NRC·CNRC

From Discovery to Innovation...

Science at work for Canada

National Research Council Canada

Audit of Risk Management

Internal Audit, NRC

June 2010

National Research Council Canada | Conseil national de recherches Canada

Canada

1.0 Executive Summary and Conclusion

Background

This audit report presents the findings of the National Research Council (NRC) Canada's audit of risk management. The decision to conduct this audit was approved by the President following the recommendation of the Audit, Evaluation and Risk Management Committee[1] on March 19, 2008 as part of the NRC 2008-09 to 2010-11 Risk-Based Internal Audit Plan. The audit was conducted from February 2009 to August 2009.

Audit objective, scope and methodology

The overall audit objective is to provide assurance that NRC's enterprise Risk Management Framework complies with Treasury Board *Risk Management Policy*, and associated directives and guidelines related to risk management. This objective allowed for making observations with respect to the extent to which NRC's risk management policies and directives correspond to Treasury Board requirements, and the adequacy of the risk management control framework that has been established for NRC.

The audit examined the extent to which NRC's enterprise risk management framework has been implemented and is operating at both the corporate level and within a sample of five Institutes, Branches and Programs (IBPs), including how it has been integrated into existing management activities including business planning and decision-making. The selection of the IBPs was based upon risk and control analyses performed during the planning stage of the audit, as well as to ensure that no one IBP at NRC is audited more so than others or conversely that smaller entities are ignored entirely in NRC's multi-year audit cycle. An

[1] In January 2009, this Committee of Council was replaced by the Departmental Audit Committee upon the appointment of its members by Treasury Board.

extensive review of relevant NRC documents related to risk management (e.g., corporate risk profile, corporate and IBP level business plans and the terms of reference for various governance committees) was undertaken in addition to IBP site visits and interviews with managers and staff in order to assess the degree to which risk management principles have been integrated into NRC's operations.

The audit was conducted using a series of detailed audit criteria that addressed the audit objective, against which we drew our observations, assessments, and conclusions. These audit criteria were derived primarily from the Treasury Board Integrated Risk Management Framework (2001) and the draft Office of the Comptroller General *Core Management Controls: A Guide for Internal Auditors* (2007)

Audit opinion and conclusion

Within the limitations of the samples drawn and the audit procedures performed, we conclude that overall, NRC's risk management framework is adequate[2] in that it complies with the Treasury Board *Risk Management Policy* and associated directives and guidelines. There are opportunities for continuous improvement that relate to: developing and formalizing a more comprehensive Risk Management Framework; improving the consistent application of risk management guidelines across NRC and its in-depth integration into NRC's business planning processes; and development and integration of formal control assessment processes and tools to ensure major residual risks are addressed.

NRC's risk management practices include all of the foundational elements expected of a mature, well-managed organization. A framework for risk management has been in place since 2005. The corporate risk profile is examined and updated annually; risks are considered during annual corporate

[2] See Appendix for the list of potential overall ratings.

and IBP level business planning exercises; and for most of the IBPs examined there is documented evidence that risks are taken into consideration when selecting research projects. Expectations for incorporating risk management principles are communicated and understood at the corporate and IBP levels.

NRC does not have a formally documented risk management policy. Rather the Risk Management Guide that is published on NRC's Intranet is the main documented source of its Risk Management Framework. While the Guide meets most Treasury Board expectations, it requires a more explicit and comprehensive description of all of its risk management activities and obligations including, among others, NRC's risk tolerance, a description of the governance model (i.e., accountabilities, roles and responsibilities) and guidelines for identifying and sharing risk information.

Enterprise-wide risks are assessed and treated on an annual basis as part of the annual risk profiling exercise. IBPs are required to assess and treat risk as part of annual business planning, however, the process, methods and tools that are defined in the NRC Risk Management Guide are not consistently applied by the IBPs examined. This could be enhanced by clearly cross-referencing the business planning process guide and tools to the Risk Management Guide to ensure consistent quality and communication of risk information.

Finally, NRC risk management practices could be enhanced by the introduction of a formal control assessment component as part of the risk assessment process. We observed at the corporate level and in the five IBPs examined that formal processes and guidelines for control identification and control assessment are not defined. Controls are considered when assessing the residual risk

exposure ratings assigned to corporate risks as part of the corporate risk profiling process but not consistently at the IBP level if at all.

Recommendations (as presented in order of priority)

1. NRC should develop and formally approve a comprehensive Risk Management Framework that includes all of its risk management activities and obligations including: defining senior management expectations; outlining specific roles and responsibilities for all employees, managers and committees; specifying a common approach for identifying and reporting risk information including escalation requirements and risk tolerances; identifying a strategy for knowledge transfer / employee training; and detailing the monitoring requirements of the framework to ensure continuous improvement. (High Priority)

NRC Management Response:

An overarching Risk Management Framework is critical for progress moving forward, defining clear expectations and accountabilities for IRM across NRC. To this end, SDB will take the lead in consulting with SEC and NRC senior management to draft a suitable document for their review and approval. The Risk Management Framework will clarify expectations while supporting NRC executive and management efforts to reinforce more consistent practice and understanding of IRM across the organization.

2. NRC should develop and implement a strategy to improve the application of risk management guidelines at IBPs during the business planning process to ensure consistent quality and communication of risk information. At a minimum, this should include an explicit cross referencing of the business planning guidance to the NRC's Risk Management Guide. (Moderate Priority)

NRC Management Response:

Business planning guidelines for 2010-2011 included explicit reference to the risk management resources on the intranet, which includes the risk management guide, as well as other tools. SDB will also assess, and implement as appropriate, other opportunities to strengthen IBPs' awareness of available IRM tools and resources.

3. As part of the development of the Risk Management Framework, NRC should clarify the importance of systematically identifying existing controls so that residual risks are assessed rather than just inherent risks.

NRC Management Response:

Controls are already assessed as part of the development of the Corporate Risk profile and considered in the risk prioritization process. The issue of assessing controls and residual risks will be addressed as part of developing the RM Framework from Recommendation 1

Statement of assurance

In my professional judgment as Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on a comparison of the situations as they existed at the time against the audit criteria. The evidence was gathered in accordance with the Treasury Board Policy, directives, and standards on Internal Audit, and the procedures used to meet the professional standards of the Institute of Internal Auditors[3].

_____

Jayne Hinchliff-Milne, CMA, Chief Audit Executive

NRC Audit Team Members[4]:

Irina Nikolova, F.C.C.A, CIA, CISA

[3] Although the Audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing, NRC Internal Audit has not undergone an external assessment at least once in the last five years as required.

[4] The NRC audit team was supplemented by a team of integrated risk management experts with audit expertise that were contracted to assist in conducting the audit work.

Appendix: Potential Overall Ratings

Management Attention Required – significant issues exist that require management's attention.

Needs Improvement – some areas of practices / processes are in compliance with Government of Canada and NRC policies and directives but many deficiencies exist.

Adequate – most of the areas of practices / processes are in compliance with Government of Canada and NRC policies and directives but there are opportunities for continuous improvement.

Strong – all areas of practices / processes are in compliance with Government of Canada and NRC policies and directives. No areas for improvement were identified.