Internal Audit

Bruce Power Ring Fence Audit

March 19, 2021

Report Rating: **Generally Effective**

© Ontario Power Generation Inc., 2021. This document has been produced and distributed for internal 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

1.0 EXECUTIVE SUMMARY

1.1 Report Rating and Summary of Findings

Report Rating: **Generally Effective**

No.	Finding	Risk Type	Risk Rating[1]		
			High	Moderate	Low
1	Two individuals were not removed from the Ring Fence Staff List after joining the Energy Markets team.	Operational		X	
2	System access reviews were not performed for Curator and Documentum for 2019.	Operational			X
Total		**2**	**-**	**1**	**1**

1.2 Background

Bruce Power leases and operates an OPG-owned, eight-unit nuclear power plant in Kincardine, Ontario. Unauthorized circulation of commercially sensitive information (which consists of Bruce Power outage information not already in the public domain and unit condition information only) with individuals in select groups at OPG could potentially create an unfair market advantage. In compliance with Part 6 of OPG's Electricity Generation Licence, OPG has committed to protecting commercially sensitive information of Bruce Power (as indicated above) through a system of internal controls, referred to as a "Ring Fence".

As part of the ongoing commitment to the Ontario Energy Board ("OEB"), and in accordance with Part 6 of OPG's Electricity Generation Licence, Internal Audit ("IA") conducts an audit of the Bruce Power Ring Fence ("BPRF") program every two years, and reports results to the OPG Board of Directors through the Audit and Risk Committee. Reports are also made available to the OEB.

1.3 Objective & Scope

The objective of this audit was to independently assess whether OPG had complied with the BPRF plan (the "Plan") requirements since the last audit completed in Q1 2019. IA also evaluated changes that were made to the Plan during the audit period, and determined if such changes were appropriate and implemented effectively. To achieve the audit objective, we reviewed processes and tested, on a sample basis, whether:

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 understood 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.

[1] Please refer to Appendix A for risk rating definitions

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 BPRF administration.

D. Classification, receipt, release and disposal of ring-fenced information

- Relevant documentation was tagged and stored according to its applicability to the BPRF 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.

E. Non-compliance handling procedures – investigation, escalation and consequence

- Incident reporting, management and escalation procedures existed to follow up and correct potential non-compliance; and
- Confirmed violations were monitored and investigated through a defined mechanism by the BPRF 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 between January 1, 2019 and December 31, 2020.

1.4 Conclusion

OPG management and staff have generally complied with the Plan. A well-defined program continues to be in place which reflects the requirements set out in the Plan. Key stakeholders were knowledgeable on the BPRF requirements, purpose, and key controls.

Positive observations

- Management has taken the initiative to begin implementation of a number of future improvements to the process including automation. These improvements include:
  - Consolidating the storage of electronic ring-fenced information to a single location, facilitating monitoring and streamlining access control administration;
  - Requiring individuals to have completed the required BPRF training within the three years prior to being added to the BPRF Staff List (previously there was no timeline requirement);
  - Removing individuals from the BPRF Staff List automatically on expiry of the associated training qualification; and
  - Automating the approval process for changes to the BPRF Staff List by using the IT Service Centre Wizard to route approvals and manage approval documentation.

- Due to space limitations at OPG's 700 University head office, legacy hardcopy BPRF documents were moved to OPG's Western Waste Management Facility. Despite COVID-19 pandemic restrictions, IA noted BPRF documents were managed in a secure manner during the move which was supervised by two OPG employees. Boxes of records were inventoried prior to shipment, accounted for at the receiving location, and placed in locked filing cabinets at the permanent storage location.

Key Findings & Recommendations

- Two employees were not removed from the BPRF Staff List in a timely manner after joining the OPG Energy Markets ("EM") team from elsewhere in the organization, one of whom was in a trading role. Neither employee was noted as having inappropriately accessed ring-fenced information. In addition, for the employee that assumed a trading role, no anomalous trading activity was noted. The onboarding process for individuals moving to the EM team from other OPG groups should be updated to include confirmation that they are not on the BPRF Staff List; and

- Following a transition to a new system storing BPRF information, system access reviews were not performed between January 2019 and February 2020 for the two systems (Curator and Documentum) that stored BPRF information, in accordance with OPG Governance established in response to the recognized risks. IA noted that system access for a former BPRF Coordinator, who had transferred to a role that did not require access to BPRF information, was not revoked from Documentum until February 2020; however, it was noted that the individual had not accessed the system after being removed from the BPRF Staff List upon her move in January 2019. Management should ensure access reviews for BPRF systems are performed on a quarterly basis.

