ONTARIO POWER GENERATION

Internal Use Only		
Document Number: OPG-PROC-0094		Revision R005
Usage Classification: Information	Sheet Number: N/A	Page: 1 of 16

Procedure

TITLE
ENTERPRISE RISK MANAGEMENT REPORTING

AUTHORIZATION	
SINGLE POINT OF CONTACT:	A. De Angelis Senior Manager, Enterprise Risk Management
DOCUMENT OWNER:	A. Chiarandini Director, Enterprise Risk Management

DOCUMENT RELATIONSHIP	
Applicability:	OPG Wide
Receives Authority from:	OPG-PROG-0004, Enterprise Risk Management Program

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

PURPOSE
This procedure is established to ensure that enterprise risks are identified, assessed, treated, and reported consistently and regularly based on a standard process.

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

EXCEPTIONS
None

© 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 4

2.0 ENTERPRISE RISK MANAGEMENT PROCESS 4

2.1 Risk Registers 5
2.2 Risk Identification 5
2.2.1 Risk Classification 5
2.2.2 Risk Definition 5
2.2.3 Risk Status 6
2.2.4 New Risks 6
2.3 Risk Assessment 6
2.3.1 Risk Scenario 7
2.3.2 Risk Validation 7
2.4 Risk Treatment Plan 7
2.5 Risk Monitoring & Reporting 8
2.5.1 Risk Monitoring 8
2.5.2 Risk Reporting 8
2.6 Business Unit and Project Risk Updates 9

3.0 ROLES AND ACCOUNTABILITIES 9

3.1 Business Unit Leadership 9
3.2 Enterprise Risk Management Team 9
3.3 Risk Owners 10
3.4 Subject Matter Experts 10
3.5 Risk SPOC 10

4.0 DEFINITIONS AND ACRONYMS 10

4.1 Definitions 10
4.2 Abbreviations and Acronyms 12

5.0 BASES, RECORDS AND REFERENCES 12

5.1 Bases 12
5.2 Records 12
5.3 References 12
5.3.1 Performance References 12
5.3.2 Developmental References 12

6.0 REVISION SUMMARY 13

Appendix A: Risk Rating Criteria 14
Appendix B: Bow Tie Model 16

1.0 DIRECTION

Enterprise Risk Management (ERM) is an integral part of Ontario Power Generation's (OPG) management system as described in OPG-PROG-0004, Enterprise Risk Management Program. Based on ISO 31000:2018, the ERM process provides a standardized approach throughout the organization for risk identification, assessment, prioritization, treatment, monitoring and reporting. To support risk-informed decision making, other factors such as cost of risk treatment are also considered during the process. The ERM process focuses on enterprise risks, which are risks that have the greatest potential to affect achievement of business imperatives and strategic objectives at the enterprise level.

2.0 ENTERPRISE RISK MANAGEMENT PROCESS

The ERM process is continuous in nature. All BUs are required to identify, assess, treat, monitor and report risks that may affect the BU's ability to achieve its objectives. BU risks shall be used as input into identifying risks related to the Business Planning process which typically starts in Quarter 2. BUs shall incorporate the cost of risk treatment plans as part of the budgeting process for Business Planning to ensure appropriate resources are available to manage the risks.

An overview of the ERM process is provided below and details on each step of the process are contained within the following subsections.

