk Management Governance 11
Appendix B: Risk Tolerance Guidance 12

1.0 DIRECTION

As stated in OPG-POL-0004, Enterprise Risk Management Policy, OPG is committed to managing risks and pursuing opportunities to achieve its strategic and business plan objectives. The purpose of this program document is to define the requirements for risk management at OPG.

1.1.1 Role of Enterprise Risk Management

OPG's Enterprise Risk Management program is based on ISO 31000:2018.

The ERM team leads OPG's risk management process and performs a risk oversight role across business units and projects to ensure that leading practices are incorporated into the process.

The ERM team facilitates ongoing and quarterly reviews of risks and reports enterprise risks to management, ERC and the Audit & Risk Committee of the Board of Directors. The process includes identification of any risks exceeding the established risk tolerance levels (where KRIs have been developed).

The relevant governance relating to ERM is contained in Appendix A.

1.1.2 Risk Appetite and Tolerance

Per OPG-POL-0004, Enterprise Risk Management Policy, OPG will define risk appetite, risk tolerance and key risk indicators for specific top risks at the discretion of the ERC. These serve as a guideline for risk-informed decision making. BU Leadership shall ensure that risk management throughout the organization is aligned with these principles.

For each risk with defined KRIs, risk tolerance thresholds will be set with risk owners and SMEs to establish risk capacity, risk tolerance limits and risk tolerance triggers. Refer to the Risk Tolerance Guidance in Appendix B. The risk tolerance thresholds will be presented to the ERC for their concurrence. For other enterprise risks, risk tolerance will be based on discussion and input from the ERC.

In the development of KRIs, risk owners and SMEs should consider metrics that measure root causes, the effectiveness of mitigation plans, existing metrics that are being tracked by the BU, as well as established industry standard metrics. Risk tolerance thresholds should be established with consideration given to the defined risk appetite level to ensure thresholds are set relative to the risk appetite.

1.1.3 Alignment with Corporate Objectives

To ensure that there is alignment between risk management and OPG's objectives, all risks are tied to one of OPG's four strategic objectives (People Powering the Future, Value Through Innovation and Efficiency, Putting Customers and Communities First and Energy Industry Leader) and business imperatives (Operational Excellence, Project Excellence, Financial Strength and Social Licence).

Enterprise risks are uncertain events that may impact the achievement of OPG's objectives. These risks include strategic, operational and project risks and risks identified as part of the business planning process.

1.1.4 Opportunities

Opportunities (positive risks) associated with new initiatives or business changes that potentially enhance value should be identified as part of the business planning process to ensure risk-informed decision making is integrated into business planning and appropriate plans are in place to manage uncertainty over the business plan period.

1.2 Risk Management Process

The following diagram illustrates the risk management framework at OPG:

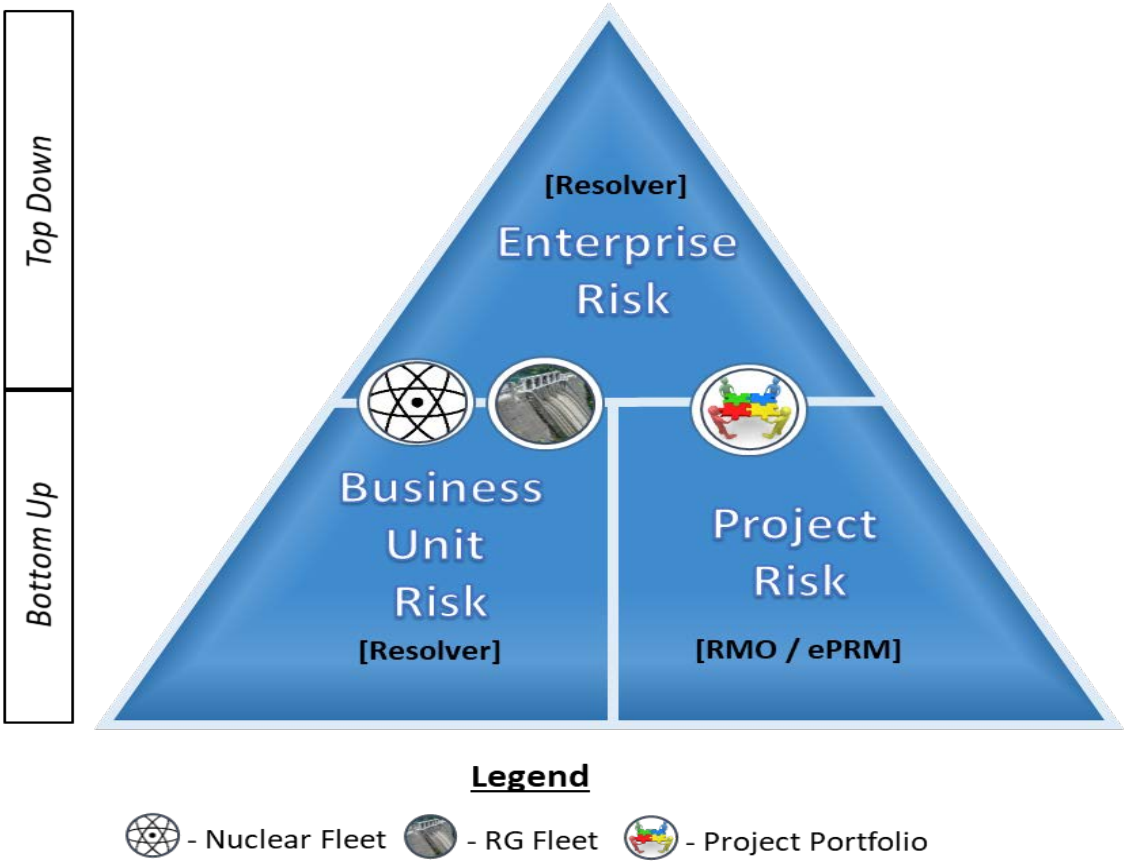


Figure 1: Risk Management Framework

As per Figure 1, OPG will manage risks at all levels of the organization. Business Units and Projects will identify risks that will impact their specific BU and project objectives. At the fleet

and project portfolio level respectively, risk will be considered from a broader strategic perspective while taking into account any significant risks identified by the various business units / projects. At the enterprise level, ERM will take into consideration all significant risks identified at the BU, project and fleet level and support management in the determination of top risks to OPG that may impact the strategic or business plan objectives.

1.2.1 Organizational Levels For Risk Management

Business Unit: Risks will be identified and assessed based on the BU's specific business objectives. Each business unit can define its own unique risk criteria, with oversight from ERM, but must apply it consistently within each risk register. Executive Leadership may use its discretion to decide whether to maintain a single risk register for the entire BU or various risk registers for individual divisions / departments. BUs have the discretion to flag or escalate significant risks determined through their assessment as potential enterprise risks.

Nuclear / Renewable Generation (RG) Fleet: Risks will be identified and assessed by NEC and RGET respectively, with a focus on the integration of strategic, fleet-wide and significant risks as determined by the various sites either individually or in aggregate, using criteria aligned with the ERM assessment criteria. Leadership may escalate risks to the enterprise level, either based on specific criteria, or by management judgement.

Project: Risks will be identified and assessed in accordance with OPG-MAN-00120-0015, Project Risk Management, which is aligned with the principles and methodology of OPG's Enterprise Risk Management program.

Project Portfolio: Risks will be identified and assessed by the EPO and Portfolio Manager at the portfolio level in accordance with OPG-MAN-00120-0009, Project Portfolio Management. The project portfolio risk criteria aligns to the ERM assessment criteria, principles and methodology of OPG's Enterprise Risk Management program. The EPO and Portfolio Manager will consider the results of risks assessed at the project level either in aggregate or on an individual risk basis should such risks be assessed as significant.

Enterprise: Risks will be identified and assessed at the enterprise level using a top down approach using ERM assessment criteria. ERM will work with the businesses to determine the top risks to OPG by considering assessment results of risks assessed by Nuclear Fleet, Renewable Generation Fleet, Project Portfolio and Corporate BUs.

Subsidiary: Subsidiaries are not required to utilize OPG's ERM procedures and tools, but must establish an effective risk management program. At a minimum, the risk management program must identify, assess, treat and monitor the top risks to their business objectives and report them to their executive and board. Any material risks that could affect OPG shall be communicated to OPG's ERM team to ensure a consolidated view of risks for ERC and ARC reporting.

1.2.2 Risk Identification

Risks shall be identified against business objectives. As part of risk identification, the hazards, as defined in the Ontario Hazard Identification and Risk Assessment Report issued

by the Office of the Fire Marshal & Emergency Management,[1] should be considered as potential risk areas.