The findings noted in this report have been reviewed with management and they have committed to specific action plans. Please refer to Section 2.0 for specific details of the above findings along with the associated risk impacts, audit recommendations and management action plans.

2.0 DETAILED AUDIT FINDINGS

Internal Audit identified the following detailed findings and recommendations which have been risk rated based on the definitions outlined in Appendix A.

1. Two individuals were not removed from the Ring Fence Staff List after joining the Energy Markets team.

Moderate

The BPRF Staff List is an administrative list of individuals who require access to BPRF information for the performance of their duties, maintained by the BPRF Administrator. Being on the BPRF Staff List indicates completion of required training, an understanding of the need to protect ring-fenced information, and being in a role in which one may encounter BPRF information in the course of performing their duties. The list is used as a reference to support requests for BPRF information made to the BPRF Administrator.

Some EM Front Office roles (i.e. positions which engage in or support market transactions) could be in a position to use BPRF information in energy pricing decisions. In response to this risk, OPG-PROC-0002 “Bruce Power Ring-Fenced Information” notes that EM Front Office staff are restricted from access to ring-fenced information and therefore should not be on the BPRF Staff List.

On a monthly basis, a list of EM Front Office staff (“EM Staff List”) is sent to the BPRF Coordinator to be published on the BPRF Intranet page. Two of 98 employees appearing across the 24 monthly EM Staff Lists during the audit period were identified as being on the BPRF Staff List while also in an EM Front Office role. As at the date of this report, both employees had either been removed from the BPRF Staff List, or left the EM team.

- One individual, on the BPRF Staff List beginning September 28, 2017, joined the EM Front Office team on July 12, 2018 from Regulatory Finance. After repeating the BPRF training on October 13, 2019, the individual submitted a request to remove himself from the BPRF Staff List (overlap of 15 months). In assessing the potential risk of inappropriate use of BPRF information, the following was noted:
  - Although the individual was in a trading role, access to Regulatory Finance information was revoked by his previous supervisor, prior to his transfer to the EM Front Office.
  - A review of the individual’s trading activity during the overlap period revealed no anomalous trades.
  - IA confirmed that the individual had no system access to Documentum or Curator, the official repositories for BPRF information, during the overlap period.

- Another individual, on the BPRF Staff List beginning March 25, 2019, was on rotation from Nuclear Engineering to the EM Front Office team between June 8, 2020 and September 10, 2020 (3 months). The individual has since been removed from the BPRF list, as his current role did not require access to BPRF information. In assessing the potential risk of inappropriate use of BPRF information, the following was noted:
  - The individual’s supervisor in the EM Front Office confirmed that his role was limited to long term market research, and the individual had no energy trading responsibilities. Physical distancing and work-from-home requirements due to the COVID-19 pandemic also resulted in the individual not being co-located with the trading team, which further limited any potential for inadvertent transmission of BPRF information.
  - The supervisor from the employee’s base organization in Nuclear Engineering confirmed that none of the systems and folders to which he had access contained any BPRF information.
  - IA confirmed that the individual had no system access to Documentum or Curator, the official repositories for BPRF information.

Potential Causes & Impact

Potential Causes:

For individuals who move to the EM Front Office from elsewhere in the organization, there is no check performed as part of the onboarding process to consider the individual's BPRF Staff List status. The absence of this automatic check places greater burden on individual supervisor accountability for removing individuals on the BPRF Staff List prior to commencing a role within the EM team. For the observed instances above, potential causes include:

- Prior supervisor overlooked removal of the individual from the BPRF Staff List when the individual moved to EM Front Office; and
- The sending department Group Contact was not made aware of the required change to the Staff List as part of the monthly review process, which requires Group Contacts to confirm the ongoing applicability of BPRF Staff List status for individuals within their department.

Potential Impact:

Although the two individuals were not provided with access to BPRF information, since they remained on the BPRF Staff List they could have requested and been provided with BPRF information. No electronic access is enabled by being on the BPRF Staff List.

Recommendation

Given the inherent risk associated with the potential misuse of commercially sensitive information by the Energy Markets group, it is recommended that the EM Team's onboarding process for individuals moving to the EM team from other OPG groups should be updated to include confirmation that:

- They are not on the BPRF Staff List; and
- They no longer have access to BPRF information prior to commencing a role within EM.

Management Action Plan

Energy Markets management will implement an onboarding check to ensure that individuals joining the EM team from other OPG groups are not on the BPRF staff list, and that the individual no longer has access to BPRF information.