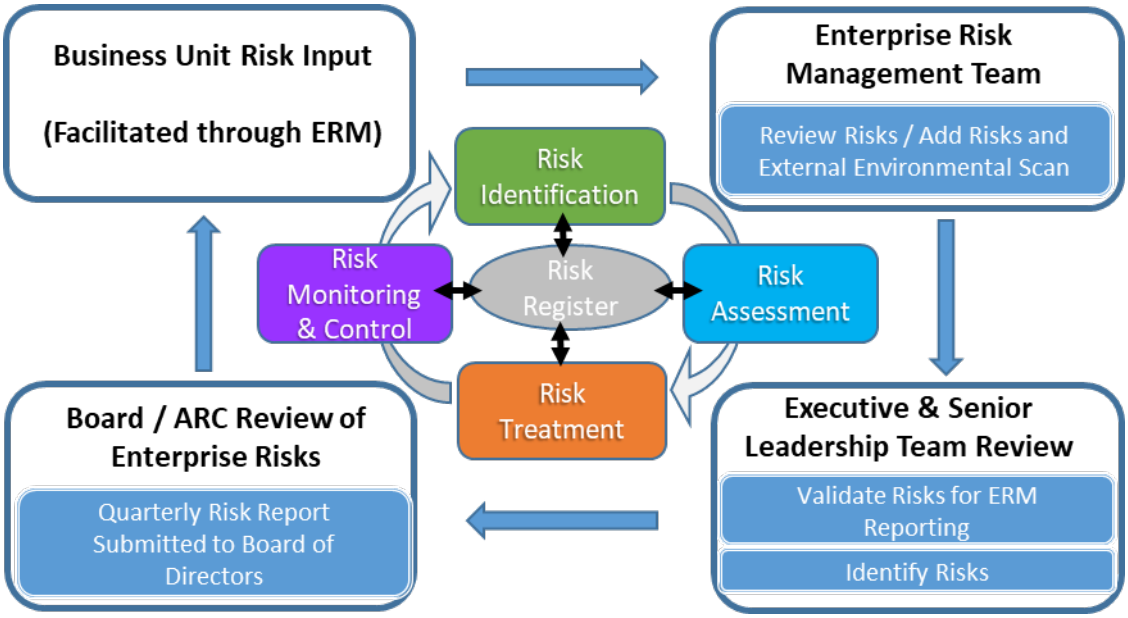


Figure 1: Enterprise Risk Management Process

2.1 Risk Registers

The following tools should be used as risk registers to identify, document and retain risk information.

Risk Level	Tool	Input / Update By:
Enterprise	Resolver	Enterprise Risk Management
Business Unit	Resolver	Risk SPOCs / Champions
Project	RMO / ePRM	Project Management Team

2.2 Risk Identification

The objective of risk identification is to ensure that all potential risks are identified, categorized and documented within a risk register. The following provides guidance on how to identify risks that may affect the achievement of applicable objectives (i.e. strategic objectives, business plan objectives, project objectives) whether they are enterprise risks, BU risks or project risks.

2.2.1 Risk Classification

Risks should be categorized as one of OPG's four business imperatives: Operational Excellence, Project Excellence, Financial Strength or Social License.

Risks should be categorized as either an Enterprise risk or a Business Unit risk to ensure they are captured in the correct risk register.

Risks that are to be escalated to ERM should be mapped to an enterprise risk using the cross reference ID field in Resolver. There may be multiple BU risks mapped to a single enterprise risk. In cases where there may be multiple enterprise risks that are applicable to a BU risk, the SME / SPOC should work with the Risk Owner and ERM to identify the most appropriate enterprise risk to map to, based on the relevance the BU risk will have on that enterprise risk.

If there is not an appropriate enterprise risk applicable to the BU risk then it should be categorized in the 'other' category pending ERM concurrence. ERM will determine if a new enterprise risk should be created. For projects, risks at the project portfolio or program level may be escalated to enterprise risks if it meets the threshold for an enterprise risk, or warrants escalation, as determined by leadership.

2.2.2 Risk Definition

OPG utilizes the bowtie model for defining the various components of a risk - refer to Appendix B. Each risk should be articulated as an event (i.e. "X may happen") and should include the following information in the risk register:

(a) Risk Name: A short description of the risk that may be used for reporting. The risk name should be self-explanatory and clearly depict the risk event. For example, Cyber / Information Security.

(b) Risk Definition: X may happen; e.g. Sensitive information may be leaked.

(c) Risk Description/ Context: The context should provide further details about the risk. It should include:

i. Summary description of the risk event;

ii. Relevant additional information (e.g. timeframe the risk is expected to be realized); and

iii. Any assumptions made regarding the risk. Discussions should be held with the ERM team to identify what risks may occur if the assumption is not realized.

