March 2020

Enterprise Risk Management & Treasury Board Secretariat: A Policy Evaluation

Connor R. Lalonde
University of Windsor, lalonde4@uwindsor.ca

Enterprise Risk Management and Treasury Board Secretariat:

A Policy Evaluation

By

Connor R. Lalonde

An Internship Paper

Submitted to the Faculty of Graduate Studies

through the Department of Political Science

in Partial Fulfillment of the Requirements for

the Degree of Master of Arts

at the University of Windsor

Windsor, Ontario, Canada

2020

Enterprise Risk Management and Treasury Board Secretariat: A Policy Evaluation

by

Connor R. Lalonde

APPROVED BY:

J. Sutcliffe

Department of Political Science

W. Anderson, Advisor

Department of Political Science

December 6, 2019

DECLARATION OF ORIGINALITY

I hereby certify that I am the sole author of this internship paper and that no part of this internship has been published or submitted for publication.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my thesis and have included copies of such copyright clearances to my appendix.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

ABSTRACT

Enterprise Risk Management is the latest form of risk management. It has become an essential part of best business practices. Under the Financial Administration Act of 1985, the Treasury Board Secretariat was established to serve as the management agency for the government. Within this mandate is included best management practices. This paper examines the Treasury Board Secretariat's main risk management guidance, the *Guide to Integrated Risk Management* and how it assists government departments, agencies, and organizations in implementing Enterprise Risk Management based on key principles. This paper evaluates whether or not the *Guide to Integrated Risk Management* does a good job is outlining those principles in an effective and explicit way for public servants within the federal government.

DEDICATION

To my dad, who couldn't be here for this moment but who always supported me

ACKNOWLEDGEMENTS

This paper would not have been possible without the support of so many people. The first person I want to thank is my good friend Tyler Romualdi who encouraged me to pursue the internship stream. He was my teammate throughout this master's program and great colleague for feedback on my ideas. I would also like to thank Samantha Crebolder, Anne Mullen and the entire Windsor-Detroit Bridge Authority. The organization was great to work for and treated me as an essential part of the team. Sam and Anne were great superiors and helped me develop my skills and capabilities so much always pushing me to improve my deliverables. Finally, I want to thank my family, including my girlfriend who helped me through the tough moments when I wanted to quit.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS/SYMBOLS

British Petroleum…………………………………………………………………BP

Enterprise Risk Management…………………….…………………………….ERM

Environmental Protection Agency……………………………………………...EPA

Guide to Integrated Risk Management……………………………………….GIRM

Integrated Risk Management Implementation Guide………………………..IRMIG

Management Accountability Framework……………………………………...MAF

Office of the Comptroller General……………………………………………..OCG

Sarbanes-Oxley Act…………………………………………………………….SOX

Treasury Board Secretariat……………………………………………………...TBS

BRIEF DESCRIPTION:

Risk Management does not attract the most attention in business management, but it is an essential element for every part of any enterprise. The application of risk management to projects and organizations is relatively recent with the emergence of guidelines for the application of risk management practices and principles emerging in the last thirty or so years. It has become a major part of best practices for business management beyond project planning and financial investing.

In accordance with best management practices, the Treasury Board Secretariat (TBS) requires federal government departments and agencies to integrate risk management into their operations. This includes the most recent form of risk management, Enterprise Risk Management (ERM). The purpose of risk management and ERM more specifically is to identify and mitigate threats that a company might be exposed to, as well as identify and enhance opportunities for the company or organization. ERM seeks to apply this practice at an organization wide level including to risks that are both not aligned specifically to, or within a specific project or portfolio, but to the entire organization. This also includes risks that have impacts great enough to seriously harm the enterprise.

As the manager of federal government activities, TBS seeks to maintain proper management and best practices among government departments and agencies. For the purposes of this policy evaluation, “agencies” refers to any sub-department organization such as a government agency like Canada Border Service Agency, or crown corporation such as Windsor-Detroit Bridge Authority. The key document published by the TBS is the *Guide to Integrated Risk Management* (GIRM) which serves to instruct the reader on implementing risk management within their government organization or agency. By evaluating the *GIRM* on the key principles of ERM derived from best practices, it will be clear that TBS does not adequately inform the reader on how to establish and conduct ERM.

PROBLEMS AND ISSUES IDENTIFIED:

Risk management, and the guidelines issued by TBS are part of making sure the public service actively adheres to corporate governance and management best practices. Risk management plays an important role in helping manage the finances of organizations both on a micro scale for individual risk items and on a macro scale for items that are organization wide. Apart from best business practices, the cause for these policy guidelines from TBS was the failure and collapse of major companies and changes made to best practices in management. It was further bolstered by the failure of management in the federal government that occurred during the sponsorship scandal.

Failure of Corporate Governance and Management

The greatest example of corporate failure was the collapse of Enron. The company had a management culture that strove for the best results possible while at the same time ignored key elements of corporate governance practices that could have prevented or mitigated its collapse.[1] This includes risk management where the former Risk Manager stated that internal pressure forced employees to close deals.[2] This led risk management to fail in its responsibility to provide accurate information or act as a

[1] Ronald R. Sims and Johannes Brinkmann, "Enron Ethics (Or: Culture Matters More than Codes)" in *Journal of Business Ethics*, 45, No. 3 (July 2003): 244-245

[2] Ronald R. Sims and Johannes Brinkmann, "Enron Ethics (Or: Culture Matters More than Codes)" in *Journal of Business Ethics*, 45, No. 3 (July 2003): 252

mechanism of accountability.[3] Without this business safety mechanism, Enron's ultimately collapse resulting in billions in lost value to its customers and investors.