Owner: Nick Pender, VP Energy Markets
Target Completion Date: March 31, 2021

2. System access reviews were not performed for Curator and Documentum for 2019.

Low

OPG-PROC-0002 “Bruce Power Ring-Fenced Information” requires that System Contacts, who are individuals responsible for access to electronic storage locations of BPRF information, perform a quarterly access review of BPRF systems, and confirm completion of the access review by email, identifying the list of current system users.

Electronic access to BPRF documentation is restricted to fewer than 20 individuals, responsible for maintaining those documents.

Due to the management initiative to consolidate the storage of electronic BPRF documents, documents were copied from Curator to Documentum, as of June 2018. BPRF information also remained in Curator until the system was decommissioned in July 2019, and access was restricted to only two individuals involved in the document migration project.

Although BPRF information existed in both systems in 2019, there was no evidence that the required quarterly access review was performed for:

- Curator, between January 18, 2019 and when it was decommissioned in July 2019; or
- Documentum, between January 18, 2019 and February 11, 2020.

Access to Documentum was reviewed in February 2020, and one individual was identified as having access despite having been removed from the BPRF Staff List. The individual was removed from the BPRF Staff List in January 2019 as they had transitioned into another role in OPG that did not require access to BPRF information. A review of system activity logs confirmed that the individual had not accessed Documentum after being removed from the BPRF Staff List.

Quarterly access reviews of Documentum were performed effectively through 2020 in accordance with the established governance requirements.

Potential Causes & Impact

Potential Causes:

- The required quarterly System Review Request emails were not sent out between Q1 2019 and Q1 2020 inclusive due to an assumption that access was restricted to the team carrying out the document migration. This was captured and noted in the BPRF Issues and Violations Log (#I-19-001, #I-20-004); and
- When documents were migrated from Curator to Documentum, miscommunication between the migration project team and the BPRF Coordinator led to a lack of clarity on where electronic documents were stored during the period, and who had access.

Potential Impact:

If periodic system access reviews are not conducted, any misalignment between access to electronic ring-fenced information and the BPRF Staff List may not be detected. This could lead to individuals not on the BPRF Staff List having inappropriate access to BPRF documents.

Recommendation

Management should ensure that Quarterly System Review Request emails are sent to the system owners for each system containing BPRF documentation, and that quarterly system access reviews are performed.

Management Response
All electronic ring-fenced information is now centralized to a single electronic storage location (i.e. Documentum). Quarterly reviews resumed in Q3 2020, and continue to be performed by CIO. Owner: Richard Collyer, Section Head Governance & Services Target Completion Date: Completed

APPENDIX A – RATING DEFINTIONS FOR AUDIT REPORTS

Finding: *Noted deficiency with potential impacts to the achievement of business unit/process area objectives, assessed using the following criteria:*

	High Risk	Moderate Risk	Low Risk
Safety & Social License	• Potential regulatory non-compliance. • Deficiencies that could result in: o Fatality, permanent disability, or lost time injury; o Data loss or unavailability of critical systems; o Security is compromised in sensitive / multiple areas; o Fraud / theft; or o Negative media coverage resulting in reputational damage	• Insufficient evidence to support regulatory compliance. • Deficiencies that could result in: o Minor injury with no lost time; o Temporary data loss or unavailability of non-critical systems; o Security is compromised; o Fraud / theft with some mitigating controls; or o Public escalating concerns to OPG Management or local media.	• Documentation improvements to support regulatory compliance. • Deficiencies that could result in incidents that do not require medical treatment. • Deficiencies that do not result in any media attention negatively impacting OPG's reputation.
Financial	• Potential loss or financial impact =>5% of the sample population's value, or the department's OM&A budget if the former is unavailable.	• 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.	• Potential loss or financial impact <2% of the sample population's value, or department's OM&A budget if the former is unavailable.
Operational Excellence	• 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.	• 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.	• 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).*

OVERALL REPORT RATING SCALE

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 B – PROCESS OWNER & DISTRIBUTION LIST

Distribution:

Chris Ginther
Chief Administrative Officer

Jason Wight
SVP Innovation and Chief Information Officer

cc:	Ken Hartwick	President & Chief Executive Officer
	John Mauti	SVP Finance and Chief Financial Officer
	Barbara Kerr	VP Controllership
	Brenda MacDonald	VP Regulatory Affairs
	Nicholas Pender	VP Energy Markets
	Adam Chiarandini	Director Enterprise Risk Management
	Janice Ding	Director Internal Audit
	Warren Hobbs	Director CIO Cyber Security
	Chris Woodcock	Director IT Services
	Kate Appleton	Senior Manager Infrastructure Services
	Karen Cooke	Senior Manager Regulatory Affairs
	Nancy Woodward	Senior Manager IT Program
	Richard Collyer	Section Head Governance & Services