(d) Root cause(s) of the risk;

(e) Potential impact if risk were to occur, including Public and Employee Safety, Financial, Reputational and Operational (as applicable);

(f) Business unit;

(g) Risk owner(s);

(h) SPOC(s); and

(i) Subject Matter Expert(s);

2.2.3 Risk Status

Each risk should be defined as new, active or inactive. Based on updates, risks may be recommended for closure due to the risk being averted, being reassessed as no longer having the potential to impact OPG's objectives, or if the risk event has occurred (i.e. risk has been realized and remediation plan in place).

2.2.4 New Risks

If a new risk is identified, the Risk SPOC should create a new risk in Resolver and complete the required fields as described in section 2.2. The ERM team will review the new risk with the SPOC to determine if it should be considered as an enterprise risk.

2.3 Risk Assessment

Each risk should be assessed on a residual risk basis (consider the effect that controls have on the risk) based on the likelihood of occurrence and impact. Enterprise assessment criteria is defined in Appendix A and project or business unit risks may be assessed using a scale that is more applicable (relative to the size). Risks must be assessed quarterly on a residual basis based on existing controls in place. Risks may be assessed on a post-risk treatment plan

residual basis as well (e.g. the expected residual risk level after the execution of all planned implementations).

For enterprise risks, impacts for Public and Employee Safety, Financial, Reputational and Operational should be considered during the assessment in order to ensure a consistency and ranking of risks within and across BUs. The impact assessment score will be based on the highest score across the different impact considerations. The rationale supporting the assessment should be documented.

2.3.1 Risk Scenario

In completing a risk assessment, it should be noted that a risk event may materialize in different ways and can have differing degrees of impact. As such, there can be a range of possible impacts that can result if a risk event occurs and each set of impacts will have its own likelihood. The assessment should focus on the risk impact most relevant to the objectives to ensure the most appropriate utilization of resources. The likelihood assessment of the risk should relate directly to the selected impact. This information should be documented under “assumptions” or “assessment rationale”.

Additionally, it may be pertinent to consider the worst case risk outcome that is plausible. The worst case risk scenario should be discussed with the ERM team to determine whether it should be classified as a black swan event.

2.3.2 Risk Validation

On a quarterly basis, the ERM team will review and challenge all existing enterprise risks and any new risks that have been flagged for enterprise risk consideration through discussions with the business unit. The ERM team will also conduct sessions with members of the senior and executive leadership team to validate the risk updates. The purpose of this review is to ensure that the risks have been adequately documented and assessed, and that there is alignment with BU leadership.

2.4 Risk Treatment Plan

Each Risk Treatment Plan (RTP) should address a root cause or an impact of the risk and represent the actions taken by OPG to prevent the risk from occurring or to reduce the impact if the risk occurs. There are several responses on how to treat a risk: mitigate, transfer, avoid or accept the risk. As applicable, details should be provided on:

(a) Risk treatment type;

(b) Specific actions to be taken to address the risk;

(c) Action owner(s);

(d) Timeframe(s) within which the risk treatment plan is targeted for implementation;

(e) Any assumptions underlying the treatment;

(f) Rationale supporting assessment and treatment options;

(g) The definition of any secondary risks that may arise due to risk treatment; and

(h) Status of implementation of the risk treatment plan.

A remediation plan to minimize the impact of the risk should be documented and would be executed if the risk were to occur. This includes:

(a) Outline the actions which will be taken if the risk treatment plan is ineffective, the risk event occurs or the risk changes significantly.

(b) Identify risk triggers and should also reference applicable emergency or continuity plans;

(c) Identify action owners; and

(d) List any assumptions underlying remediation.

It should be noted, however, that once a risk has occurred, mitigating action plans to minimize the impact are limited.

2.5 Risk Monitoring & Reporting

Risk monitoring activities should be documented for risks where applicable. Enterprise risks will be reported to the ERC and ARC on a quarterly basis.

2.5.1 Risk Monitoring

It is expected that risks will be monitored, at a minimum, as part of the quarterly risk review process. In addition, the risk owner should determine and document any additional methods to monitor the risk including:

(a) Risk monitoring activities (e.g. data analytics, external environmental scans, OPEX reviews);

(b) Specific early warning signals (events, trends, developments), metrics (including key risk indicators), risk triggers, etc. that will be monitored;

(c) Frequency of risk monitoring activities; and

(d) Timeframe(s) within which the risk monitoring activities will be conducted.