The guidelines for risk management within the federal government and its entities are issued by the Office of the Comptroller General (OCG). This is the main office within TBS concerned the management of the federal government agencies, departments, etc. and their requirements of risk management processes and procedures. It is directly involved, acting as the office in charge of the government's financial management, internal audit, federal assets, and acquired services. This office was originally established in 1978 but was subsumed by the TBS in 1993, only being reborn in the wake of the sponsorship scandal in 2003. Under its current mandate since its revival, the OCG is responsible for promoting and maintaining professional financial and internal auditing systems across the various departments and agencies of the federal government.[4] Part of these auditing systems is risk management. Overall, the office serves an important function within TBS's responsibility to serve as the government and public service management agency.

The Sponsorship Scandal and the Gomery Commission

As was mentioned, the OCG was revived in the wake of the sponsorship scandal. The Gomery Commission which was created in the wake of the scandal to investigate and make recommendations, made several observations that have since moved into the purview of the OCG. The Gomery Commission concluded that the sponsorship scandal resulted from insufficient oversight at very senior levels, secrecy surrounding the

[3] Robert Eli Rosen, "Risk Management and Corporate Governance: The Case of Enron," Connecticut Law Review 35, no. 3 (Spring 2003): 1160
[4] Clinton Free and Vaughn Radcliffe, "Accountability in Crisis: The Sponsorship Scandal and the Office of the Comptroller General in Canada" in *Journal of Business Ethics* 84 no. 2 (January 2009): 197

administration of the Sponsorship Program, deliberate actions to avoid compliance with federal laws, and a sense of entitlement among officials involved with the program.[5] These findings among others made clear the need to implement better management practices in the federal government. While not directly related to the sponsorship scandal, risk management and other management practices and their role in federal government agencies is still related to the effects of the scandal.

HISTORICAL CONTEXT

The field of risk management has its origins in the financial sector. Generally, a tool used by the insurance and investment industry, it was later adopted by construction and engineering as a tool of project management to prevent or limit projects from going over time and over budget, and managing project contingencies. As it became more common on projects in various fields, risk management and its practices and principles eventually became applied to organizations and enterprises. This is known as Enterprise Risk Management.

Risk management's earliest forms emerged in the 1950s as certain business risks were too costly or out-right impossible to insure. This evolved to include scenario planning in the 1960s, an essential element of risk management today. While all this was developing in the business sector, the engineering sector was developing technological risk management models for their projects.[6] Risk Management is part of internal systems of control whether it be business risk where the practice aims limit unforeseen liability, project risk where it aims to limit schedule and cost increases, or enterprise risk which

---

[5] Commission of Inquiry into the Sponsorship Program and Advertising Activities, "Major Findings" (2005): 5-7.

[6] Georges Dionne, "Risk Management: History, Definition, and Critique," in *Risk Management and Insurance Review* 16 no. 2 (2013): 147-148

seeks to limit threats to the organization. Thus, Risk Management is conducted through internal procedures as outlined within the organization and its structure based on the type of industry it operates in.

Government Guidelines for Risk Management

In the past few decades governments and their institutions have issued guidelines and mandated risk reporting for various departments and organizations both in the public sector among government agencies and departments, as well as for publicly traded companies. Examples come from across the globe but three prominent cases are the guidelines from the Government of the United Kingdom through Her Majesty's Treasury, the Australian government through the Ministry of Finance, and via the TBS for the Canadian federal government, in addition to the development of ISO 31000 by the International Organization for Standardization.[7] Each of these guidelines endorses the concept of ERM, which applies the procedures and methodologies or risk management at an organizational wide level. The guidelines issued become essential parts of government management procedures and how their departments and agencies are managed.

ERM being the newest field of Risk Management (after financial/business and project risk management) has become increasingly important in the field of corporate governance. Publicly traded companies, government agencies, and crown corporations have been implementing ERM into their more traditional risk management strategies and structures. ERM expands these pre-existing pieces of management and business; and implements company, organizational, institutional, or enterprise wide cultures of

[7] She-I Chang, Shi-Ming Huang, Jinsheng Roan, I-Cheng Chang and Pu-Jui Liu, "Developing a risk management assessment framework for public administration in Taiwan" in *Risk Management* 16 no. 3 (Aug. 2014): 165

managing risk both for issues that affect the company as a whole but also as a part of practice by employees and managers.

The TBS issued its first guidelines for Risk Management in 2001 with the *Integrated Risk Management Framework* followed by the *Integrated Risk Management Implementation Guide* in 2004. These two documents were intended to work in tandem to developed appropriate Risk Management procedures and structures among federal government entities. These documents have subsequently been replaced in 2010 by the *Framework for the Management of Risk* (replacing the *Integrated Risk Management Framework*) and the *GIRM* (replacing the *Integrated Risk Management Implementation Guide*).

Treasury Board Secretariat

In 1985, the federal government passed the Financial Administration Act, under which TBS of Canada was created. Under the legislation TBS was given the authority to regulate the general administrative policy in the federal government.[8] In addition under s7.4 of the legislation the TBS was given authority to make regulations regarding the governing of the corporation including any that adapt any provisions of both the Canada Business Corporations Act and the Canada not-for-profit Corporations Act. This put administration of Crown Corporations and their administrative requirements under the guidance of the TBS in addition to their respective ministries.

The TBS serves as the management board for the federal government. In this role it is responsible for making sure that the Government of Canada is managed in a manner that is consistently coherent and effective across all departments and agencies. This is

---

[8] *Financial Administration Act, Consolidated Acts* 2019, c.F-11.

done through a management regime that is based in rules, practices, and values which sets about how ministers and deputy heads use their authority and their available resources.[9] All of the TBS's policy directives are based on an approach including the policy and materials on risk management.

