KPMG

Ontario Power Generation

FINAL

Review of Enterprise Risk Management (ERM)

Overall Audit Rating:
Requires Improvement

October 30, 2019

Contents

1.0 Executive Summary 4

1.1. Objectives and Scope 4

1.2. Assessment Approach 4

1.3. Assessment Results 5

1.4. Overall Assessment 7

2.0 Observations & Recommendations 12

Appendix 1 — Documents Reviewed 24

Appendix 2 — Interviewee List 25

Appendix 3 — Classification of Internal Audit Findings 26

Appendix 4 — Disclaimer 28

Distribution

For Action:

Name	Title
Liane Kim	VP Assurance, Chief Risk & Audit Executive
Adam Chiarandini	Director, Enterprise Risk Management

For Information:

Name	Title
Ken Hartwick	President & Chief Executive Officer
John Mauti	Chief Financial Officer & SVP, Finance
Mike Martelli	President, Renewable Generation
Sean Granville	Chief Nuclear Officer
Christopher Ginther	Chief Administrative Officer
Dietmar Reiner	SVP, Enterprise Projects
Andy Moeck	Director, Nuclear Oversight
Michael Gore	Director, External Reporting & Accounting Policy
Stephanie Chang	Manager, External Reporting
Alexander DeAngelis	Senior Manager, Enterprise Risk Management
Janice Ding	Director, Internal Audit

1.0 Executive Summary

1.1. Objectives and Scope

KPMG LLP ("KPMG") was engaged by Ontario Power Generation ("OPG") to conduct an independent review of OPG's Enterprise Risk Management ("ERM") programme. The objective of the audit was to independently assess the design adequacy and operating effectiveness of the processes and controls in place for ERM, and determine its overall maturity level against KPMG's ERM framework and methodology, industry standards (e.g. COSO ERM and ISO 31000) and peers' practices.

1.2. Assessment Approach

KPMG's work involved a combination of the following procedures:

- Examination of documents (See *Appendix 1* for the "Documents Reviewed");
- Interviews and discussions with relevant Management and Board members (*See Appendix 2* for the "Interviewee List"); and
- Observations.

The audit scope period covered was August 15, 2018 to August 15, 2019. The scope of the audit included:

(a) Review the ERM components required by OPG: (a) Risk Oversight & Governance, (b) Risk Management Integration, (c) Risk Training & Awareness, (d) Risk Identification, (e) Risk Assessment, (f) Risk Monitoring & Reporting, (g) Risk Appetite & Tolerance, (h) Risk Response, (i) Risk Register, (j) Systems & Technologies, (k) Risk Modelling & Analysis and (l) Risk Management Staffing & Resources;

(b) Review the ERM components in line with KPMG's ERM Methodology (**Figure 1**) aligned with industry standards (e.g. COSO ERM and ISO 31000); and

Figure 1: KPMG's ERM Framework and Methodology

(c) Provide OPG with observations and recommendations on the adequacy of the current ERM framework and risk governance structure.

Areas out of Scope

The scope of this audit does not include a review of the adequacy and / or effectiveness of the following:

- OPG's adequacy and effectiveness of risk management strategies and internal controls to manage its risks across the organisation;
- Any metric and/or indicator (including thresholds) used to measure and/or monitor risks; and
- Other risk management policies, procedures or practices in place at OPG to manage specific risks (e.g. Credit Risk Management, Safety Risk Management, Project Risk Management, etc.).

1.3. Assessment Results

Overall Audit Rating	Requires Improvement

# of Findings		
	High	0
	Moderate	5
	Low	1

The key findings identified during the course of this audit are summarised in the following table and rated using the priority scheme detailed in *Appendix 3* of this report.

Summary of Findings					
#	**Finding**	**Action Owner(s)**	**Due Date**	**Risk Type**	**Risk Rating**
1	Risk Reporting	Adam Chiarandini – Director, ERM Liane Kim – VP Assurance, CRAE	1.1 – Q1 2020 1.2 – Q4 2020 1.3 – Q1 2020	Operational	**Moderate**
2	Risk Appetite and Risk Monitoring	Adam Chiarandini – Director, ERM Liane Kim – VP Assurance, CRAE	2.1 – Q1 2020 2.2 – Q1 2020 2.3 – Q1 2020	Operational	**Moderate**
3	Risk Culture	Adam Chiarandini – Director, ERM Liane Kim – VP Assurance, CRAE	3.1 – Q4 2019 3.2 – Q3 2020	Operational	**Moderate**
4	Embed ERM in Objectives & Strategy Setting	Adam Chiarandini – Director, ERM Liane Kim – VP Assurance, CRAE	4.1 – October 2020 4.2 – Q2 2020	Operational	**Moderate**
5	Risk Governance, Clarity of Risk Accountabilities	Adam Chiarandini – Director, ERM Liane Kim – VP Assurance, CRAE	5.1 – NA 5.2 – October 2020 5.3 – Q1 2020 5.4 – Q4 2019 5.5 – Q1 2020	Operational	**Moderate**
6	Risk Policy Documentation	Adam Chiarandini – Director, ERM Liane Kim – VP Assurance, CRAE	6.1 – Q1 2020	Operational	**Low**

Details for each of these findings and underlying recommendations are included in **Section 2** of this report. These findings and recommendations were discussed with Management.

Management has accepted the findings and has identified resolution plans to address the related recommendations which will be included in the tracking process of recommendations maintained by the Internal Audit function. Given the dual accountabilities of the Chief Risk and Audit Executive covering both Internal Audit and ERM, Internal Audit will work with the External Reporting Group, who provided oversight for this audit to preserve independence of the audit process, to coordinate and validate the closure of recommendations.

Within the context of the audit scope, approach and agreed procedures, the overall rating for this internal audit review is "**Requires Improvement"**, as described in *Appendix 3*.

1.4. Overall Assessment

1.4.1 Sentiment Analyses

Interviewees provided positive feedback on the foundational changes the ERM function has made in the past 18 months, yet have identified additional opportunities to create greater value. It was consistently recognised that OPG's leadership was instilling an increasingly collaborative culture and improving the risk management processes. This is a necessary leadership initiative to overcome historical silo'ed organisational culture challenges which may have affected the ERM program in the past. Please refer to *Appendix 2* for the list of interviewees.

