
Internal Audit

Bruce Power Ring Fence Audit

February 8, 2017

Report Rating: **Effective**

Distribution:

Ken Hartwick

Senior Vice-President Finance, Strategy, Risk
& CFO

Chris Ginther

Chief Administrative Officer

Ian Roberts

Chief Information Officer

cc: Jeff Lyash	President & Chief Executive Officer
Chris Fralick	Vice-President Regulatory Affairs
Janice Ding	Director Internal Audit
Bosco Yuan	Acting Director Controllershship and Finance Controller
Kim Kotyk	Senior Manager, Enterprise Risk Management
Shujat Omer	Senior Manager, IT Audit
Shelley Tucker	Senior Manager, Information Management and Program Authority
Steven Troup	Section Head Governance and Services

Table of Contents

1.0	EXECUTIVE SUMMARY	3
1.1	Report Rating and Summary of Findings	3
1.2	Background	3
1.3	Objective & Scope.....	3
1.4	Conclusion	5
	APPENDIX A – RISK RATING DEFINITIONS FOR AUDIT FINDINGS	6

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) will conduct audits of the Ring Fence program every two years with results reported to OPG Board and the OEB.

1.3 Objective & Scope

The objective of this audit was to independently assess whether OPG has complied with the Ring Fence Plan ("Plan") requirements since the last audit completed in March 2015. IA also evaluated changes made to the Ring Fence plan during the audit period and determined that changes were appropriate and implemented effectively. Substantive testing was performed on the authorized staff list for confirmation of employment status, access authorization and appropriateness of their role to access Ring Fence information.

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

A Governance Program
<ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> Appropriate system access controls were in place to avoid unauthorized access to ring-fenced information including: <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Appropriate physical access controls were in place to avoid unauthorized access to ring-fenced information including locked rooms and cabinets; Appropriate monitoring of the use and movement of protected documents in restricted areas was applied; 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 <ul style="list-style-type: none"> Relevant documentation was classified and stored according to its applicability to the Ring Fence program; Centralization of information requests were consistently routed through the OPG single point of contact; User authority was regularly validated by the Record Centre and Record Custodians; and Release and disposal of information is in accordance to the Ring Fence program.
E Non-Compliance Handling Procedures – Investigation, Escalation and Consequence <ul style="list-style-type: none"> Incident reporting, management and escalation procedures were in place to follow up and correct potential non-compliance; and Monitoring and investigation was performed through a defined mechanism.
F Fraud Risk Considerations <p>Commercially sensitive ring-fenced information exposed to and used by unauthorized individuals / departments within OPG to gain unfair competitive advantage.</p>

Scope Period: The scope included activities from April 1, 2015 to December 31, 2016.

1.4 Conclusion

OPG management and staff have complied with the Ring Fence control program requirements.

Positive Observations

- A well-defined program is 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.

Findings & Recommendations

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 presents a risk that could potentially have severe/major impact on financial sustainability ($\geq \$5M$), operational excellence, project excellence, safety, environment and reliability, reputation, regulatory relationship, or compliance with laws and regulations.
Moderate Risk	The finding presents a risk that could potentially have a moderate impact on financial sustainability (\$500K to $< \$5M$), operational excellence, project excellence, safety, environment and reliability, reputation, regulatory relationship, or compliance with laws and regulations. If not remediated, this risk could escalate to high risk.
Low Risk	The finding could potentially have a minor impact on financial sustainability ($< \$500K$), operational excellence, project excellence, safety, environment and reliability, reputation, regulatory relationship, or compliance with laws and regulations. Recurring “low risk” findings may be elevated to medium risk status.

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.