



Internal Audit

Bruce Power Ring Fence Audit

March 2013

Distribution:

Chris Ginther, Senior Vice-President, Law & General Counsel

cc: Tom Mitchell
Bruce Boland
Donn Harbidge
Carlo Crozzoli
Jong Kim
Colin Anderson
Jody Hamade
Rosemary Watson

Table of Contents

1.0 EXECUTIVE SUMMARY1

2.0 BACKGROUND2

3.0 AUDIT OBJECTIVES AND SCOPE2

APPENDIX A

1.0 EXECUTIVE SUMMARY

Audit Rating¹:	Generally Adequate
Enterprise Level Impact:	Low

Internal Audit (IA) has completed the Bruce Power Ring Fence Audit as part of OPG's ongoing commitment to the Ontario Energy Board (OEB). The purpose of this audit was to independently assess OPG's compliance with the established requirements of the Ring Fence plan (the "Plan") since the last audit completed in March 2011. IA also evaluated the design and implementation of significant changes made to the Plan, if any, during this time period.

Throughout the audit, key stakeholders have demonstrated a high level of awareness of the confidentiality nature of Bruce Power information. The ring-fence program received consistent and visible executive sponsorship, which helped set the right tone at the top. A rigorous training program was established to educate employees on the principles and requirements of the ring-fence program, and structured escalation procedures were in place to enable the formal reporting and timely resolution of potential issues.

The audit identified two key findings concerning the timeliness of ring-fence membership and system access maintenance respectively. While the existing ring-fence program had established periodic reviewing requirements to address these areas of concerns, audit test results revealed that the required control activities had not been performed consistently. Going forward, stronger enforcement of periodic reviews over ring-fence membership and system access is required to prevent the reoccurrence of similar exceptions. Our review did not identify any instances of inappropriate use of information resulting from these exceptions, and none of the involved individuals had transferred to "sensitive" market operations roles during the audit period.

Key inspection and maintenance service agreements between Bruce Power and OPG officially terminated in June 2011. As a result, OPG had limited access to commercially sensitive Bruce Power information in the period of the audit. Taking into account the organization's reduced access to current commercial information, the nature of the findings and the strengths noted in other key components of the ring-fence program as mentioned above, enterprise-level impact of the audit results was assessed to be low.

These findings have been reviewed with management and they have committed to specific action plans to address these findings. Please see Section 4.0 for specific details of the above findings along with the associated risk impact, audit recommendations and management action plans.

IA would like to take this opportunity to thank all those who were involved their assistance and co-operation during this audit.

Approved By:



Lou Pollieri
VP & Chief Audit Executive

¹ Please see Appendix A for ratings definition

2.0 BACKGROUND

The exchange of certain commercially sensitive information (i.e., BP outage information not already in the public domain and unit condition information) between the two companies could raise issues relating to OPG's Electricity Generation License and general competition compliance. Accordingly, and in compliance with OPG's Electricity Generation License conditions, OPG has committed to a system of internal controls to limit access to this information. This system of controls is referred to as a "Ring Fence".

As part of OPG's ongoing commitment to the Ontario Energy Board (OEB), IA will conduct bi-annual audits of the Ring Fence plan with results reported to OPG Board and the OEB.

3.0 AUDIT OBJECTIVES AND SCOPE

The objective of this audit is to independently assess whether OPG has complied with the Ring Fence plan requirements since the last audit completed in March 2011. IA will also evaluate changes made to the Ring Fence plan during the audit period, if any, and determine if changes were appropriate and implemented effectively.

Key plan components that IA will include in the audit scope are outlined below:

- Ring Fence program and governing documents
- Roles and accountabilities
- Training program
- Logical and physical security over ring-fenced information
- Classification, receipt, release and disposal of ring-fenced information
- Non-compliance handling procedures – investigation, escalation and consequence