Notwithstanding recent improvements, interviewees consistently suggested that ERM should be formally integrated in strategic and operational planning and decision-making, further aligned across the various risk programmes and cascaded down to operations. We have summarised the interviewees' feedback into the table in **Figure 2** below. Please note that the table below is a summary of the feedback received from the interviewees and not an assessment or representation of KPMG's views.

Figure 2: Interviewees' feedback

Areas of strength
The following areas of strength (not classified in order of importance) have been consistently identified across the interviewees: • **Strong leadership and tone at the top:** Board members have confidence in leadership's ability to articulate and action positive changes within the organisation such as improving risk management collaboration, transparency and accountability. • **Structured and periodic risk assessment:** On a quarterly basis the ERM function engages with Business Unit Leads and Single Point of Contacts ("SPOC") to develop a bottom-up risk report issued to the Executive Risk Committee ("ERC") and the Audit and Risk Committee ("ARC"). • **Improving collaboration:** The strong organisational cultural focus (i.e. 'One OPG Culture') has contributed to further improve collaboration across Business Units and Risk Owners. • **Lessons learned:** Leadership is highly cognisant of historical operational, major project performance and reputational risk management challenges. OPG continuously engages with employees, contractors and the government to improve the operational and major project performance, for example through 'lessons learned' analyses. • **Refined ERM processes:** All interviewees recognised the improvements to the overall ERM process in recent months including changes to the dashboard, risk definitions and composition to the ERC. • **Scenario analyses:** Third-party facilitation services have been retained to develop and analyse scenarios of the business strategy for the next 5 to 10 years. • **Cyber risk deep-dives:** ERM has worked with the Chief Information Officer to improve cyber risk reporting, trends and mitigation strategies. These efforts have been put in place to further inform the Board and Management of overall cyber risk exposures and control effectiveness.
Opportunities for improvement
The following opportunities (not classified in order of importance) have been consistently identified across the interviewees: • **Decision support:** Interviewees recognised the recent improvements to the quarterly risk reports as a decision support tool. However, the timeframe between the initial key risk identification, assessment, mitigation decisions and treatment plans of accountable management was consistently deemed '*too long*'. The risk identification, decision making and action cycle should be reduced. It was viewed that ERM should be further matured as a key 'real-time' decision support function for strategic operational and special projects / initiatives. This perspective is aligned with risk management standards (i.e. ISO 31000 and COSO ERM) and peers' leading practices. • **Earlier ERM engagement in major projects / initiatives:** Further formalise and provide transparency on the involvement and interface of the ERM function into key projects / initiatives (e.g. independent review, risk aggregation and reporting). • **Alignment of methodologies:** Align risk management methodologies and language across various risk programmes (e.g. Nuclear and Project). • **Cascade ERM:** Interviewees were confident in Senior Leaderships' appreciation and support of ERM. However, they raise the need to further cascade down ERM to the whole organisation (operational and tactical levels). • **Real-time dashboards:** Currently, and despite progress, the ERM information shared provide a 'static picture' of the risk information (versus fluid) which is updated on a quarterly basis for reporting purposes. • **Clarity of risk appetite statements:** Interviewees are overall not able to appropriately articulate, communicate and action risk appetite statements across all material risks.

We have asked each interviewee to rate the following three (3) statements on a scale of 1 (strongly disagree) to 10 (strongly agree). The results (individual and average scores) are reflected in **Figure 3** below.

Figure 3: Interviewees' responses distribution and rationale

Statement 1: *"The existing ERM Programme provides confidence* to the Board and Management that all material/significant risks are adequately and effectively managed across the organisation".*

Avg.	1	2	3	4	5	6	7	8	9	10
7.5						●◖	●◖	●●●◖		

Rationale: Interviewees acknowledged that recent changes to the ERM programme, including updates to the risk report, risk definitions and in-depth risk discussions on cyber risk for example, have contributed to improve the overall confidence that significant risks are being adequately managed. However, interviewees believe that there is still room for improvement including:

- Additional in-depth risk discussions on key / material risks to focus the discussion on areas that matter the most, such as Labour Relations, Government Policy and the Darlington Refurbishment project;
- Risk appetite statements are too high-level and do not provide enough context to understand the level of risk the organisation is willing to accept in pursuit of its strategy, and hence whether the control environment in place is adequate; and
- Use of additional quantifiable risk measures (such as Key Risk Indicators ("KRI")) to further inform risk reports.

***Note:** During the interviews it was further clarified that the ERM programme is not an assurance function and therefore cannot provide confidence with respect to the effectiveness of risk management. However, ERM develops and implements the ERM framework and processes that support through effective risk identification, assessment and management, including reporting risks to the Executive and Board.

Statement 2: *"All risk management activities (including ERM) are well coordinated across the company and between different functions".*

Avg.	1	2	3	4	5	6	7	8	9	10
6.6					●	●●●◖	●	●◖		

Rationale: Interviewees believe that Senior Leadership has been more collaborative in addressing significant enterprise and projects risks. However, concerns were expressed that risk management was not consistently cascaded down to operations. Interviewees identified the following improvement areas:

- Ensure that risk methodologies are appropriately aligned throughout the organisation (i.e. ERM, Projects, Nuclear, Renewable Generation ("RG"), etc.);
- Reinforce the need to be more transparent about risks between Business Units; and
- Co-ordinate risk management activities to help reduce potential redundancies (e.g. different risk management methods and tools used across Business Units).

Statement 3: *"The overall ERM programme is adequate to generate the expected value to the organisation".*

Avg.	1	2	3	4	5	6	7	8	9	10
7.5						●◖	●●	●●◖	●	

Rationale: Interviewees were confident in the ERM function and the progress that has been made over the past 18 months. The general sentiment has been to continue improving as the Board and Management rely on the information shared to exercise their risk oversight and make decisions. Additional value-added decision support the ERM function could provide are:

- Ensuring that Business Units have relevant real-time risk information through an effective and integrated risk dashboard;
- Earlier engagement of ERM in the business planning and enterprise strategic planning; and
- Actively engaging the Board in strategic risk discussions, emerging risks and scenario analysis, including for low probability – high impact events (e.g. Darlington Refurbishment may be subject to a Public inquiry).

