Internal Audit

Bruce Power Ring Fence Audit

February 12, 2019

Report Rating: **Effective**

Table of Contents

1.0 EXECUTIVE SUMMARY

1.1 Report Rating and Summary of Findings

Report Rating: **Effective**

There were no findings noted during the audit.

1.2 Background

Bruce Power leases and operates an OPG owned, eight-unit nuclear power plant in Kincardine, Ontario. Unauthorized circulation of non-public, commercially sensitive information (i.e. outage information) on the Bruce site with individuals in selected groups at OPG (e.g. Energy Markets) could potentially create an unfair market advantage. In compliance with OPG's Electricity Generation License conditions, OPG has committed to protecting commercially sensitive information at the Bruce site through a system of internal controls, referred to as a "Ring Fence".

As part of the ongoing commitment to the Ontario Energy Board (OEB), Internal Audit ("IA") conducts audits of the Ring Fence program every two years, and reports results to the OPG Board and the OEB. The result of the last audit conducted by IA in January 2017 was "EFFECTIVE", confirming that OPG's management and staff had complied with the Ring Fence control program requirements, and there were no findings noted during that audit.

1.3 Objective & Scope

The objective of this audit was to independently assess whether OPG had complied with the Ring Fence plan requirements since the last audit completed in January 2017. IA also evaluated changes (if any), that were made to the Ring Fence plan during the audit period, and determined if such changes were appropriate and implemented effectively.

In order to achieve the audit objective, we reviewed the process and tested, on a sample basis, the following:

A. Governance Program
• An adequate governance program was established to define, implement and monitor Ring Fence requirements; • Appropriate training and awareness programs were established to ensure that employees and contractors within the Ring Fence clearly understand applicable rules and restrictions; • Individuals authorized to possess ring-fenced information were identified and restricted on a need-to-know basis; and • Roles with potential conflict of interest were prohibited from the authorized staff list.

B. Logical Access and Security

• Appropriate system access controls were in place to avoid unauthorized access to ring-fenced information including:
  ○ centralized request tracking and approval;
  ○ logging of changes;
  ○ defined and restricted shared folders;
  ○ password protection; and
• User access was removed in a timely manner based on termination of employment or change in employee role.

C. Physical Access and Security
• Appropriate physical access controls were in place to avoid unauthorized access to ring-fenced information including locked rooms and cabinets; • The use and movement of protected documents in restricted areas was appropriately monitored; and • General “clean desk” policies were applied by OPG staff responsible for Ring Fence administration.
D. Classification, Receipt, Release and Disposal of Ring-Fenced Information
• Relevant documentation was tagged and stored according to its applicability to the Ring Fence program; • Information requests were consistently routed and centralized through the OPG single point of contact; and • User authority was regularly validated by the Record Centre and Record Custodians; and
E. Non-Compliance Handling Procedures – Investigation, Escalation and Consequence
• Incident reporting, management and escalation procedures were in place to follow up and correct potential non-compliance; and • Confirmed violations are monitored and investigated through a defined mechanism by the Ring Fence Executive Sponsor and Chief Ethics Officer.
F. Fraud Risk Considerations
• Commercially sensitive ring-fenced information was exposed to and used by unauthorized individuals / departments within OPG to gain unfair competitive advantage.

Scope Period: The scope included activities from January 1, 2017 to December 31, 2018.

1.4 Conclusion

OPG management and staff have complied with the Ring Fence control program requirements. A well-defined program continues to be in place which articulates the requirements set out in the Plan; and key stakeholders were knowledgeable on the Ring Fence requirements, purpose, and key controls.

There were no findings noted during the audit.

APPENDIX A – RISK RATING DEFINITIONS FOR AUDIT FINDINGS

Ratings are derived through professional judgment by the audit team and discussion with management. The ratings for individual control findings are outlined below.

Rating	Definition
High Risk	The finding results in levels of risk exposure for the organization that, if not mitigated, could have a potentially severe/major impact on safety, project excellence, operational excellence and reliability, regulatory compliance, social license, environment, or financial results. The finding requires immediate attention.
Moderate Risk	The finding presents a risk that could potentially have a moderate impact on safety, project excellence, operational excellence and reliability, regulatory compliance, social license, environment, or financial results. If not remediated, the risk could escalate.
Low Risk	The finding could potentially have a minor impact on safety, project excellence, operational excellence and reliability, regulatory compliance, social license, environment, or financial results. Implementation of the recommendation may lead to improvement in the quality and/or efficiency of the area or process being audited.

OVERALL REPORT RATING SCALE

An overall report rating has been assigned as an indication of the overall design, existence and effectiveness of the components of the internal control structure that was subject to the internal audit. The internal audit rating should be considered in conjunction with the definitions noted above.

- *Effective:* control and risk management practices provide reasonable assurance that business process objectives will be achieved and may include minor improvements and/or opportunities for improvement.
- *Generally Effective*: control and risk management practices require more than minor but less than significant improvements to provide reasonable assurance that business process objectives will be achieved.
- *Requires Improvement*: control and risk management practices require significant improvements in high risk and/or core areas to provide reasonable assurance that business process objectives will be achieved.
- *Not Effective:* control and risk management practices are not designed and/or are not operating effectively.

APPENDIX B – PROCESS OWNER & DISTRIBUTION LIST

Distribution:

Chris Ginther
Chief Administrative Officer

Ian Roberts
Chief Information Officer

cc:	Jeff Lyash	President & Chief Executive Officer
	Ken Hartwick	CFO and SVP Finance
	Brenda MacDonald	VP Regulatory Affairs
	Adam Chiarandini	Director Enterprise Risk Management
	Janice Ding	Director Internal Audit
	Shelley Tucker	Director Info Management Services
	Karen Cooke	Manager Regulatory Affairs
	Richard Collyer	Section Head Governance