2.5.2 Risk Reporting

The ERM team will review the information input into Resolver against the requirements described in this procedure, including a periodic review of risk treatment plans to ensure effective management of top risks to the organization. The ERM team summarizes the results in a consolidated risk report for submission to the appropriate management and board committees and identifies which risks should be presented to the ERC for final validation. New risks identified by the BU or project teams as potential new enterprise risks would be assessed by the ERC.

The ERM team finalizes the consolidated risk report based on comments received from the ERC and provides a quarterly submission to the ARC of the Board of Directors. The submission includes a heat map of enterprise risks, description of enterprise risks, risk treatment plans related to extreme and high rated risks as well as relevant external events

which could have implications for OPG. Black swans, defined as high impact events with remote likelihood of occurrence, will be presented to the ERC and ARC of the Board of Directors on an annual basis. The information included in the report is to support risk-informed decision making.

2.6 Business Unit and Project Risk Updates

All BUs are required to identify, assess and document risks following the guidance provided in Section 2.2 of this document. As part of this activity, hazards referenced in OPG-PROG-0004 shall be considered as potential risk factors.

Projects should identify, assess and manage risks as per the guidance provided in OPG-MAN-00120-0015.

The Risk SPOC is responsible for inputting or updating risks within the risk register. If a risk is partially or fully realized, the SPOC should raise this to the ERM team. SMEs should be consulted as required for risk updates. The risk owner is responsible for final review and approval of their risks.

BUs and project management teams are required to flag any risks that could have implications at the enterprise level. At a minimum, any BU risk that is assessed on a residual risk basis as:

(a) High; or

(b) Medium <u>and</u> has a financial impact of $25M or greater

should be flagged for consideration as an enterprise risk after discussions are held with the risk owner. Other risks may be flagged for consideration as an enterprise risk at the discretion of the risk owner.

3.0 ROLES AND ACCOUNTABILITIES

3.1 Business Unit Leadership

(a) Ensuring that quarterly risk assessment updates are completed;

(b) Ensuring that risks are appropriately documented in risk register(s); and

(c) Assigning Risk SPOC(s) for their business unit and SME(s) for specific risk(s).

3.2 Enterprise Risk Management Team

(a) Consolidating, challenging, and trending enterprise risks across the company;

(b) Ensuring risk treatment plans are monitored, with any significant gaps in implementation identified and brought to the attention of the risk owner;

(c) Participating in risk-related management meetings;

(d) Reviewing and providing input on risks and risk treatment strategies;

(e) Meeting with risk owners or SMEs, as required;

(f) Consolidating risk updates and risks; and

(g) Ensuring Resolver meets governance requirements, knowledgeable administrators are in place, and the system is working as intended.

3.3 Risk Owners

(a) Identifying and characterizing new risks;

(b) Reviewing their risk(s) at least quarterly, and updating as required to ensure their risk(s) are correctly characterized and assessed;

(c) Implementing risk treatment plan(s) and remediation plan(s) as required;

(d) Monitoring risk(s) and risk treatment plan(s);

(e) Ensuring risks are communicated to the appropriate stakeholders in the organization; and

(f) Flagging BU risks for consideration as enterprise risks.

3.4 Subject Matter Experts

(a) Assisting the risk owner in assessing, monitoring and reporting on the risk, as required; and

(b) Maintaining knowledge of the risk.

3.5 Risk SPOC

(a) Inputting new risks(s) and/or making changes to existing risk(s) within Resolver, as per direction from the risk owner or SME;

(b) Ensuring that any changes to the ERM reporting process are communicated to and implemented by the BU;

(c) Notifying the ERM team of changes to Risk SPOC(s) and Resolver users; and

(d) Attending periodic training on risk management.

4.0 DEFINITIONS AND ACRONYMS

4.1 Definitions

Accept: An action associated with acknowledging the potential impact of a risk when mitigation is either impossible, not cost effective, or resources are better directed to other higher profile risks.

Active: An ongoing risk that has been vetted by the ERM group and the business.