1.4.2 Benchmark

We have provided ERM industry average and leading practices across key ERM attributes based on a sample of similar and relevant peers (e.g. Duke Power, Tennessee Valley Authority, Exelon, etc.). Although there is a wide range in ERM maturity across the industry peers, there are a number of practices OPG can leverage / learn from, which are reflected in **Figure 4** below.

Figure 4: Peer Practices

Attribute	Industry common practice	Leading practices
Risk Strategy & Appetite	● High-level qualitative risk appetite statements are defined and approved by the Board and relevant sub-committees (e.g. Audit Committee)	◎ Align ERM with the corporate strategic planning and reporting process ◎ Qualitative and quantitative risk appetite statements are defined for each of the key material risks ◐ KRIs are developed, linked to the risk appetite statements ◐ Risk tolerances have been established
Risk Governance	● Risk management most commonly reports to the Audit (and Risk) Committee (or equivalent) ● Executive Risk Committees are established and meeting at least quarterly to review, challenge and approve risk reports before issuance to the Board	◎ ERM function reports independently to the dedicated Board Risk Committee ● CRO (or equivalent) has a direct and independent reporting line to the Risk Oversight Committee (e.g. Audit and Risk Committee) ◐ CRO has the authority within the organization to independently report on areas of high threat or opportunity exposure ◐ The Board is actively and regularly engaged in high exposure strategic, operations, special projects and emerging risk discussion ◐ Distinct Business Units' Risk Committees formed to discuss strategic and tactical risks ◎ Overarching ERM policy with related 4 supporting policies that cover Operational risk, Strategic risk, Finance risk and Project risk
Risk Culture	● Conservative risk appetite due: to low-profit margin business model; safety focus; and highly regulated business	◐ Pro-active and continuous identification and communication of risks ◐ Risk culture focused on risk mitigation in pursuit of strategy ◐ Business unit staff rotational programme into ERM department
Risk Assessment & Measurement	● ERM methodologies have been established however have not been integrated / operationalised with Business Units ● Risk assessments are re-evaluated on an annual basis	◐ ERM methodologies are aligned and embedded into Business Units ◐ Risks are evaluated continuously and support strategic, operational and major project decision-making ◎ Annual risk refresh with scenario analyses
Risk Management & Monitoring	● Risk treatment plans and status of are reported at least quarterly ● Minimal validation / collaboration with Internal Audit	◎ KRIs and other quantifiable risk measures are reported ◎ Internal Audit Plan and resulting control effectiveness recommendations are aligned with the enterprise risk profile ◐ Internal Audit Plan expectations are to ensure high exposure risks are managed effectively
Risk Reporting & Insights	● Quarterly risk-report refresh provided to the Board and Management	◐ Analysis and reporting tools used (e.g. PowerBI) to automate risk collation and provide interactive dashboards for the Board and Management ◐ Risk deep-dives for emerging and high risk-exposures
Data & Technology	● Microsoft office based risk registers ● Sharepoint / e-mail used to update risk registers	◐ Common Governance Risk and Compliance ("GRC") technology to automate risk collation consistently across the organization which integrates enterprise, operational and project risk management

Legend:
● Fully in place
◐ Partially in place
◎ Not in place

1.4.3 Positive Attributes

Throughout our review of existing documentation, benchmarks and interviews conducted (see sections 1.4.1 and 1.4.2 above), we observed a number of good practices in place in OPG, such as:

- Risk information for quarterly risk reports are gathered using a bottom-up approach (i.e. through the Business Unit Leads and SPOCs);
- The risk taxonomy has been aligned to OPG's strategic imperatives (i.e. *Operational Excellence, Financial Strength, Project Excellence and Social License*);
- The overall ERM 2019 Roadmap is indicative of what other major utilities are pursuing in terms of maturing their ERM programmes (e.g. better alignment with strategic planning, further embedding ERM into business operations, stronger integration with project risk management, establishing an active and engaged Executive Risk Committee, active Board engagement of key strategic risks during Board Offsite Strategy sessions, further refining risk appetite statements and risk tolerances, and emerging risk identification and management);
- Governance, Risk, Compliance ("GRC") technologies (i.e. Resolver and PowerBI) are automating risk management workflows; and
- Regular risk reporting to the various Management and Board Risk Oversight Committees.

There was general consensus on the results to further structure, formalise and streamline the existing ERM programme and supporting practices. The *ERM 2019 Roadmap* has established a number of actions to further mature the ERM programme since Q1 2019 - although further details were not provided in terms of the exact scope, stages and expected content changes - including:

- **Risk Governance:** Rotating the Chairmanship of the Executive Risk Committee between Business Unit Leaders to further reinforce risk management as an accountability of Management **(Status: Completed)**;
- **Risk Definitions:** Redefining and reframing risk definitions from a risk issue statement to a risk event **(Status: In Progress)**;
- **Risk Assessment / Methodology:** Redesigning the risk rating methodology from an 'impact * probability * urgency' formula to a simpler 'impact * probability' calculation **(Status: In Progress)**;
- **Risk Appetite:** Revisiting the risk appetite statements, risk tolerances and KRIs to inform Board risk reporting **(Status: In Progress)**;
- **Business Unit ERM Maturity:** Further embedding ERM principles and processes within key business units (e.g. RG, Nuclear) **(Status: In Progress)** including:
    - Operationalising a top-down risk assessment at the Enterprise level and to be validated continuously using the bottom-up approach at the Business Unit level;
    - Formalising SPOC responsibilities into job descriptions;
    - Refreshing computer-based training material for SPOCs and Management; and
    - Using ERM information to inform Business Unit Executive Committees (e.g. Renewable Generation Executive Team, Nuclear Executive Committee) of emerging risks and status of treatment plans.

1.4.4 ERM Improvement Opportunities

Based on our review of the existing documentation in place, and interviews, the following areas for improvement have been identified, and further detailed in the section 2 that follows:

- Enhance existing ERM reports, including the design, content and usability of risk information to better inform Board and Executive Leadership's decision-making **(F.1, F.2)**;
- Improve the overall risk-culture by further cascading ERM principles into the whole organization and proactively engage the CRAE and ERM function in strategic and business planning initiatives to better inform strategies based on existing and future risks **(F.3, F.4);**

- Empower/enable the ERM function to further operationalize risk management principles with a clear mandate that defines its objectives and authority. This should also include allocating more time at the ARC and Board as a whole for focused risk discussions **(F.5)**; and
- Review and update the ERM information (i.e. frameworks, programs, policies, mandates) to ensure that the documented requirements are aligned with existing / future practices **(F.6)**.

