Managing internal policy risk: Australia, the UK and the US compared

Michael Howlett\textsuperscript{a}, Ching Leong\textsuperscript{b} and Sonam Sahu\textsuperscript{b}

\textsuperscript{a}Political Science, Simon Fraser University, Vancouver, BC, Canada; \textsuperscript{b}Lee Kuan Yew School of Public Policy, National University of Singapore, Singapore, Singapore

ABSTRACT

Most studies of risk management examine only exogenous risks – that is, those external to the policy-making process such as the impact of climate change, extreme weather events, natural disasters or financial calamities. But there is also a large second area of concern – “internal risks” or those linked to adverse or malicious behavior on the part of policy makers. This behavior to deceive or “game” the intentions and expectations of government is a part of the policy world which also requires risk management. The paper reviews three archetypal cases of efforts to manage this side of policy risk in the UK, the US and Australia and draws lessons from them about how best to deal with or manage this “darkside” of policy-making.

1. Introduction: internal and external risks in policy-making

Effective risk management in government needs to address both external and internal risks including the oft-observed behavior in policy-making that (a) policy-makers are often driven by malicious or venal motivations rather than socially beneficial or disinterested ones and (b) policy targets or “policy takers” have proclivities and tendencies toward activities such as gaming, free-ridership and rent-seeking (Howlett 2022).

That is, risks are not all exogenous to the policy process. Most studies of policy risk management, however, examine “external” risks such as the impact of climate change, extreme weather events or financial calamities. But there is a large second area of concern which exists: “internal risks.” These are those risks related to adverse or malicious behavior of policy makers or to policy “takers” evading or otherwise undermining government initiatives (Howlett 2020a; Leong and Howlett 2021).

Ignoring these risks does a disservice to both policy design and policy studies by failing to address a significant area of policy risk that contributes to many policy failures and continuing policy problems. Both these risks, as well as external ones of the types cited above, must be curbed if policies are to achieve their aims (Hoppe 2018; Feldman 2018).
2. Internal threats to policy resilience and robustness

External risks stemming from causes such as wars, famines, pandemics and other kinds of crises are well studied and understood (Boin et al. 2005; Boin and ’t Hart 2010). These kinds of risks are the subject of most current risk management regimes, both in the public and private sector, which monitor and observe the external environment for signs of financial and other threats to supply chains, product lines, legal liability and other dynamics that can affect profitability and shareholder value (e.g. FATF 2021; Human Rights Watch 2021; Pandemic Prevention Institute 2021). And some internal risk factors, such as fraud, malfeasance, dishonesty, and other actions on the part of public officials or general public are addressed by other means, such as audits and accountancy practice, performance reviews and hiring and other kinds of personnel and corporate compliance “best” practices.

Neither of these literatures, however, is tied very well to that on public policy, being a feature instead of studies of public and business management and administration.

But both internal and external risks are aspects of policy-making and policy design which can contribute to instability and the unpredictability of a policy outcomes, ultimately often contributing to policy failure (Leong and Howlett 2021). Because of the incorporation of instruments that come with high risk of failure, and by creating situations leading to the implementing of such tools, internal and external risks often lead to unstable policy results. When these risks are clearly understood and mitigation measures adopted in policy designs, however, better outcomes are more likely (Howlett 2020a).

One way that this can be achieved is through the use of tools that singly or in combination are less “volatile” or combine together in positive rather than negative or counter-productive ways. Another is ensuring that instead of being rigid and stiff, policies should be agile and flexible. And a third is to ensure some level of accountability, including risk management processes in designed into a policy from the outset.

This means that policy design, as well as implementation, may require more redundancy in the form of resources, capabilities, and planning to allow for enough flexibility as and when required that they may remain robust over different circumstances. Ensuring feedback and allowing adjustments of assessments and policy elements tarting from the initial stages of policy making has been suggested by many in the research community as a valuable way to ensure policy dynamics evolve in a positive fashion (Pierson 1992, 1993; Baumgartner and Jones 2002; Jacobs and Weaver 2010).