Avoid: An action associated with a risk treatment plan that involves removing the risk source and/or eliminating the activity that creates exposure to the risk.

Black Swan: A risk event with potentially catastrophic impact and remote likelihood of occurrence.

Business Unit Risk: A risk that has the potential to affect achievement of business unit objectives.

Enterprise Risk: A risk that has the potential to affect achievement of OPG's objectives.

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

Impact: An estimate of the potential consequences associated with an identified risk should the risk occur.

Inactive: A risk that has passed or has been averted (i.e., the risk is closed).

Likelihood: The measure of the chance of a risk occurring, expressed as a percentage between 0% and 100%, where 0% is impossibility and 100% is absolute certainty.

Mitigate: An action associated with a risk treatment plan that involves reducing the probability and/or impact of the risk.

New Risk: A risk that has been raised which may not be fully understood but is perceived to be potentially significant to OPG's objectives.

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

Risk Rating: A measure of the significance (Extreme, High, Medium, Low) of residual risk assigned to each enterprise risk based on risk score.

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

Risk Trigger: An indicator, precursor, or condition that initiates a risk, or forewarns that it is about to occur.

Secondary Risk: A new risk that is introduced as a result of executing a risk treatment plan.

Transfer: An action associated with a risk treatment plan that involves implementing a mechanism or agreement whereby an outside party assumes responsibility for all or part of the risk.

4.2 Abbreviations and Acronyms

ARC - Audit and Risk Committee
BU - Business Unit
CRAE - Chief Risk and Audit Executive
ERC - Executive Risk Committee
ERM - Enterprise Risk Management
GRC - Governance, Risk and Compliance
OPG - Ontario Power Generation
SME - Subject Matter Expert
SPOC - Single Point of Contact

5.0 BASES, RECORDS AND REFERENCES

5.1 Bases

- ISO 31000:2018

5.2 Records

The following records may be generated by use of this document and shall be registered in appropriate document management system in accordance with the following table.

Record Created	Associated Form or Template Number	QA Record? Y/N	Filing Information/Retention
Enterprise Risk Register; BU Risk Register	N/A	N	Active risks will be maintained within the Resolver software tool until they are closed. Inactive risks will be retained for a period of 7 years.
Quarterly Risk Report	N/A	N	Retained by Corporate Secretary as part of the Board material.

5.3 References

5.3.1 Performance References

- OPG-POL-0004, Enterprise Risk Management Policy.
- OPG-PROG-0004, Enterprise Risk Management Program.
- GRC Instructions.

5.3.2 Developmental References

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

- RG Risk Committee Charter

6.0 REVISION SUMMARY

This is an **intent** revision.

- Aligns the ERM Procedure with revised ERM Program.
- All references to strategic risk removed.
- Updated Risk Rating Criteria in Appendix A.
- Included Bow Tie Model in Appendix B.
- Updated roles and responsibilities consistent with the ERM policy and program.
- Updated risk terminology for clarity and consistency.

Appendix A: Risk Rating Criteria

ERM Risk Rating Criteria

OPG's enterprise risks are assessed based on likelihood and impact with consideration given to the effectiveness of controls. The following tables provides a description of these criteria and their respective rating scales.

LIKELIHOOD CONSIDERATIONS		
Assessment	**Rating**	**Chance to occur within 3 years**
Almost Certain	5	90 - 100% chance
Likely	4	50 - 89% chance
Possible	3	30 - 49% chance
Unlikely	2	5 - 29% chance
Rare	1	< 5% chance