Risk management programmes need to be adapted and tailored to the size, nature and complexity of each organisation. We hence suggest OPG continue to focus on a more holistic and "top-down" lens in reviewing its overall risk management operating model, which should cover both the hard (policies, procedures, guidelines) and soft (people and culture) components of an adequate and effective risk management programme.

2.0 Observations & Recommendations

F.1: Risk Reporting	Audit Finding Rating: *Moderate*
The ERM report lacks some key components (e.g. risk profile against risk appetite statements), in order to help Management and the Board (and sub-committees) to undertake their risk oversight roles and responsibilities.	

Observations

OPG's ERM Report is submitted on a quarterly basis to the ERC and ARC, in line with the requirements set in the ERM Policy and ARC Charter. As part of the quarterly risk update, the ERM function engages with the Single Point of Contacts ("SPOC") across the Business Units to gain an appreciation of the risk profile. The role of the SPOC is to input and update risk information into the Governance Risk and Compliance ("GRC") software which is then used by the ERM function to inform the ERM report. However, based on the recent changes in the ERM report, we observed some limitations in the design, content and usability of the report.

Structure and content of the ERM report:
The information provided in the ERM report should provide the ARC and ERC with the relevant insights and measures in place and to be implemented to manage the risks within acceptable levels, the (emerging) risks, potential key business disrupters and forward outlook. Through our review we observed the following**:**

- There is no formal 'Agenda' that clearly articulates and focuses the key objectives and expected approvals / decisions from the ARC or ERC;
- There is a lack of clarity on what constitutes an 'emerging risk' and the internal mechanisms to identify, manage (e.g. develop action plans), monitor, and potentially escalate them into key enterprise risks;
- On a quarterly basis, the ERM function provides one specific risk deep-dive (e.g. *Information Security Initiatives* in Q2 2019). There has been positive feedback on the in-depth risk discussion, yet members of the Board and Management would value obtaining additional quarter-on-quarter risk insights (i.e. progress on action plans, risk management strategies, assurance reports, etc.) for high-risk areas such as '*Labour Relations, Darlington Refurbishment, Government Policy*'. Note that based on Management representation, we understand some relevant information may be shared as part of other Board / Sub-Committees meetings;
- Risk appetite performance indicators (i.e. indicators for reporting realised risk events) have been developed however are not tracked or reported in the ERM reports; and
- Objective Risk Appetite Statements (RAS) and monitoring mechanisms (e.g. KRIs) are not formally defined or reported.

Usability of the ERM report:
The ERM report should enable the ARC, ERC and Management to discuss, challenge and ultimately support decision-making. Through our review we observed the following:

- The report provides a more 'static' picture in the information shared quarterly with the ERC and ARC. The existing dashboard built into the GRC solution does not enable Management to consistently utilise risk information on a day-to-day basis; and
- There is no formally defined minimum escalation requirement that describes when a Business Unit risk should be escalated to the ERM function (e.g. due to breaches in risk tolerances or treatment plan delays).

Impact

Without incorporating the elements noted above within the ERM report, Management and the Board (and its Sub-committees) may not be able to effectively undertake their risk oversight duties and responsibilities and make decisions.

No.	Recommendation(s)	ERM Roadmap
1.1	Revisit the ERM Report to provide additional clarity to the ARC and ERC. We have identified the following sections for consideration: • Agenda items with objectives and required approvals; • Summary of breached RAS, performance indicators, KRIs (exception reporting), and corresponding action plans / management responses; and • Quarter-on-quarter risk insights for the ARC and ERC for high-risk areas (e.g. Labour Relations, Public Policy, Government Relations, etc.). This would include detailed progress plans, additional assurance reports from IA and third parties.	Partially, there has been a recent initiative to refresh the top risk dashboard. However, can be further improved.
1.2	Further improve the GRC solution or better integrate analysis and reporting (e.g. Power BI) to visualise real-time risk data and gather insights from operational and project management risk repositories.	There are no plans known to us to integrate the mid-modules to visualise real-time data in the ERM roadmap.
1.3	Consider defining some minimum criteria to trigger the escalation of Business Unit risks to the ERM report (e.g. any risks including ethics, loss of life, and loss of confidential data). Note these criteria are not meant to substitute qualitative quarterly discussions between SPOCs, Business Units and the ERM function on what should be escalated.	There are no plans known to us to define the escalation criteria in the ERM roadmap.

Agreed Management Action			
1.1 Although there have been changes to the ERM risk assessment process and ensuing quarterly report, ERM recognizes that we are on a continuous improvement journey. ERM will begin to address these items in Q4 2019 and beyond, and will be reflected in the quarterly risk reports. **1.2** ERM's existing plan already included making changes to the Resolver GRC system as part of the overall improvements to the ERM Framework. This includes mapping of BU risks to the top enterprise risks. For project risks, ERM will work with the EPO to improve alignment with risks contained in RMO. **1.3** ERM will add guidance on criteria to consider for escalating a business unit risk to the enterprise risk report as part of the improvements to the ERM Framework.			
Responsible Officer	Adam Chiarandini – Director, ERM Liane Kim – VP Assurance, CRAE	**Target Date**	**1.1** Q1 2020 **1.2** Changes to Resolver GRC and Power BI will require a business case and support from CIO to implement. Target for completion by Q4 2020 **1.3** Q1 2020

F.2: Risk Appetite and Risk Monitoring	Audit Finding Rating: ***Moderate***
Risk appetite statements and key risk indicators are not appropriately defined in order to help the organisation measure and monitor risks.	

Observations

Clarity of Risk Appetite Statements ("RAS"):

The ERM function helps define the risk tolerances for the strategic imperatives (i.e. *Operational Excellence, Financial Strength, Project Excellence and Social License*) using the risk scores (impact * probability * urgency). For example, the corporate RAS for Financial Strength is categorised as "Flexible" and a RAS definition of "*OPG is willing to take on higher level of financial risk on a controlled basis in pursuit of its strategic imperatives or innovation*". However, the feedback from Management on the current RAS was that they were difficult to use to define and operationalise the risk strategies. Industry leading practices suggest that the organisation defines RAS and risk tolerances at a more granular level, and where possible, in quantifiable terms (i.e. at the sub-risk category level) to effectively operationalise and monitor risks to the company.