This may be attributable to the OCG taking a proactive approach and organizing risk assessment sessions for various roles of involved individuals.[10] In 2003 the TBS developed the Management Accountability Framework (MAF) as a tool and set of processes for deputy ministers and agency heads that sets out "expectations of senior management for good public service management."[11] It was designed as a tool that could be used across departments based on measurable evidence.[12] An assessment report of the MAF for TBS generally shows an effective strategy to instill various elements of management among public service employees including risk and risk management through internal audit practices and procedures.

Risk Management and its reporting requirements are grounded in the *Policy on Internal Audit* of TBS under the control of the OCG. Through the internal audit function via Departmental Audit Committees, deputy heads are to improve among other things risk management control and governance. The Departmental Audit Committees are to provide advice and recommendations on the sufficiency and quality of the framework for risk management for the department.[13] An assessment report commissioned by TBS had

---

[9] *Foundation Framework for Treasury Board Policy*, Government of Canada, June 24, 2008
[10] Treasury Board of Canada Secretariat, *Report on the State of Comptrollership in Canada*, (March 2011): 22-23
[11] Phil Charko, "Management improvement in the Canadian public service, 1999–2010" in *Canadian Public Administration* 56 no. 1 (March 2013): 95
[12] Ibid: 95
[13] *Policy on Internal Audit*, Government of Canada, April 1, 2017. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16484&section=html.

also shown that based on annual reports that the internal audit function that one of the improvements was the development and implementation of risk management frameworks.

The Office of the Comptroller General

Under TBS, the main office concerned with the management of the federal government agencies-departments. and the requirements of risk management is the OCG of Canada. It is directly involved, acting as the office in charge of the government's financial management, internal audit, federal assets, and acquired services. This office was originally established in 1978 but was subsumed by the TBS in 1993, only being reborn in the wake of the sponsorship scandal in 2003. Under its current mandate since its revival, the OCG is responsible for promoting and maintaining professional financial and internal auditing systems across the various departments and agencies of the federal government.[14] Overall, the office serves an important function within the TBS role and has responsibility to serve as the government and public service management agency.

The role of the Office of Comptroller General is emblematic of the role of TBS and, working with the various federal ministries it serves the role of a general manager for the Federal Government. It is also unique in that the Treasury Board is enshrined in legislation as other departments and ministries are not.[15] The TBS effectively acts as a unique department that is inherently matrixed with all other agencies, and departments of the federal government because of the nature of its role and responsibilities. Its role is

[14] Clinton Free and Vaughn Radcliffe, "Accountability in Crisis: The Sponsorship Scandal and the Office of the Comptroller General in Canada" in *Journal of Business Ethics* 84 no. 2 (January 2009): 197

[15] Paul Barker and Tim A. Mau, *Public Administration in Canada* 2nd ed. (Toronto: Nelson Education, 2017): 111-112

somewhat contradictory in that it strives to enhance the public service in its ability to provide services but also seeks to maintain strict use of government limited resources.[16]

Business Sector Enterprise Risk Management

In 1999 the Internal Control: Guidance for Directors on the Combined Code (from hereon referred to as Turnbull Guidance) was issued by the Institute of Charted Accountants of England and Wales. This new guidance required a "holistic approach that integrates these separate areas, into core corporate governance processes."[17] Under the guidance company directors have four requirements essential to an organizational approach to risk management. These include the development of accepted risk management policies, implementation of accepted risk management policies through internal control systems, period reviews of the systems' effectiveness, and finally annual compliance reports to shareholders.[18] This new approach to risk meant that older systems which may silo risk based on project or department of the organization are now forced into a single system that encompasses all risk and is adaptable to risks and their potential impact on the organization. Any pre-existing risk management system needs to be incorporated and adapted to fit this new system that is organization wide in its scope. The Turnbull Guidance does a good job of laying out how ERM needs to be encompassed within the larger corporate culture of the organization in order to ensure that ERM is successfully implemented and practiced. However, the Turnbull Guidance details risk management procedures and practices on day-to-day management, only stating what ERM needs to be effective. The effect of this shortfall led companies to develop risk

---

[16] Ian D. Clark, "Restraint Renewal and Treasury Board Secretariat" in *Canadian Public Administration* 37 no. 2 (1994): 212
[17] Michael McCrae and Lee Balthazor, "Integrating Risk Management into Corporate Governance: The Turnbull Guidance" in *Risk Management* 2 no. 3 (2000): 36
[18] Ibid: 36

management systems operating in parallel and perhaps separately from other reporting and control systems which while compliant are not effective in managing risk.[19] However the Turnbull Guidance was only directed at the financial sector in the United Kingdom and thus had limited reach beyond the specific targeted audience.

Enterprise Risk Management & Legislation: Sarbanes-Oxley Act

Within a few years of the Turnbull Guidance being issued in the United Kingdom, ERM was included in the 2002 Sarbanes-Oxley Act (SOX) in the United States. This legislation was passed in the wake of several instances, including some very high-profile instances, of corporate governance failures and scandals. The most notable case of corporate failure was the collapse of Enron in 2001, although there were numerous other cases that contributed to the push for tighter regulations. Sarbanes-Oxley changes the environment in which management has to operate and forces management to include risk management within in its internal control structure.[20] The internal control structure is then monitored by the internal audit function which assures both management and the audit committee (the implementation of which is required by Sarbanes-Oxley) of the organization's system of internal control, risk management, and governance.[21] Given the independent nature of the audit committee as prescribed by the SOX there is an effective system of checks and balances in which risk management is routinely monitored. However, Sarbanes-Oxley only prescribes risk management within the internal audit

---

[19] Stephen Ward, "Approaches to Integrated Risk Management: A Multi-Dimensional Framework" in *Risk Management* 5 no. 4 (2003): 9

[20] Colin Linsley, "Auditing, Risk Management and a Post Sarbanes-Oxley World" in *Review of Business* (2003): pp. 23-24

[21] The Institute of Internal Auditors, *Sarbanes-Oxley Section 404: A Guide for Management by Internal Control Practitioners* 2nd ed. (Jan. 2008): p. 20

function, it does not prescribe or dictate how an organization has to go about implementing any form of risk management. Rather it is simply a part of internal auditing, formal adoption of risk managers, risk management departments, and full implementation is still at the discretion of individual companies and their leadership.