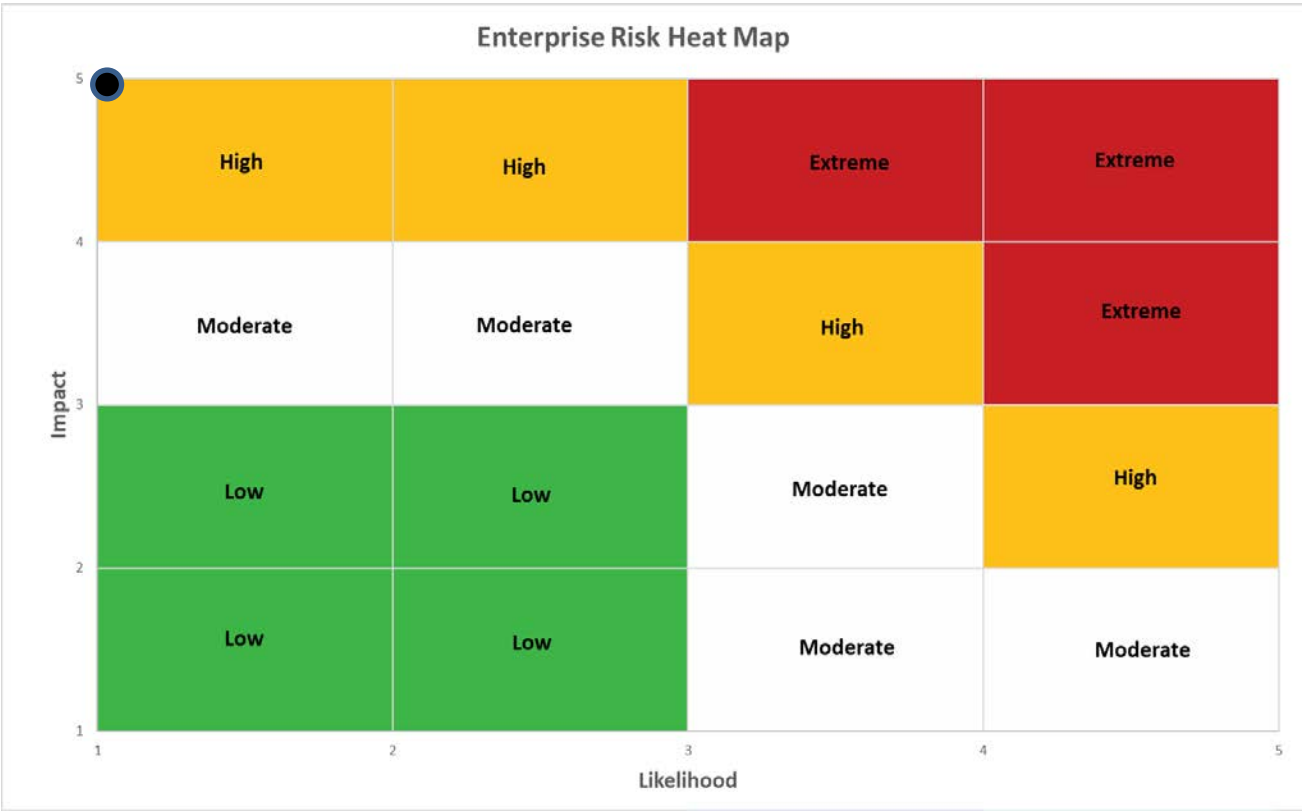
IMPACT CONSIDERATIONS					
Assessment	**Rating**	**Public or Employee Safety**	**Financial**	**Reputational**	**Operational**
Severe	5	Fatality of employee, contractor or member of the public	> $500 M	Sustained significant negative event covered by the media for >1 week; Loss of confidence in OPG by key stakeholders / communities of interest	500 MW or greater interruption lasting > 3 months
Major	4	OHSA defined critical injury to employee, contractor or member of the public; Life-altering occupational disease	$250 M - $500 M	Significant negative event with coverage by the media for < 1 week	500 MW or greater interruption lasting 1 - 3 months
Moderate	3	Injuries resulting in more than two lost days; Regulatory compliance infraction.	$100 M - $250 M	Negative event with coverage by the media lasting a few days	500 MW or greater, or business interruption lasting 2 – 4 weeks
Minor	2	Injuries resulting in less than two lost days; Corporate or station policy non-compliance	$25 M - $100 M	Public escalating concerns to OPG Management	Interruption lasting 1 - 2 weeks
Minimal	1	Accident requiring First Aid or no attention	< $25 M	No media coverage or business as usual	Interruption lasting up to 1 week

Note: Impact considerations for reputational risks are guidelines. Assessors may consider reputational impacts from other stakeholders (i.e. regulators) and mediums (i.e. social media).