Use of Risk Appetite Performance Indicators:

As documented in the ERM Policy, risk appetite performance indicators have been identified to 'report significant risk events'. For example, Thermal Equivalent Forced Outage Rate ("EFOR") %: Actual EFOR increases by greater than 25% (report to shareholder), 15 – 25 % (report to Board). However, the performance indicators are not formally used to inform risk reporting or track historic performance of risks to provide additional insight on risk ratings and trends.

Development and Integration of KRIs:

In recent months, the ERM function has developed 5 KRIs for Cyber Security, Talent Attraction & Retention, Safety, U2 Return to Service, and Vendor Capability & Capacity risks. A KRI score is calculated for each risk and based on the composite weight of various indicators. A 'leading' indicator is assigned a greater weightage than a 'lagging' indicator. However, the proposed KRIs and approach to monitor and report them have not been formally approved, fully integrated within Business Units or used in the quarterly ERM reports.

Impact

Without clear articulation of RAS and monitoring mechanisms (e.g. KRIs), the organisation may not be able to adequately and effectively identify and manage its key risks within acceptable levels.

No.	Recommendation(s)	ERM Roadmap
2.1	Review the overarching RAS and qualitative / quantitative risk measures across the risk categories to ensure they are succinct, clearly express "how much risk OPG is willing to take / accept", regularly refreshed and to include a measurable component. As part of this process, clearly document and communicate the development of RAS, including governance and roles and responsibilities across the organisation (e.g. Board of Directors, Management and the ERM function).	There are plans to refresh the existing risk appetite and risk tolerances.

2.2	Re-evaluate the Performance Indicators defined, in line with the RAS: • Assess the adequacy of existing Performance Indicators; • Assign Performance Indicator Limits for Shareholders, Board and Management; • Use Performance Indicators to inform risk ratings and objectively challenge Business Units and Risk Owners; and • Leverage Performance Indicator Limits to inform Risk Management discussion at the Board and Management level.	There are plans to refresh the existing risk appetite and risk tolerances.
2.3	Review and finalise meaningful KRIs including thresholds and limits, linked to the RAS and risk tolerances. KRIs should be: • Leading versus lagging by nature (i.e. inform Management of risks before they materialise); • Easy to use and timely; and • Support effective decision-making at the Board and Management level.	There are plans to re-evaluate KRIs.

Agreed Management Action			
2.1 Per ERM Roadmap, ERM will work with the BU owner(s) to develop risk appetite statements for each key risk. These will be communicated to relevant stakeholders through existing ERM reporting or education / training to business line management. **2.2** ERM believes that the performance indicators noted in the governance are duplicative of performance reporting, such as the corporate balanced scorecard, and do not provide value to the overall risk management framework. As such, ERM will remove this section from the ERM Policy in the next update. **2.3** Per ERM Roadmap, ERM is working on the first 5 KRIs and intends to present in our Q4 2019 ERC / ARC reporting and track the KRIs formally beginning in the Q1 2020 reports. Additional KRIs will be developed in the future where appropriate.			
Responsible Officer	Adam Chiarandini – Director, ERM Liane Kim – VP Assurance, CRAE	**Target Date**	**2.1** Q1 2020 **2.2** Q1 2020 **2.3** Q1 2020

F.3: Risk Culture	Audit Finding Rating: ***Moderate***
The overall ERM programme is largely perceived as a process / exercise (versus a continuous tool to inform decision-making), and has not been cascaded throughout the organisation to support a strong risk culture.	

Observations
As part of OPG's strategic plan, under the '*Social License*' strategic imperative, a key initiative has been to build the '*One OPG Culture*'. As part of this initiative, the organisation has increased its focus on diversity in its workforce and building a more transparent and collaborative environment. Per discussion with Management, the recent changes have helped improve the risk culture. The sentiment has been that previous risk ownership was silo'ed. However, in recent months, risk owners have started to better collaborate across Business Units. Management has indicated that risk assessments are only refreshed as part of the quarterly report to the ARC (or based on other reporting requirements). This may suggest that the ERM process is considered as a 'compliance and post-mortem' exercise and not consistently used to inform day-to-day decisions. This may reflect a procedural organisational culture resulting from a highly regulated veil under which OPG operates. It is the moral hazard of procedural risk management which can detract from strategic and scenario-based risk analysis. Management has also indicated that ERM has not been fully cascaded down to the operational level of the organisation.

Impact
Without a strong risk culture, the organization may not be able to effectively embed risk management.

No.	Recommendation(s)	ERM Roadmap
3.1	Improve the overall risk management awareness, adoption and alignment across the organisation, through periodic rotation of Business staff.	There are no plans known to us to formally rotate staff into ERM.
3.2	Develop a cascading risk change management strategy (similar to what Nuclear is currently completing for the project risk management through the EPMO). This would include, training and improving general awareness of: • Value of the ERM programme to Business Unit planning and decision-making; • ERM methods; • ERM tools and technologies; • Risk analytics; • Facilitating and communication skills; • Understanding of cognitive biases in risk decision-making; and • Integration of ERM methodologies and results in business planning and day-to-day operational decision-making. The change management strategy should include a resourcing plan to ensure adequate coverage across all Business Units.	Partially, there are plans to refresh the computer-based training material, however change management initiatives should be 'high-touch' and require an effective strategy.
1.2	As part of the **F.1 Risk Reporting**, develop risk reporting mechanisms to ensure information inputted into the GRC technologies enable continuous risk decision-making.	N/A see above.

4.2	As part of **F.4 Embed ERM in Objectives & Strategy Setting**, consider formally engaging the ERM function in the business planning cycle.	N/A see below.
5.3	As part of **F.5 CRAE Mandate**, empower the CRAE and ERM function to have sufficient authority to enable changes.	N/A see below.

Agreed Management Action			
3.1 ERM does not have available FTEs in the business plan to accommodate rotations from other BUs, but will discuss this item with the ERC to determine if there is interest in developmental rotations funded from the base BU. **3.2** ERM agrees with providing additional education and training on ERM and risk-informed decision making. ERM will engage with the Change Management function to develop a comprehensive change management plan. **1.2 / 4.2 / 5.3** – Refer to respective sections.			
Responsible Officer	Adam Chiarandini – Director, ERM Liane Kim – VP Assurance, CRAE	**Target Date**	**3.1** Q4 2019 (ERC discussion) **3.2** Q3 2020 (roll-out of training as part of overall ERM Framework improvements)

F.4: Embed ERM in Objectives & Strategy Setting	Audit Finding Rating: ***Moderate***

Risk management is not consistently integrated to the strategic and business planning processes, in order to help ensure that risk management helps the organisation meet its objectives.