Given the major reforms instituted by the SOX for corporate governance and the reasons behind its creation it should come as no surprise that the legislation served as a template for similar legislation in other jurisdictions including in Canada. The Ontario legislature passed the *Keeping the Promise for a Strong Economy Act (Budget Measures), 2002* (also known as Bill 198 or C-SOX) as the Canadian version of the SOX including the risk management requirements. SOX and its Canadian counterpart demonstrate the importance of EMR in best business practices as an essential part of corporate governance. The use of EMR then translates quite well into public sector management, especially in the wake of the sponsorship scandal.

OBJECTIVES OF THE SOLUTION

The objectives of the guidelines issued by TBS are to develop and implement robust risk management practices and procedures. Risk Management is an internal system of control that can affect company planning and operations. Based on industry best practices, Risk Management has the potential to lead to changes that may require decisions at the appropriate levels of management about personnel, budgets, and commitments with stakeholders.[22] This is because risk management takes into consideration outside factors and influences that go beyond the initial planning of any project or investment. The purpose of risk management is to scenario plan and determine

[22] Project Management Institute, *Practice Standard for Project Risk Management*, (2009): p. 5

the limits of risk acceptable or tolerable risk. This is for both the project to move forward from the design phase and while it is ongoing during construction through qualified personnel like risk managers and high-level management.[23] Not every company will have a role or department devoted to risk management but that does not mean that risk management does not occur with various sub-departments, departments, and/or the organization depending upon how management chooses to include the practice.

Effective Risk Management based on industry best practices requires the establishment of a risk management plan. This plan outlines how Risk Management is practiced within the organization, the roles of individuals within the organization and how it pertains to the management of risk. It should be adaptive to the evolving needs of the organization. The Risk Management plan should outline how risk is tracked and monitored as well as how responses are developed. Additionally, it should outline the escalation procedure for individual risk items so that those items which have high probability and/or impacts can be reviewed and overseen by higher level management. The Risk Management should also outline the frequency with which risk management processes are to be repeated.[24]

A general risk management process involves several steps. First is identifying a potential risk, then assessing whether or not this risk is viable. If the risk is viable, it is determined who is liable should such risk occur, followed by an internal risk owner. The risk owner assesses the probability of the risk occurring and the impact it would have if it did occur. The risk owner is also responsible for monitoring the risk, developing a mitigation strategy, and providing any updates concerning the risk to risk management. If

[23] Andrey Y. Rogachev, "Enterprise Risk Management in a Pharmaceutical Company" in *Risk Management* 10 no. 1 (Feb. 2008): 78
[24] Project Management Institute, *Practice Standard for Project Risk Management*, (2009): pp. 19-20

risk management desires a quantitative evaluation of the specific risk (expected cost incurred should risk occur), the risk owner assists in providing the necessary information. If the risk occurs, the risk owner is responsible for making sure that the mitigation plan is put in place. Once the risk is no longer viable, the risk owner in conjunction with risk management closes the risk. This process ensures that the risk portfolio is consistently kept up to date with the most recent information and that all risk items are supervised by the appropriate levels within the organization. Each organization can customize this process in ways that best fit their organization and their needs but will generally fit within this procedure.

CRITIQUE OF POLICY RESPONSE IN MEETING OBJECTIVES

There is a critique of risk management from a psychological perspective when examining human cognitive biases. The value of risk management comes from the costs incurred from risks against the costs in resources in reducing the impacts and probabilities of the events that incur those costs. The value of risk management is that the costs in resources to mitigate or limit the risk item or event should be less overall than the original impact of the risk or the risk portfolio.[25] The underlying challenge is that risk management is, at least in part, a human exercise and thus subject to human psychological tendencies. Zeckhauser and Viscusi applied this knowledge to health policy, which while not-directly related to project or business management, is an excellent example that details how humans evaluate risk.[26] They point to the fact that individuals tend to over-assess small risks and under-assess broader and more consequential ones. Risks that are harder to assess the impact of are often given more

[25] Richard J. Zeckhauser and W. Kip Viscusi, "The Risk Management Dilemma" in *The Annals of the American Academy of Political and Social Science*, 545 (May 1996): 149
[26] Ibid: 149

attention than they truly warrant given their impact or likelihood and risks derived from actions taken are often given more attention than those derived from inaction regardless of whether they are greater than those of the latter.[27] It is also extensively documented that individuals underestimate the amount of uncertainty they actually face, and individuals who have high stature within an organization are even more confident in their assessments given the nature of their position.[28] That is not to say that investment in risk management is useless because of how we as humans interpret risk, but rather, there is a point where the resources devoted to risk outweigh the potential costs of the risk based on its impact and likelihood.

Similarly, while ERM strives to make risk management an organizational priority, if the culture of the organization does not embrace it, any written policy will have limited effect. While still early in the lifetime of ERM, it existed before Enron's collapse and was acknowledged to be part of best business management practices. There are even more modern examples where companies will take a short cut on risk management if given the right opportunity. The best-case study for this is the 2010 BP oil spill in the Gulf of Mexico.