Bruce Power Ring Fence Audit

4.0 AUDIT FINDINGS

#	Finding	Process Risk Rating	Recommendation	Management Action Plan
4.1	<p>System Contacts had not enforced access controls over ring-fenced systems in a consistent manner.</p> <p>System Contacts are assigned the responsibility to enforce proper controls over ring-fenced systems to restrict access to authorized Bruce Power Ring-Fence ("BPRF") Staff List members only. However, IA noted exceptions in four of the ring-fenced systems sampled when examining the user access reports of these systems. The following provides details of the exceptions and their causes:</p> <ul style="list-style-type: none"> IMS Network Folders –exceptions were noted in three ring-fenced folders, where access was not removed for individuals who had already moved outside of the ring-fence. IA noted that quarterly access review, which would have kept access rights current, was not performed by the respective System Contacts due to insufficient understanding of / responsiveness to the process. This is a repeated issue from previous audit. Concur Expense Processor (Audit) role – System Contact had stopped validating users' ring-fence membership, as Concur did not contain any commercially sensitive Bruce Power information. The Ring-Fenced Systems List ("Systems List"), however, was not updated accordingly to reflect that. <p>IA notified relevant stakeholders of these exceptions upon identification, and noted that progress have been made since then to address the specific incidents identified above – Concur has been removed from the Systems List as appropriate, and several change requests have been submitted to update IMS network folder access. Going forward, however, an action plan needs to be developed to reinforce and monitor the completion of system-related control activities as defined in the governance.</p> <p><u>Risk Impact Analysis</u> Ring-fenced information was accessible to unauthorized individuals for use to gain competitive advantage. Impact of the</p>	High	<p>System Contacts should enforce proper access controls over ring-fenced systems, as per OPG-PROC-0002 – Section 1.6.2.</p> <p>To facilitate compliance, the Ring-Fence Administration Team should reinforce the governance requirements with System Contacts and establish a mechanism to monitor the completion of the required activities on an ongoing basis.</p> <p>Recommended actions include:</p> <ul style="list-style-type: none"> Reinforce roles and responsibilities with key stakeholders, clarify expectations and control procedures; Make arrangements with IT to have user access lists for all ring-fenced systems provided on a recurring basis; Establish an attestation process that requires System Contacts to provide confirmation on the completion of control activities, and gives the BPRF Administrator authority to escalate for lack of responses; and Monitor adverse trends for triggers of escalation. 	<p><u>Action Plan(s):</u></p> <ol style="list-style-type: none"> Identify owner for each system or folder to allow for escalation in case required. Update quarterly reminder email to require positive confirmation from System Contacts for the completion of periodic review activities (including reconciliation of user list from IT with BPRF's list), with follow-up and escalation process for lack of responses. Meet with System Contacts to reinforce expectations. <p><u>Owner:</u> BPRF Administrator</p> <p><u>Target Completion Date:</u></p> <ol style="list-style-type: none"> March 15, 2013 – Complete. March 15, 2013 – Complete. <i>Note: to be validated by IA by June 15, 2013.</i> May 15, 2013