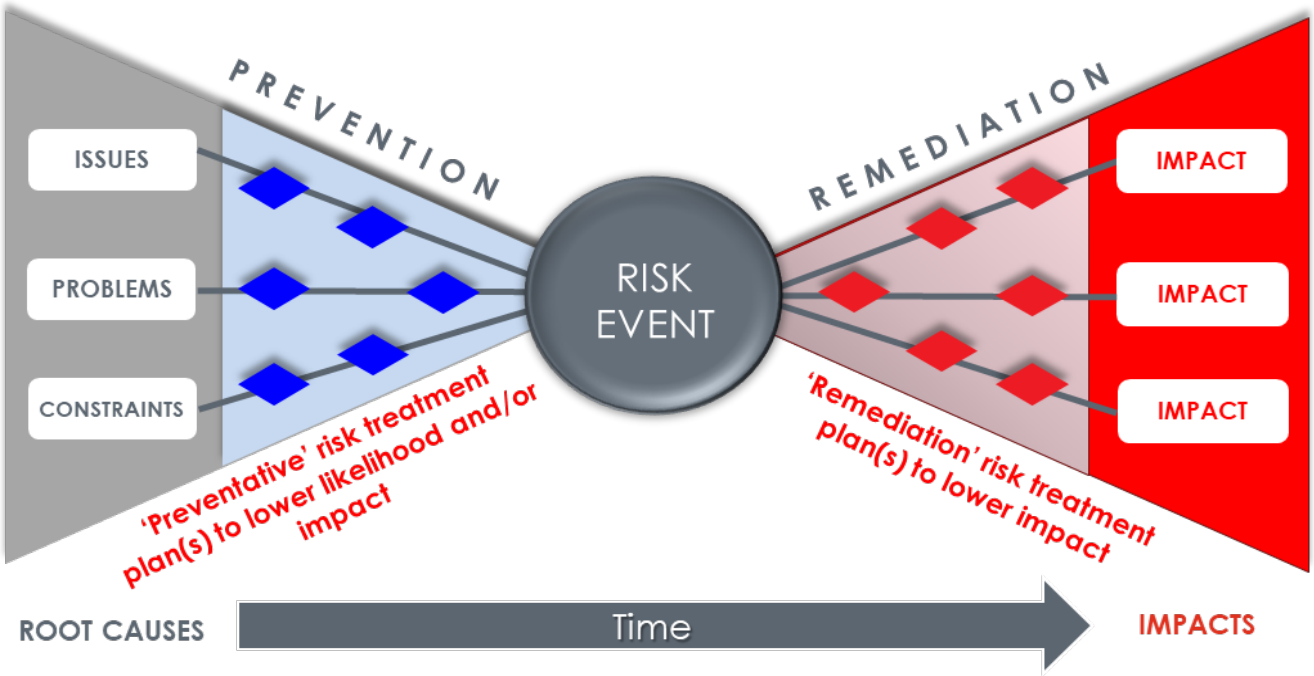
CONTROLS EFFECTIVENESS SCALE		
Assessment	**Score**	**Indicative Description**
Controlled	5	Response to risk is completely appropriate for all scenarios, and working as planned
Effective	4	Response to risk is appropriate for most foreseeable scenarios
Moderate	3	Response to risk is appropriate for many scenarios but gaps have been identified that could result in unplanned incidents or outcomes
Weak	2	Controls in place are not adequate to prevent or mitigate this risk and could readily lead to unplanned incidents or outcomes under normal operating conditions
Uncontrolled	1	Response to risk does not reduce inherent risk rating; No controls in place to prevent or mitigate this risk

ERM Heat Map

Risks are mapped on a heat map based on its likelihood rating and the highest impact rating for Safety, Financial, Reputational and Operational. For enterprise risks that are assessed on the cusp of two or more assessment categories (e.g. for risks that are assessed on the cusp of an overall assessment), the ERC will make the final determination regarding which category is most applicable to the risk.



● - Black Swans

Appendix B: Bow Tie Model

- Describes how a risk may happen – i.e. problems/issues today (root causes) that could lead to the risk event
- Determines potential *impacts* should the risk occur
- Establishes what we are doing about the risk (i.e. to prevent and/or recover)