BP Deepwater Horizon and Risk Management Failure

A clear example of a failure of risk management is the April 2010 British Petroleum (BP) oil spill from its Deepwater Horizon project. An explosion and resulting leak from the underwater oil-well left eleven people dead and spilled almost five million barrels of oil into the Gulf of Mexico before BP was able to cap the well almost three

[27] Ibid: 149-150

[28] Philip Bromiley, Michael McShane, Anil Nair, and Elzotbek Rustambekov, "Enterprise Risk Management: Review, Critique, and Research Directions" in *Long Range Planning* 48 (2015): 270

months later. The joint report issued by the United States Coast Guard and the Bureau of Ocean Energy Management, Regulation, and Enforcement specifically cited risk management failures.[29] In the report issued by the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, the commission found that BP was missing any systemic updating of their risk management and risk assessment tools and procedures. While systemic updating is part of industry best practices, it was not required by regulation. This is in contrast to the system used in the North Sea where operators are required to conduct risk assessments for each individual operation instead of prescriptive regulation of operators.[30]

The Deepwater Horizon oil spill is not only an example of a failure of risk management from a basic project level, but also from an enterprise level. This is apparent in both the failure of BP to promote and maintain a risk management culture (an essential element in ERM) but also in the scale of the impact that the event caused. According to a 2015 report by the Congressional Research Service found that at minimum based on court rulings regarding the amount of oil released into the Gulf, BP was liable for a three-and-a-half billion dollar fine. If the court determines that BP was grossly negligent and committed willful misconduct, the company was liable for a fine of almost fourteen billion dollars.[31] The ultimate criminal fine was four billion dollars, plus an additional approximately half-billion fine paid to the Securities and Exchange Commission for fraud

[29] Rodd Zolkos and Michael Bradford, "BP disaster caused by series of risk management failures, according to federal investigation of Gulf spill," in *Business Insurance* (September 18, 2011)

[30] National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, *Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling* (January 2011): 251-252

[31] Jonathan L. Ramseur, "*Deepwater Horizon* Oil Spill: Recent Activities and Ongoing Developments," Federation of American Scientists, (April 17, 2015): 5

including statements concerning the flow-rate for the oil well.[32] These figures did not include additional civil suit penalties resultant from lawsuits. Additionally, BP's license for exploration and production was suspended by the Environmental Protection Agency (EPA) resulting from information that came to light in discussions with the Department of Justice. This suspension was in place for almost a year-and-a-half until BP came to an agreement with the EPA.

The critique arising from the BP Deepwater Horizon case is that risk management and specifically ERM is only successful if it instills a culture of risk management. The failure to implement the necessary procedures to avoid catastrophe are evident in this case and the cost was billions of dollars for BP.

ASSESSMENT

The assessment of the TBS's risk management policy is based on whether it meets the criteria of what is accepted industry best practice for ERM and whether it adequately explains how to implement it within an organization. These two conditions are essential for any successful policy directive from any government department or agency. However, before the formal assessment of the policy issued by TBS, a brief section will be devoted to outlining the key features of ERM.

Enterprise Risk Management Features

The simplest definition to encompass an enterprise-wide integrated and holistic approach is defined by DeLoach as "a truly holistic, integrated, forward looking and process orientated approach is taken to manage all key business risks and opportunities - not just financial ones- with the intent of maximising shareholders value for the

[32] Ibid: 9

enterprise as a whole."[33] ERM ensures that organizations have an across-the-board approach to identify, monitor, and manage risk at the same time ensuring that management has an understanding of what an individual risk's likelihood or impact could be to the organization and its goal(s).[34] While similar to financial or project risk management, the key features used by ERM make it unique to organization governance beyond trying to limit expose and maximize opportunities.

Craig Cameron in his article about strategic and legal risks concerning work-integrated learning, outlines the key principles of ERM in the context of a university institution. However, the five key principles he outlines are universal in their application for ERM applicable to all institutions or organizations. The five principles outlined by Cameron are defined below:

> *Dual perspective* on risk is the consideration of both positive (opportunities) and negative risks (threats) while trying to limit the impact and probability of the latter and enhance the same on the former.
>
> *Holistic perspective* on risk is an organizational or institutional approach to issues that affect the organization or institutes ability to meet its goals and objectives
>
> *Strategic focus of risk management* is 'mission centered' (Tufano, 2011), linked to institutional governance and aligned with the goals and objectives of the university (organization)

[33] Stephen Ward, "Approaches to Integrated Risk Management: A Multi-Dimensional Framework" in *Risk Management* 5 no. 4 (2003): 9
[34] Edward Giniat and Joseph Saporito, "Sarbanes-Oxley: The Impetus of Enterprise Risk Management" in *Healthcare Financial Management* (Aug 1, 2007): p.66

Shared responsibility for risk management is the involvement of all areas of the organization or institution in practicing and encouraging risk management to develop a healthy risk management culture

Integration with tradition risk management is the inclusion of the previous four factors in combination with best practices of risk management[35]

Of these five features the feature of holistic perspective is extremely important and can be interpreted in two distinct manners of equal significance. In the most basic sense for risk management it means to consider all sources from which risk can arise. However, in regard to ERM, the term holistic also refers to recognition and management of the interactive relationship between the organization's activities and the risks associated with them.[36] Holistic perspective also means that risk management is not practiced in silos within various departments or sub-departments. Risks that effect a public and stakeholder relations department also might affect the legal department as well. For example, lack of properly trained workers for a project would seem a simple human resources risk, but it is also a communications risk because the root cause might just be unawareness of the need for workers.

Just as each company faces differing risk portfolios, each company has its own approach to implementing ERM. While reporting requirements exist under legislation, this does not mean that an organization has fully adopted an ERM programme. Beasley et. al note that several key indicators were correlated to the likelihood that an organization had fully embraced and implemented ERM. These include the presence of a

[35] Craig Cameron, "The strategic and legal risks of work-integrated learning: An enterprise risk management perspective" in *Asia-Pacific Journal of Cooperative Education* 18 no. 3 (2017): 243-244
[36] Stephen Ward, "Approaches to Integrated Risk Management: A Multi-Dimensional Framework" in *Risk Management* 5 no. 4 (2003): 9

risk officer in management capacity (ex. Chief Risk Officer), board level encouragement, and stock exchange listing guideline compliance. In that order, both the presence of a risk officer and board level encouragement indicated a more than fifty-percent likelihood of an organization employing ERM. Stock listing exchange guideline compliance demonstrated an over thirty percent chance that a company has a programme in place.[37] Given their profitability driven nature, private organizations will, for the most part, only commit to a full-scale programme if they are forced to by legislation or regulation, or if they can see some benefit from full implementation of ERM. This work is focused on TBS regulations regarding risk management.