Observations

ERM Alignment with Strategic and Business Planning:

As documented in the ERM Policy, Business Units (i.e. Corporate Functions, Chief Administrative Office, Renewable Energy, Nuclear, Projects, etc.) are required to integrate risk management practices to inform business planning and day-to-day decision making. We observed the following:

- In recent months the Strategy team and a third-party vendor assisted the Executive Leadership Team in the development and analysis of scenarios to further inform strategic planning process, which was positively received based on the feedback from the interviewees. Accordingly, the Board has been engaged in the "Annual Board Offsite" to discuss OPG's strategy moving forward including results from the scenario analysis. However, the ERM function has not been formally included or engaged to ensure that there is appropriate linkage between proposed strategy and risk profile;
- Business Units must complete an annual risk assessment of their business plans. However, Business Units are not consistently using risk analysis (i.e. risk assessments) to inform strategic / business and resourcing decisions – which is suggested by industry standards and aligned with leading practices. This is evidenced as Management has acknowledged ERM assists the Business Units in identifying "*otherwise overlooked risks or obvious risks that were not recognised*".

Impact

Without a clear link and integration of risk management the organisation may take excessive risks and/or miss opportunities to take more calculated risks and reduce control efforts.

No.	Recommendation(s)	ERM Roadmap
4.1	Formally include the CRAE (and ERM function) as active contributors for the Annual Board Offsite sessions.	There are no plans known to us to include the CRAE (or ERM function) in the Annual Board Offsite sessions.
4.2	Formally engage the ERM function in the annual business planning process to facilitate the risk assessment and provide an independent view of key risks, controls and action plans.	There are plans to complete risk assessments for Nuclear and RG and align them with the business planning cycle.

Agreed Management Action

4.1 ERM agrees that including the CRAE in the Annual Board Offsite would be beneficial in engaging the Board in risk discussions and ensuring that risk management is integrated in setting the strategic plan. ERM will coordinate with Strategy and the Corporate Secretary to request participation and an agenda item for the 2020 session.

4.2 While ERM provides business planning instructions on incorporating risks and risk treatment plans in the annual business plans, ERM agrees with the recommendation, and will communicate the finding with Management within the business planning function to ensure there is formal engagement and input with BU management starting with the 2021 business plan.

Responsible Officer	Adam Chiarandini – Director, ERM Liane Kim – VP Assurance, CRAE	**Target Date**	**4.1** October 2020 **4.2** Q2 2020

F.5: Risk Governance, Clarity of Risk Accountabilities	Audit Finding Rating: *Moderate*

The Board / ARC may not dedicate sufficient time in order to adequately discuss, question and challenge the ERM report. In addition, the mandates of the CRAE and ERM function has not been comprehensively defined in order to provide clarity on the expected risk management roles and responsibilities from across the organisation. Furthermore, there may be confusion and potentially fatigue from the various risk management / assurance initiatives across the various Business Units.

Observations

Board Accountability: As per its mandate, the ARC is responsible for overseeing OPG's compliance, control environment and ERM programme. In recent months, the number of Directors at the Board of Directors has reduced from 14 Directors to 8 Directors (with 2 additional incumbents planned). As a result, the full Board has been in attendance for all Sub-Committee meetings planned. The full Board discussions on emerging risks and high impact scenarios (i.e. Information Security) have been viewed as a distinct enhancement to the existing risk governance practices and further enable the members to discharge their risk oversight roles and responsibilities. Through our review we have identified the following:

- The CRAE is allocated 20 minutes to present Internal Audit findings and ERM information. This may not provide sufficient time for the CRAE or Directors to effectively inform, engage, discuss and challenge ERM risks;
- Feedback from interviewees indicated that Board members have not been actively engaged in the identification of key strategic risks to the organisation. Industry leading practices suggest it may be beneficial to validate the Annual Strategic Enterprise Risk Assessments with the Board in an active and engaged manner.

Mandate of CRAE and ERM: The accountabilities of the Chief Risk and Audit Executive ("CRAE") and ERM function have been defined at a high-level within the various ERM policies and procedures. The role of the Risk Management function is to primarily facilitate, challenge and report material risks to the ARC and ERC. However, there is no formally documented mandate that clearly defines the objectives, roles and responsibilities and authority of the CRAE and ERM function. In line with leading practices, a formal mandate allows the ERM function to ensure that risk accountabilities, methodologies and Governance requirements are aligned and operationalised throughout the organisation.

Through our review, we noted that the Enterprise Project Management Office ("EPMO") developed and approved a Project Risk Management Standard in March 2019. The standard states that EPMO '*conducts portfolio level risk reviews and interfaces with the ERM department*', however there is no formal integration of the ERM function to effectively challenge the initial risk assessments of projects as per their accountability defined in existing ERM policies and procedures. Furthermore, leading practices suggest that the CRAE (or equivalent) should approve all Risk Management documentation to ensure all methodologies and proposed changes are aligned across the organisation.

A revitalised mandate should be supported by an effective change management strategy to better position the ERM function and its value proposition to the Business Units.

Assurance Programmes: OPG has several risk oversight / compliance / assurance functions across the three lines of defence: including ERM (2nd LOD), EPMO (2nd LOD), Nuclear Oversight (2nd LOD), Legal (2nd LOD), Internal Audit (3rd LOD), etc. The objective of these functions are to ensure:

- OPG is meeting its regulatory obligations(e.g. Canadian Nuclear Safety Commission, Ontario Energy Board, etc.); and
- Business Units have adequately accounted for risks in the design and execution of activities.

Management had indicated there may be confusion from the front-line staff regarding duplication of work (or work similar in nature) between the various risk oversight / compliance / assurance activities. While there have been significant improvements to align various assurance activities for the Darlington Refurbishment project, for example, there may be opportunities to further streamline activities across other OPG risk management functions.

Impact
Without clear risk accountabilities, planning and resources (e.g. time) allocated to risk management (and linkage with assurance programmes), the organisation may fail to exercise appropriate management and oversight over its material risk exposures.