1.2.3 Risk Treatment

Once risks have been identified and assessed, an appropriate risk treatment plan should be developed with consideration to the cost-benefit of such risk treatment. Options include avoiding, transferring / sharing, mitigating / reducing, or accepting the risk. For risks where OPG has established a low risk appetite, avoiding and mitigating should prevail. Remediation or contingency plans should be developed as required to reduce the impact of the risk.

1.2.4 Risk Registers

Risks should be documented in a systematic format (referred to as a risk register), which are maintained at the following organizational levels:

a) Enterprise risks in the Resolver risk database maintained by ERM;
b) BU risk registers (including operational and key process risks) in the Resolver risk database maintained by the BU; and
c) Project risk registers in the RMO/ePRM risk database maintained by EPO.

1.2.5 Project Risk Management

Project risk management is an integral part of OPG projects, and will follow OPG-POL-0004 Enterprise Risk Management Policy and industry accepted practices. Risk Management requirements shall follow the scalable project delivery model requirements as defined by OPG-PROG-0039 and OPG-MAN-00120-0015.

1.3 Risk Oversight

The top risks and associated risk management strategies will be systematically monitored, evaluated and updated. The ERM team shall review all enterprise risks with the Executive Risk Committee on a quarterly basis and report results to the Audit & Risk Committee of the Board of Directors.

2.0 ROLES AND ACCOUNTABILITIES

2.1 Management Committees

Management shall establish controls to ensure the risk management process is implemented and executed, and risks are monitored from identification to closure (i.e. when a risk is mitigated). Risk treatment strategies should be monitored for effectiveness and cost efficiency.

The following table summarizes the management committees that provide risk management oversight as part of their mandate.

[1] https://www.emergencymanagementontario.ca/english/emcommunity/ProvincialPrograms/HIRA/Report/Intro.html

Management Committee	Risk Responsibility
Executive Risk Committee (ERC)	Provides oversight of the Enterprise Risk Management program and enterprise risks
Nuclear Executive Committee (NEC)	Provides risk oversight of the nuclear business: nuclear safety, operations and major projects.
Renewable Generation Executive Team (RGET)	Provides risk oversight of RG's business: renewable generation safety, operations and major projects.
Transactional Risk Approval Committee (TRAC)	Provides risk oversight of financial and operational transaction activities carried out by BUs, including but not limited to: Energy Markets and Treasury.

2.2 Executive Risk Committee

As part of managing the business, the ERC is responsible for:

(a) Providing direction on the corporate risk appetite;

(b) Maintaining BU risk tolerances and limits consistent with the corporate risk appetite;

(c) Managing risks;

(d) Ensuring that risk management processes within their areas of accountability are developed and applied;

(e) Disclosing risks and reporting risk management information and compliance violations to the CRAE;

(f) For enterprise risks, assigning a risk owner to monitor risk status, risk treatment effectiveness, and report quarterly to ERM; and

(g) Provides oversight and direction to ERM activities and processes.

2.3 Management (including Risk Owners)

All management is responsible for:

(a) Identifying, assessing, prioritizing, treating and monitoring risks on a day-to-day basis in their span of control;

(b) Communicating significant risks (including emerging risks) to senior management and the ERM team; and

(c) Ensuring staff are familiar with corporate requirements for risk management.

2.4 Enterprise Risk Management Team

The ERM Team is responsible for:

(a) Acting as OPG's Risk Management Centre of Excellence, by providing guidance on risk management methodology, benchmarking and leading practices.

(b) Overseeing, developing, implementing, optimizing and maintaining the corporate risk governance and ERM process, based on leading practices and feedback, to manage risks in a consistent, coherent manner across the company;

(c) Developing tools to assist BUs in identifying, assessing, managing, monitoring and reporting on risk and risk strategies;

(d) Facilitating risk discussions in key initiatives such as strategic and business planning, entry into new markets and other strategic initiatives

(e) Scanning for changes in the business environment (i.e. regulatory changes, new markets, assets, strategies, etc.) that could impact the corporate risk profile; and

(f) Preparing and reviewing the consolidated risk report, for presentation to the Executive Risk Committee and the Audit & Risk Committee of the Board of Directors.

3.0 DEFINITIONS AND ACRONYMS

3.1 Definitions

Hazard: A risk event with a potential for harm to persons, property, or the environment.

Inherent Risk: The risk that exists without giving consideration to risk treatment plans in place.