Evaluation of Treasury Board Secretariat Guidelines:

The evaluation of the risk management guidelines from TBS will be based on Cameron's five criteria outlined above. The key document that will be examined is the TBS's *GIRM*.

The guide does a good job of explaining what risk is and the key elements of risk management and what is needed for it to be successful in any federal department or agency. Section two of the guide is a good reference for the key elements of risk management and including basic outlines of the elements of ERM. This is good for a basic understanding of risk and is approachable to anyone who consults it. However, the guide really dives into the detailed intricacies in sections four through seven, which will be the focus of this evaluation.

[37] Mark S. Beasley, Richard Clune, and Dana R. Hermanson, "Enterprise risk management: An empirical analysis of factors associated with the extent of implementation," in *Journal of Accounting and Public Policy* 24 (2005): 523

The guide is very good at the fifth criteria as outlined by Cameron; integrating traditional risk management. In section 4.6, the guide outlines the key parts of proper risk management and section 7 outlines maintaining, reviewing and updating risk management approaches within the organization. This includes the necessary elements in the process of risk management (identification, assessment, communication, and monitoring) and the required components of the individual elements.[38]

The guide is light on material covering the dual perspective of risk management. In its own definition of risk, only passing mention is made of the distinct forms of risk: "threats and opportunities."[39] Further discussion on the identification of opportunities and threats is limited and covered only in broader and more traditional risk management practices. It succinctly says; "it is important to develop an understanding of the organization's willingness to accept the possibility of negative events and its openness to opportunities in the pursuit of an objective or outcome."[40]

The guide takes a similar approach when it comes to strategic focusing of risk management with some additional information covered outside of its coverage of traditional risk management practices. The guide emphasizes the importance of context in which it is applied that is organization specific tailored to the environment in which it operates[41] and mentions how there is no "one-size-fits-all" option when it comes to developing and implementing risk management.[42] However the guide also stresses the importance of performance and success monitoring that should be updated upon resource

---

[38] *Guide to Integrated Risk Management,* Government of Canada, (May 12, 2016): Section 4.6
[39] Ibid: Section 2.1
[40] Ibid: Section 4.2
[41] Ibid: Section 4.1
[42] Ibid: Section 2.3

allocation.[43] In section 6.1 of the *GIRM*, it advises that risk management systems should be synced to align with both the nature of the project and the scale so as to not cause administrative burden.[44]

In contrast to a dual perspective, the idea of shared responsibility for risk management is broadly covered. In section four, the guide outlines the importance of having staff with proper knowledge and competencies to carry out their responsibilities in the planning stage of risk management.[45] Additionally, it advises implementing training for staff to understand the organization's approach to risk management and their role in the organization's risk management processes.[46] Additionally, the guide devotes a good section to "creating the culture" in which it provides considerations for its risk management culture among staff. The guide focuses specifically on practicing risk management and changes being made and how employees will react.[47] Building on this the *GIRM* advocates continuous education and training for risk management. For a shared responsibility of risk management to be successfully implemented, it is essential that individuals at all levels understand the organization's risk management policies and procedures. The *GIRM* encourages learning at individual, team, and organization levels, sharing experiences, and developing responsible risk-taking environments within an organization's overall tolerance for risk.[48]

Finally, there is also a brief, but important mention, of external stakeholders in the risk management process as to inform other entities of potential shared risks concerning

[43] Ibid: Section 5.1
[44] Ibid: Section 6.1
[45] Ibid: Section 4.1
[46] Ibid: Section 5.1
[47] Ibid: Section 5.2
[48] Ibid: Section 6.3

them.[49] This inclusionary approach helps bolster the risk management process and procedures, and could help identify risks that might not have otherwise been proposed or discovered. This specific item should be a larger part of the *GIRM*, and it deserves its own section that clearly explains its importance. External coordination increases accountability and further incentivizes risk management and monitoring at all levels. Given the nature and scale of government, communication with external stakeholders, whether part of the government or outside of it, is essential.

Of the five elements of ERM espoused by Cameron, the holistic approach needed is the element covered most by the guide. The guide stresses the role of management in this area in creating a holistic approach. In its Risk Management Principles, the *GIRM* advises that organizations use risk management in a manner that supports other management functions, is integral in the decision-making process, and applied organization wide.[50] In Section 5.1, the guide goes over a litany of areas that management should consider incorporating risk into. These include among others, governance structures, oversight processes, legislation and regulation compliance, and staff work plans.[51] It encourages management to "visibly encourage the practice of risk management and information sharing across all business lines and functional units."[52] Section 6.2 of the *GIRM* advises the development of a corporate risk profile to get a corporate perspective of the organization's risks.[53] This is in addition to the risk management culture among employees already discussed when examining the concept of shared responsibility. This is clearly the most extensively covered element of ERM.

[49] Ibid: Section 6.1
[50] Ibid: Section 2.3
[51] Ibid: Section 5.1
[52] Ibid: Section 5.2
[53] Ibid: Section 6.2

The coverage of various elements of ERM varies. The guide has this same problem in expressing how to implement it within the organization. Section 5 and 6 cover the implementation and practice of risk management from an organizational approach. However, these sections are limited in covering the essential elements of ERM. An example is the limited advice on the dual perspective of risk management, while again emphasizing the establishment of a holistic approach to risk management.