Bruce Power Ring Fence Audit

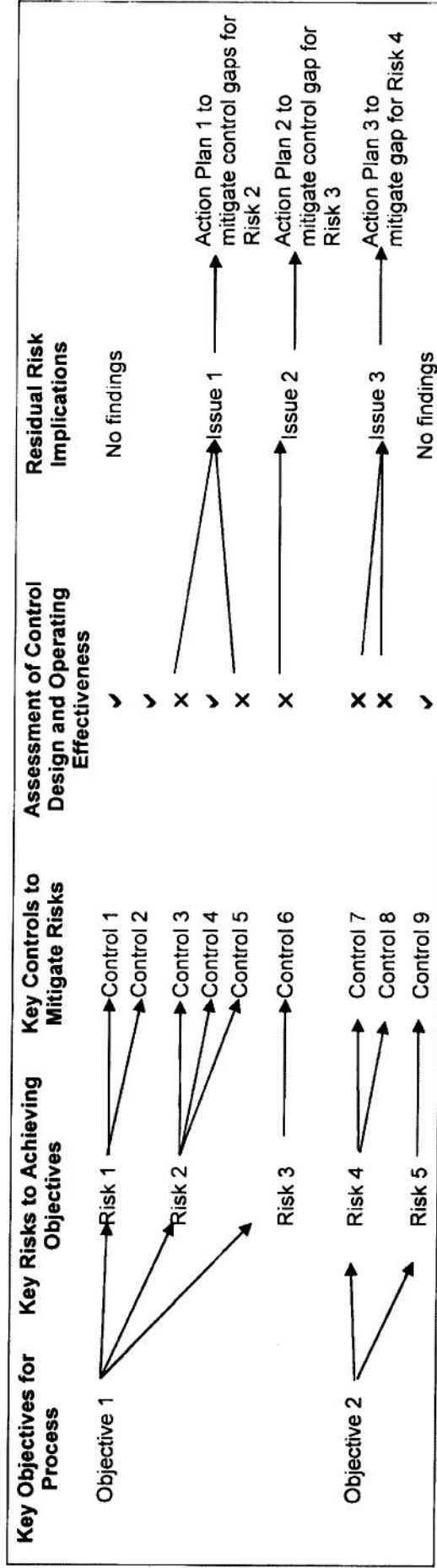
#	Finding	Process Risk Rating	Recommendation	Management Action Plan
	<p>finding was significantly reduced, however, due to the following mitigating circumstances noted:</p> <ul style="list-style-type: none"> • One of the exceptions pertained to Concur, a system that no longer contains ring-fenced information. • For the three IMS network folders, IA further analyzed the exceptions and noted that: <ul style="list-style-type: none"> i. A number of exceptions were associated with terminated / retired employees. No ring-fence risk, as network access of these individuals would have been revoked upon termination under the existing IT process. ii. Among the active employees, none have been transferred to roles / departments that could benefit from commercially sensitive Bruce Power information (i.e., Commercial Operations' Front Office). 			
4.2	<p>The Bruce Power Ring-Fence Staff List was not updated to reflect necessary membership changes in a timely manner.</p> <p>The BPRF Staff List ("Staff List") is a list of individuals authorized to access ring-fenced information due to their job functions, and should be kept current with changes in staffing and individual job responsibilities. From HR's 2011-2012 staff change records, IA selected 25 changes concerning ring-fenced job positions and noted eight exceptions where the Staff List was not updated within the established timeframe. As per governance, designated Group Contacts are required to examine staff changes and report necessary Staff List updates to the BPRF Administrator within 30 days upon receipt of reminder at a minimum.</p> <p>IA acknowledged that the BPRF Administrator had self-identified the timeliness issue with Staff List maintenance, and had documented, investigated, corrected and reported the noted exceptions in accordance with governance procedure. Going forward, the BPRF Administration team should continue its effort in reinforcing and monitoring the timely completion of monthly review as defined in the governance.</p> <p><u>Risk Impact Analysis</u> Ring-fenced information was accessible to unauthorized individuals for use to gain competitive advantage. Impact of the finding was significantly reduced, however, due to the following</p>	Medium	<p>Group Contacts should perform the required monthly Staff List review, as per OPG-PROC-0002 – Section 1.6.1.</p> <p>To facilitate compliance, the Ring-Fence Administration Team should reinforce the governance requirements with Group Contacts and establish a mechanism to monitor the completion of the required activities on an ongoing basis.</p> <p>Recommended actions include:</p> <ul style="list-style-type: none"> • Reinforce roles and responsibilities with key stakeholders, clarify expectations and control procedures; • Establish an attestation process that requires Group Contacts to provide confirmation on the completion of control activities, and allows the BPRF Administrator to escalate for lack of responses; and • Monitor adverse trends for triggers of escalation. 	<p><u>Action Plan(s):</u></p> <ol style="list-style-type: none"> 1. Update monthly reminder email to require response from Group Contacts even if there were no changes, with defined follow-up and escalation process 2. Clearly define and communicate Roles & Accountabilities in a face to face meeting. <p><u>Owner:</u> BPRF Administrator</p> <p><u>Target Completion Date:</u></p> <ol style="list-style-type: none"> 1. March 15, 2013 – Complete. <i>Note: to be validated by IA by June 15, 2013.</i> 2. December 31, 2012 – Complete.

Bruce Power Ring Fence Audit

#	Finding	Process Risk Rating	Recommendation	Management Action Plan
	<p>mitigating circumstances noted:</p> <ul style="list-style-type: none"> • The BPRF Administrator had a feedback mechanism and an established set of issue handling procedures to identify and correct these exceptions. • Further analysis of the exceptions revealed that all individuals in question had completed the comprehensive ring-fenced training in a timely manner – annually before exiting the ring-fence, or within two weeks upon employment status change for those new to the ring-fence. Their awareness of the ring-fence rules reduces the likelihood of them committing violated acts. 			

**APPENDIX A
OVERVIEW OF AUDIT RATING METHODOLOGY**

IA's ratings for operational audits of OPG business processes are derived from an assessment of the management controls that are in place to mitigate key risks to the achievement of process objectives. The diagram below illustrates IA's basic approach to conducting an audit. If control deficiencies are identified that prevent IA from providing reasonable assurance that the process objective will be met (i.e. key risks are adequately mitigated), an audit issue will be noted and a corrective action plan from management will be required.



The ratings for the audit will be assigned based on a two-tiered assessment of residual risk exposure. The first tier rating assesses the residual risk at the local, process level and is guided by an evaluation of the 5 interrelated components of control, as defined by the COSO Internal Control Framework (i.e. control environment, risk assessment, control activities, information and communication, monitoring). This results in one of the following audit opinions:

- **Not Adequate:** a management control system is not in place or not operating effectively.
- ▲ **Generally Adequate:** sufficient controls are in place and generally operating effectively with some improvements required.
- **Adequate:** an appropriate management control system is in place and operating effectively.

The second tier to IA's audit rating is an indication of the implications of the residual risk at the broader, enterprise level. This rating of "High", "Moderate" or "Low" is intended to answer the "so what?" question for senior management and the Audit and Finance Committee by giving context to audit results in terms of their impact on OPG as a whole.