No.	Recommendation(s)	ERM Roadmap
5.1	The Board and Management should re-evaluate whether ERM should report directly to the full Board or remain within the ARC. As part of its decision, all Charters should be reflective of the change.	There are no plans known to us to re-evaluate the risk oversight structure at the Board and Sub-committee level.
5.2	Management should further involve the Board and/or ARC members earlier in the Enterprise Risk Assessment process to further align and challenge the proposed risk ratings between Management and the Board.	There are no plans known to us to ensure the Board / ARC are involved earlier in the ERA process.
5.3	Management should revisit and consider formally documenting the mandate of the CRAE and ERM function (either in the relevant existing documents or through separate Terms of Reference). This should include: ● Definition of the purpose / objective of the CRAE and ERM programme; ● Accountability of the CRAE and ERM programme (i.e. assisting Management in operationalising risk management principles, co-ordinating with Business Units, reporting to the Audit and Risk Committee, etc.); and ● Authority of the CRAE and ERM programme (i.e. empowered by the Audit and Risk Committee).	There are no plans known to us to formalise the CRAE and ERM function mandate.
5.4	As part of the current initiatives to streamline various oversight / assurance activities ensure continued coordination of existing oversight / assurance programmes to develop a streamlined schedule that is communicated to all relevant stakeholders.	There are no plans known to us to streamline assurance activities. However, this has been completed for the Darlington Refurbishment project.
5.5	Senior Leadership should clearly define the risk operating model and governance for projects, with respective roles and responsibilities identified and clarity provided regarding the interface model between ERM and the EPMO.	There are no plans known to us to further define roles, responsibilities and interfaces.
3.2	As part of **F.3 Risk Culture**, develop a cascading risk change management strategy (similar to what Nuclear is currently completing for the project risk management through the EPMO). The change management strategy should include a resourcing plan to ensure adequate coverage across all Business Units.	N/A see above.

Agreed Management Action			
5.1 ERM does not agree with a change in the Board delegating responsibility for risk management to a Committee other than the Audit & Risk Committee. To ensure that the full Board is engaged and understands the risk profile, refer to 5.2 below. **5.2** Refer to management response to 4.1 above regarding CRAE attendance and ERM agenda item at Board Strategic Offsite. **5.3** ERM agrees and will update the existing ERM governance (specifically OPG-POL-0004) to include these areas. **5.4** Internal Audit leverages the ERM process in the development of the annual internal audit plan. Internal Audit will map internal audits to key enterprise risks to ensure appropriate coverage. **5.5** ERM agrees with the recommendation and will discuss with the responsible Executive Leadership on proposed roles & responsibilities to ensure alignment of project risk management with the overall ERM program. The output of any Executive decision will be reflected in the appropriate governance documents. **3.2** Refer to respective section			
Responsible Officer	Adam Chiarandini – Director, ERM Liane Kim – VP Assurance, CRAE	**Target Date**	**5.1** N/A **5.2** October 2020 **5.3** Q1 2020 **5.4** Q4 2019 **5.5** Q1 2020

F.6: Risk Policy Documentation	Audit Finding Rating: *Low*
Risk policies and procedures are not updated to reflect (recent) changes in the ERM programme which may create inconsistencies in implementation.	

Observations

We observed some redundancies, inconsistencies and/or lack of clarity in and between various risk policy documentation, including:

- Changes to the ERM programme have not been reflected in the ERM policy, procedure, programme, and training documentation. This includes recent updates to:
  - Risk rating methodology used (i.e. simplified likelihood * impact formula);
  - Risk rating criteria used to determine the probability, impact and urgency of material risks;
  - Use of GRC technologies used to automate risk monitoring and reporting; and
  - Shifting the accountabilities of credit risk and third-party risk back to Business Units.
- Risk roles and responsibilities lack clarity and/or may be inconsistent within documents. The Board's charter defines its accountabilities as responsible for "*identifying principal risks of OPG*". Where as in the ERM Procedure states that "*BU's and project teams should use the GRC tool to identify or update enterprise risks*" and the ERC is responsible for "*identifying emerging and strategic risks*".
- The process to develop, communicate, monitor and update the Key Risk Indicators and Risk Appetite Performance Indicators has not been clearly documented.

Impact

Without formal, complete and concise risk policies, procedures and/or guidelines, OPG's stakeholders may not be able to understand and adequately and effectively undertake their risk roles and responsibilities.

No.	Recommendation(s)	ERM Roadmap
6.1	Develop a clear risk policy architecture, and refresh the key risk documents (e.g. ERM policy and procedures) to ensure they are and remain relevant, accurate and user-friendly.	Partially, per discussion with management there are plans to refresh the risk documents once the Governance and Processes have been updated.

Agreed Management Action

6.1 ERM plans to update governance documents as part of the improvements to the ERM Framework. We will incorporate the findings above in revisions to the relevant sections of the ERM Policy, Program and Procedure.

Responsible Officer	Adam Chiarandini – Director, ERM Liane Kim – VP Assurance, CRAE	Target Date	**6.1** Q1 2020

Appendix 1 — Documents Reviewed

List of documents received
Strategic documentation: 1. Organisation chart with detailed roles & responsibilities 2. FY19 Strategic plan with key strategies and KPIs
ERM documentation: 1. ERM Framework / Policy / Guidelines, with any other underlying procedure (if any) 2. Other Risk Management Policies / Guidelines • Enterprise Project Office Risk Management program 3. Corporate Policy & Guideline on Business Conduct 4. Risk Management Roadmap (1 pager) 5. Risk Taxonomy / Risk Inventory 6. Latest enterprise risk assessment / risk register 7. Latest BU risk assessment / risk register 8. Latest project risk assessment / risk register 9. Latest contract risk assessment / risk register 10. Sample of all 'Risk Reports' (with Minutes) – in line with OPG's reporting structure e.g. Management, Audit & Risk Committee 11. Risk Communication Plan and Risk Trainings 12. ERM Risk Management Tools 13. ERM business plan presentation risk template & example of 1 completed business plan template 14. Risk assessment tools and templates for business planning
Mandates / Terms of Reference: 1. Board of Directors 2. Audit & Risk Committee 3. Compensation, Leadership & Governance Committee 4. Generation Oversight Committee 5. Executive Risk Committee 6. Chief Risk & Audit Executive
Internal Audit Documentation 1. Internal Audit Methodology (including Report & Findings Template) 2. Internal Audit Universe & Plan 3. Latest IA Reports / Findings
Enterprise Project Office 1. Mandate of the Enterprise Project Office (with organisation chart if available) 2. EPO Risk Management Standards & Methodology 3. EPO Risk Management Tools 4. Enterprise Project Management Governance Framework 5. RMO Toolkit screenshots 6. PowerBI Reports 7. Heatmap Reports