Pre-Existing Policy

The *GIRM* replaces the *Integrated Risk Management Implementation Guide (IRMIG)*. This document issued in the early 2000s is more detailed than the *GIRM* in explaining how to set-up integrated risk management within a government organization. This came as a result of two separate reports in 2009 recommending an increased focus on risk management (one from the Prime Minister's Advisory Committee on the public service and a clerk report to the Prime Minister on the public service).[54] By reviewing the same elements as before we can see commonalities among the two guidelines for risk management. Sections two through four of the *IRMIG* are where the previously mentioned five key principles of ERM are outlined in this document.

Section 2 outlines key features for successfully implementing both the holistic approach to, and the shared responsibility of, risk management. Under "The Fundamentals" portion of section 2, it is clearly written that risk management must be integrated within existing governance structures and decision-making processes. This includes developing a corporate risk profile. With senior leadership on-board with risk management and communicating its importance, risk management can be encouraged and

[54] Ibid: Section 1.1

developed in the various areas of the entity.[55] It encourages individuals to assess the consequences of their work and the impact it may have, and to develop synergy between overall risk management and more localized risk management.[56] These two elements are extensively covered throughout the *IRMIG*. The document does a great job not only in outlining the key principles of shared responsibility and a holistic approach, but also advocating these principles be included in risk management practices.

For the strategic focus principle of risk management, the *IRMIG* takes a broad approach. It tends to breakdown this principle based upon the level of the organization. The *IRMIG* advocates that all levels include risk management in their differing divisions with both micro and macro scale implementation. The micro scale would be local units and the macro being the larger department. The IRMIG encourages the development of corporate profiles for risk management to assist in developing and managing the risk portfolio for each specific organization. This is good in that it allows each agency or entity some latitude to in managing risk to their specific goals and needs but at the same time pushes for broader risk management strategies for department needs.

Perhaps the most helpful part of the *IRMIG* are the addendums that are included. These are charts that outline the crucial parts of integrated risk management such as “developing a corporate profile” with columns outlining what needs to be done and some ways to go about doing it.[57]

While the *IRMIG* does a good job in outlining those key principles, it distinctly lacks guidance on the dual perspective of risk management. The document lacks any

[55] *Integrated Risk Management Implementation Guide*, Government of Canada (May 2004): 15-16
[56] Ibid: 21
[57] Ibid: 29

specific mention of risk management's dual nature which seeks out both positive opportunities and negative threats. There is no discussion within this document concerning the dual nature, rather the term risk management is simply used without any elaboration on what the term "risk" entails. The negligence of this key principle is carried over into the more recent *GIRM*.

Similarly to the *GIRM,* the *IRMIG* only outlines risk management more broadly, rather than specifically ERM. Risk management is essential for best business practices but without proper ERM that connects the five key principles together, any system is limited in its effectiveness. The *IRMIG* is severely lacking in the dual perspective principle of ERM, but in many ways covers risk management in an easier to understand manner than the *GIRM.* Taking some elements, particularly the addendum charts that outline what and how to proceed with developing key tools to implementing risk management would greatly benefit the *GIRM.*

LIMITATIONS

This policy paper is solely focused on the guidelines issued by the TBS and how they assist or instruct the respective user in implementing an ERM system and protocol. Thus, this study does not address other types of risk management and how TBS guidance relates to their implementation. While overlap can exist between the differing and distinct types of risk management, their implementation and practice are done based on an individual organization's needs and the personnel involved in risk management processes.

Furthermore, this study does not assess any individual federal government department, agency, or organization's system or procedures for practicing ERM. As previously mentioned, the day-to-day practice of risk management of any type is conducted based on individual personnel and organizational needs and goals. The best way to conduct such an assessment would involve some sort of scoring system to evaluate the effectiveness of ERM practices on the organization.

This area is rich with potential future research opportunities. This is especially true from a political science and policy perspective as the field of risk management tends to be examined mostly through business and finance literature. Immediate opportunities lie in comparative research both in domestic and international fields. Cross departmental, agency, or organizational research could be conducted to determine best use and application of TBS's *GRIM.* In the international sphere as differing countries and jurisdictions routinely update their guidelines for risk management, constant comparative research can be conducted. This is furthered as more and more countries adopt risk management guidelines and protocols. In these emerging cases research can be conducted to determine causal factors that lead to policy development such as whether they are a reactionary in nature or imposed for alternative means.

The application and use of the *GIRM* is an additional source of research. Are those responsible for risk management and ERM among federal entities using the guide or relying on other resources. As noted in the assessment, this guide does a good job outlining some of ERM key principles, is this reflected in how ERM is practiced among federal entities. These questions could even be applied to TBS to determine whether its own risk management and ERM practices are reflective of its guidance.

A final area of potential research that could be developed upon is the translation of ERM among other best business practices to public administration. What key factors contribute to government adoption of best business practices and how does this process occur. Perhaps most interesting is how do best business practices morph or adapt within the context of their use in public administration.

CONCLUSION

It is clear that the TBS's *GIRM* covers the various key elements of ERM. However, these elements are not treated equally with the *GIRM* focusing more of some of these elements than others. It is clear that it tends to focus on ERM's holistic approach and the shared approach of risk management while letting its explanation of risk management and its processes and procedures cover other elements. The biggest benefit as well as the biggest weakness of the *GIRM* is its broad applicability across differing departments. This is understandable as the policy is for government wide application among the various departments and agencies, each with different responsibilities deriving from their differing operating contexts. As a guide to implementing risk management for an enterprise, it is good at outlining how to apply risk management systems and procedures while not being overly prescriptive. This allows it to be tailored to the needs of the agency or department applying it.

The other major conclusion that can be drawn from the *GIRM* is that it needs experienced personnel to be effective. The *GIRM* lacks enough guidance for individuals inexperienced with risk management to establish good ERM procedures without supplemental material. Without experienced or confident personnel, government agencies, departments, or organizations can implement underdeveloped ERM procedures, or be forced to rely on outside firms to conduct manage their ERM portfolios.