Major Project: Encompasses projects requiring CEO and Board of Director approval as per the OPG's OAR. Projects not requiring CEO and Board of Director approval may be deemed major at the discretion of the BU Leadership.

Objective: A favourable or advantageous goal an organization or project team is working to achieve. Business or project objectives are generally considered to be short term goals (i.e. within the business planning time horizon). Strategic objectives are generally considered to be longer term goals.

Remediation: Activities or actions taken to reduce the impact of the risk if the risk treatment activities are ineffective and the risk occurs or changes significantly. Remediation plans are also referred to as "contingency" plans.

Residual Risk: The risk that remains after taking into consideration status of implementation of the risk treatment plan.

Risk: An uncertain event that has the potential to affect the achievement of objectives. The effect can be positive or negative. Risks with a positive effect are typically referred to as opportunities.

Risk Appetite: The amount of risk an entity is willing to accept or retain in order to achieve its strategic objectives and business imperatives. It is a statement or series of statements that describes the entity's philosophy towards risk-taking. It requires board approval.

Risk Capacity: The maximum level of risk an entity is willing to take to meet its goals.

Risk Owner: The person with the accountability and authority to manage a risk.

Risk Register: Database of risk information, which includes, but are not limited to, risk description, root causes, impacts, risk treatments and risk owner.

Risk Tolerance: The levels of risk-taking acceptable to achieve a specific objective or manage a risk, based on operational and/or financial capacity. Risk tolerance represents the practical application of risk appetite.

Risk tolerance limit: The level of risk which, if breached, would necessitate immediate escalation to risk owner and ERC for corrective action.

Risk tolerance trigger: The level at which escalation occurs as a result of a risk being sufficiently close to the risk tolerance limit that corrective action is considered.

Risk Treatment: The actions taken to address the risk or opportunity.

3.2 Abbreviations and Acronyms

BU	Business Unit
CRAE	Chief Risk and Audit Executive
ELT	Executive Leadership Team
EPO	Executive Project Office
ERC	Executive Risk Committee
ERM	Enterprise Risk Management
NEC	Nuclear Executive Committee
OAR	Organizational Authority Register
OPG	Ontario Power Generation
RGET	Renewable Generation Executive Team
RMO	Risk Management Oversight Tool

4.0 BASES, RECORDS AND REFERENCES

4.1 Bases

- ISO 31000:2018.

4.2 References

4.2.1 Performance References

- OPG-MAN-00120-0009, Project Portfolio Management.
- OPG-MAN-00120-0015, Project Risk Management.
- OPG-PROG-0039, Project Management.
- OPG-POL-0004, Enterprise Risk Management Policy.
- OPG-POL-0023, Management Systems Policy.
- OPG-PROC-0094, Enterprise Risk Management Reporting Procedure.
- OPG-PROG-0016, Credit and Market Risk Management Program.