Appendix 2 — Interviewee List

Interviewee List	
Name	**Title**
Wendy Kei	Board of Directors, Chair
Ani Hotoyan-Joly	Audit & Risk Committee, Chair
Ken Hartwick	President & Chief Executive Officer
John Mauti	Chief Financial Officer & SVP, Finance
Mike Martelli	President, Renewable Generation
Sean Granville	Chief Nuclear Officer
Christopher Ginther	Chief Administrative Officer
Dietmar Reiner	SVP, Enterprise Projects
Andy Moeck	Director, Nuclear Oversight
Liane Kim	VP Assurance, Chief Risk & Audit Executive
Adam Chiarandini	Director, Enterprise Risk Management

Appendix 3 — Classification of Internal Audit Findings

The following framework for internal audit ratings has been aligned with OPG for prioritising internal audit findings according to their relative significance depending on their impact to the process. The individual internal audit findings contained in this report have been discussed and rated with Management.

	Safety & Social License	Financial	Operational Excellence
High Risk	Potential regulatory non-compliance. Deficiencies that could result in: • Fatality, permanent disability, or lost time injury; • Data loss or unavailability of critical systems; • Security is compromised in sensitive / multiple areas; or • Fraud / theft.	Potential loss or financial impact =>5% of the sample population's value, or the department's OM&A budget if the former is unavailable.	Governance non-compliance or lack of/inadequate controls that may impact achievement of business or project objectives. Errors in or insufficient internal reporting that drives senior management decision making. Test results where =>25% of the sample had deficiencies in the execution of a key control.
Moderate Risk	Insufficient evidence to support regulatory compliance. Deficiencies that could result in: • Minor injury with no lost time; • Temporary data loss or unavailability of non-critical systems; • Security is compromised; or • Fraud / theft with some mitigating controls.	Potential loss or financial impact >=2% and <5% of the sample population's value, or department's OM&A budget if the former is unavailable.	Governance non-compliance or lack of/inadequate controls with alternate controls in place to mitigate the impact to business or project objectives. Errors in or insufficient internal reporting that could affect management decision. Test results where >=10% and <25% of the sample had deficiencies in the execution of a key control.
Low Risk	Documentation improvements to support regulatory compliance. Deficiencies that could result in incidents that do not require medical treatment.	Potential loss or financial impact <2% of the sample population's value, or department's OM&A budget if the former is unavailable.	Governance compliance with procedural concerns or documentation issues which could impact OPG's ability to demonstrate appropriate due diligence. Errors in or insufficient internal reporting that has minimal decision making impact.

			Test results where <10% of the sample had deficiencies in the execution of a key control.
Opportunity for Improvement	Observation with no risk impact that is provided to management for consideration to improve efficiency of processes and documentation (e.g. automation, duplication of activities).		

Our overall rating for the internal audit project is based on the nature and type of findings identified within the scope, approach and agreed procedures. These ratings have been discussed with Management. The overall rating should be considered in conjunction with the classification of internal audit findings.

An overall audit rating is assigned based on the number of observations identified for the audit and their assigned risk rating.

	Number of Findings			
Finding Risk Rating	**1**	**2**	**3 – 4**	**>5**
High	**Requires Improvement**	**Not Effective**	**Not Effective**	**Not Effective**
Moderate	**Generally Effective**	**Generally Effective**	**Requires Improvement**	**Not Effective**
Low	**Effective**	**Effective**	**Generally Effective**	**Requires Improvement**

Appendix 4 — Disclaimer

Though we endeavor to provide accurate and timely information at the time of review, there can be no guarantee that such information will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG was not engaged to perform an audit, review, or compilation of financial statements or financial information and, accordingly, it expresses no opinion or other form of assurance on financial statements or financial information. Furthermore, KPMG was not engaged or qualified to conduct and has not conducted any legal analysis or to provide any legal conclusions, opinions, or advice. In conducting this assessment, KPMG made subjective judgments in a variety of areas relating to legal, regulatory, and financial services industry standards. These judgments are based on relevant laws and regulations, and on KPMG's knowledge and experience in understanding relevant guidance. There is no guarantee, however, that KPMG's views will be consistent with those of regulators and, therefore, KPMG makes no representation in this regard. During the course of the assessment, KPMG was provided with various documents and explanations. If further documentation or explanations come to light after the issuance of our report, KPMG reserves the right to, but is not obligated to, amend its observations and, recommendations or considerations for enhancement.

The observations and recommendations of KPMG as presented in this report are based on the procedures performed as described above, and on the information supplied by OPG, its management and officers, or employees, and on the analysis of relevant documents that we relied upon, which were provided at the time of our request. Were KPMG to perform expanded procedures, or should the information that had been provided to KPMG be inaccurate for any reason, it is possible that our assessment and observations would be different. OPG is solely responsible for identifying any remedial actions that may be appropriate to address any compliance gaps.

Our report is intended for the use of the Board of Directors and management of OPG. Other than the above noted distribution and use of our reports, they are not to be published, circulated, reproduced or used for any purpose without our prior written permission in each specific instance. We do not assume any responsibility or liability for any costs, damages, losses, liabilities or expenses incurred by OPG as a result of circulation, publication, reproduction, use of or reliance upon our report, other than as outlined above. We do not assume any responsibility or liability for any costs, damages, losses, liabilities or expenses incurred by anyone else as a result of circulation, publication, reproduction, use of or reliance upon our report.

Contact us:

Edouard Bertin-Mourot
Engagement Partner
(416) 777 3543
edouardbertinmourot@kpmg.ca

Peter Heimler
Engagement Director
(416) 777 3509
pheimler@kpmg.ca

Matt Sivakumar
Senior Consultant
(416) 228 4541
msivakumar@kpmg.ca

www.kpmg.ca

kpmg.com/socialmedia

© 2018 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.