What can be drawn from this analysis is that TBS lacks essential guidance on ERM. The *GIRM* does a decent job of outlining risk management that, with the properly trained and experienced personnel, can be used to set up well developed risk management processes and procedures. However, TBS would be wise to develop its own guide to developing and practicing ERM within government entities based on the five key principles outlined above. The *GIRM,* in combination with such a document, could serve as a tool to further develop or entrench risk management systems and ERM systems in particular. A clear outline of these five principles to provide context to the *GIRM* could easily translate into a well-developed ERM guide.

BIBLIOGRAPHY

Barker, Tim and Tim A. Mau. *Public Administration in Canada* 2nd ed. Toronto: Nelson Education, 2017.

Beasley, Mark S., Richard Clune, and Dana R. Hermanson. "Enterprise risk management: An empirical analysis of factors associated with the extent of implementation." *Journal of Accounting and Public Policy* 24 (2005): 521-531

Bromiley, Philip, Michael McShane, Anil Nair, and Elzotbek Rustambekov. "Enterprise Risk Management: Review, Critique, and Research Directions." *Long Range Planning* 48 (2015): 265-276

Cameron, Craig. "The strategic and legal risks of work-integrated learning: An enterprise risk management perspective." *Asia-Pacific Journal of Cooperative Education* 18 no. 3 (2017): 243-256

Chang, She-I, Shi-Ming Huang, Jinsheng Roan, I-Cheng Chang and Pu-Jui Liu. "Developing a risk management assessment framework for public administration in Taiwan." *Risk Management* 16 no. 3 (August 2014): 164-194

Charko, Phil. "Management improvement in the Canadian public service, 1999–2010." *Canadian Public Administration* 56 no. 1 (March 2013): 91-120

Clark, Ian D. "Restraint Renewal and Treasury Board Secretariat." *Canadian Public Administration* 37 no. 2 (1994): 209-248

Commission of Inquiry into the Sponsorship Program and Advertising Activities. "Major Findings." 2005. http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/sponsorship-ef/06-02-10/www.gomery.ca/en/phase1report/summary/es_full_v01.pdf.

Dionne, Georges. "Risk Management: History, Definition, and Critique." *Risk Management and Insurance Review* 16 no. 2 (2013): 147-166

Financial Administration Act, Consolidated Acts 2019, c.F-11. https://laws-lois.justice.gc.ca/PDF/F-11.pdf

Foundation Framework for Treasury Board Policy. Government of Canada. June 24, 2008. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13616

Free, Clinton and Vaughn Radcliffe. "Accountability in Crisis: The Sponsorship Scandal and the Office of the Comptroller General in Canada." *Journal of Business Ethics* 84 no. 2 (January 2009): 189-208

Giniat, Edward, and Joseph Saporito. "Sarbanes-Oxley: The Impetus of Enterprise Risk Management." *Healthcare Financial Management* (August 1, 2007): 65-70

Guide to Integrated Risk Management. Government of Canada. May 12, 2016.
Integrated Risk Management Implementation Guide. Government of Canada (May 2004).

Linsley, Colin. "Auditing, Risk Management and a Post Sarbanes-Oxley World." *Review of Business* 24 no. 3 (2003): 21-25

McCrae, Michael and Lee Balthazor. "Integrating Risk Management into Corporate Governance: The Turnbull Guidance." *Risk Management* 2 no. 3 (2000): 35-45

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling. *Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling.* January 2011.

Policy on Internal Audit. Government of Canada, April 1, 2017. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16484&section=html.

Project Management Institute. *Practice Standard for Project Risk Management*. 2009.

Ramseur, Jonathan L. "*Deepwater Horizon* Oil Spill: Recent Activities and Ongoing Developments." Federation of American Scientists. April 17, 2015. https://fas.org/sgp/crs/misc/R42942.pdf

Rogachev, Andrey Y., "Enterprise Risk Management in a Pharmaceutical Company." *Risk Management* 10 no. 1 (February 2008): 76-84.

Rosen, Robert Eli. "Risk Management and Corporate Governance: The Case of Enron." *Connecticut Law Review* 35, no. 3 (2003): 1157-1184.

Sims, Ronald R. and Johannes Brinkmann. "Enron Ethics (Or: Culture Matters More than Codes)" *Journal of Business Ethics*, 45, No. 3 (July 2003): 243-256

The Institute of Internal Auditors, *Sarbanes-Oxley Section 404: A Guide for Management by Internal Control Practitioners* 2nd ed. January 2008.

Treasury Board of Canada Secretariat. *Report on the State of Comptrollership in Canada.* March 2011.

Ward, Stephen. "Approaches to Integrated Risk Management: A Multi-Dimensional Framework." *Risk Management* 5 no. 4 (2003): 7-23

Zeckhauser, Richard J., and W. Kip Viscusi. "The Risk Management Dilemma." *The Annals of the American Academy of Political and Social Science*, 545 (May 1996): 144-155

Zolkos, Rodd and Michael Bradford. "BP disaster caused by series of risk management failures, according to federal investigation of Gulf spill." *Business Insurance* (September 18, 2011). https://www.businessinsurance.com/article/20110918/NEWS06/309189982/bp-disaster-caused-by-series-of-risk-management-failures-according-to-federal-investigation-of-gulf-spill

VITA AUCTORIS

NAME:	Connor R. Lalonde
PLACE OF BIRTH:	Windsor, ON
YEAR OF BIRTH:	1991
EDUCATION:	Walkerville Collegiate Institute, Windsor, ON, 2009
	University of Windsor, B. A. [H], Windsor, ON, 2014 (History)
	University of Windsor, B. A. [H] , Windsor, ON, 2018 (Political Science)