4.2.2 Developmental References

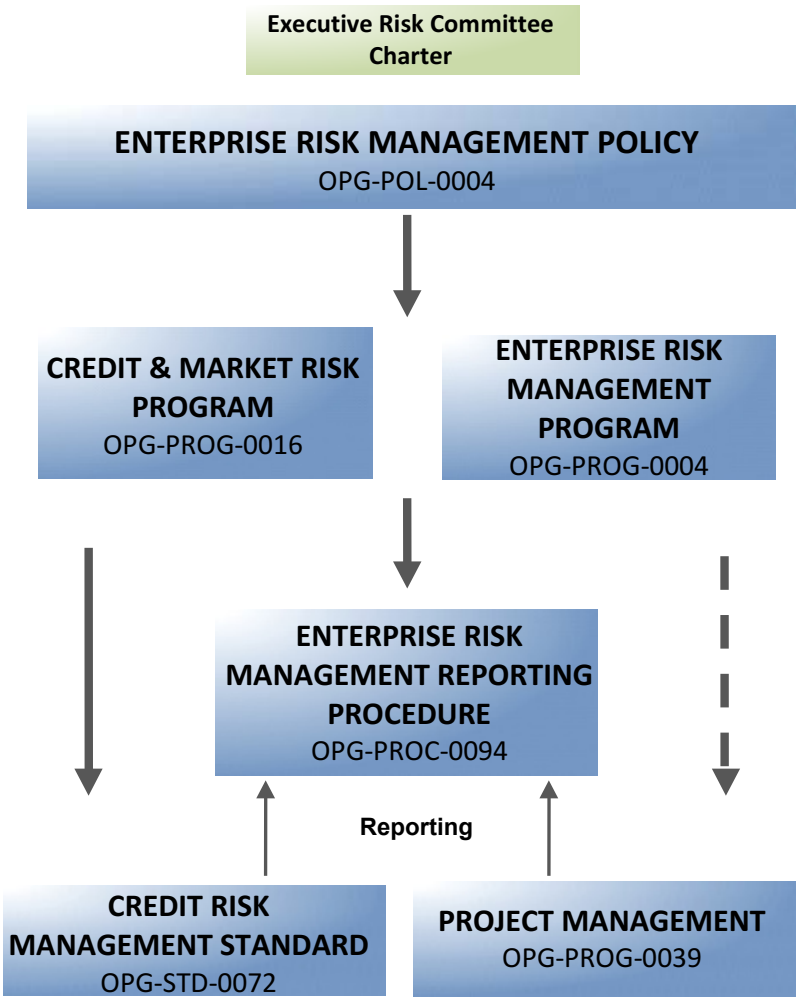
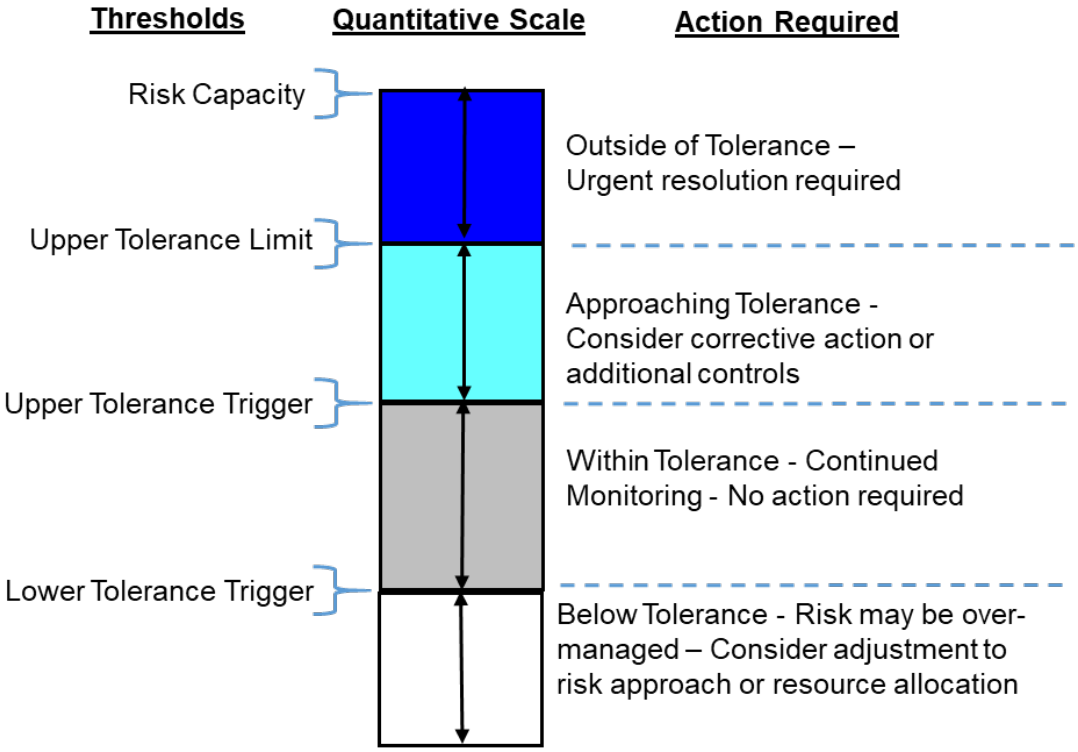
- Audit & Risk Committee Charter.
- Nuclear Risk Committee Charter.
- RG Risk Committee Charter.
- Executive Risk Committee Charter.

5.0 REVISION SUMMARY

This is an **intent** revision.

- Refined and clarified program requirements consistent with new ERM framework
- Removed reference to specific guidelines for risk appetite and risk tolerance
- Removed all references to strategic risks
- Removed hazard list in Appendix B and replaced with reference to list in body of Program
- Removed responsible parties and storage locations of contract risk registers
- Updated Roles & Accountabilities to better align to ERM Policy
- Added risk tolerance guidance

Appendix A:
Enterprise Risk Management Governance



Appendix B:
Risk Tolerance Guidance