Risk management processes generally go through a cycle of risk identification, assessment, mitigation (or response) and review (Hussain et al. 2018; Persson and Mathiassen 2010).

This process may translate into different steps in different organizations (Aven and Renn 2010a; Aven and Renn 2010b; Burnaby and Hass 2009; Harvey 2012; Hopkin 2018). In general, consultants such as PricewaterhouseCoopers’s urgesan approach to managing risk which involves carrying out the following steps (PwC n.d.):

- assessing risk,
- conducting assessment,
- analyzing collaboration between risk and compliance functions,
- designing and reviewing migration plans
This is similar to the model proposed by other major accounting and auditing firms. Deloitte, for example, approaches risk management using the following procedure (Deloitte 2009):

- identifying risk,
- assessing and measuring risk
- responding to risk
- designing implementing and testing controls
- monitoring and escalating

Compared to external risks, the academic literature has generally been slow to realize the problem of internal risks, jeopardizing these efforts. Many countries, however, have risk management regimes in place which apply such frameworks to their external risks. And some governments have developed several means through which internal risks may be assessed and addressed. Three case studies of these efforts are presented below.

3. Methodology and case selection

Case selection for this study began with a review of risk management practices among OECD countries. Documentary evidence was required and out of the 36 OECD countries, six countries where English is used as the official language – Ireland, Canada, New Zealand, the United States, Australia and the United Kingdom – were selected for more detailed analysis.

A database of administrative agencies that existed in each country to deal with risk assessment and management, was constructed including detailed information on the location of risk management within government organization, their personnel and budgets, mandates, and other important institutional variables.

Secondary research was then conducted and data collected from each country’s official central government’s official website through the examination of organization charts, government reports, and documents. At this point, countries that did not have a substantial amount of information publicly available on internal risk management related agencies and procedures (Canada, Ireland and New Zealand) were excluded from the final list, leaving Australia, the US and the UK as countries where publicly available information details organizational structures and processes for internal risk management.

4. Models of internal policy risk management

The risk management frameworks followed by the central governments of the US, the UK and Australia were found to be broadly similar. But important differences also exist. This section sets out the processes and structures uncovered in this study and explores the similarities and differences in the pattern of practices found.
4.1. The United States: an early starter but lately, a laggard

The US federal government requires that all federal agencies comply with the Federal Managers Financial Integrity Act (FMFIA Act) and with Office of Management and Budget (OMB) and Government Accountability Office (GAO) standards for internal control (also called “management control” in OMB documents) of regulations and operations (Hardy 2010).

The GAO’s “Green Book” (GAO 2014) delivers the standards for internal risk management in the federal government through the five components of internal control listed below. These components apply to staff at all organizational levels and to all categories of objectives of the organization.

The components of GAO’s internal control (GAO 2014) are:

1. Control Environment – This environment influences how objectives are defined in the system and how risk mitigation activities are structured. Agencies are expected to provide the discipline and structure that achieves high quality of internal risk management.
2. Risk Assessment – All federal agencies are expected to undertake assessment which provides the basis for developing appropriate risk responses.
3. Control Activities – These are the actions management takes in order to achieve objectives and respond to internal risks in the system. The response is usually channeled through policies and procedures developed specifically for this purpose.
4. Information and Communication – in this component, the organization is expected to develop and use quality information to support its internal control system.
5. Monitoring – Since internal risk management is a dynamic process that has to be adapted continually, this component assesses the quality of risk management performance over time and promptly resolves the findings of audits and other reviews.

This generally complies with the principles of external risk management cited earlier. But the US does not have a single national internal risk management framework. Rather there are several commonly used frameworks.

First, there is the GAO Risk management framework, cited above, which was developed from the Government Auditing Standards, GAO’s Green Book, guidance from OMB, work on President’s Management Agenda, and the ERM approach of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) (NIST 2018) This framework is flexibly designed to be applicable to departments of various levels.

Second, there are International Standard 31000 (ISO 2018) procedures. These provide a standard risk management framework for use across various entities, sectors and organizations. A US Technical Advisory Group approved ISO 31000:2009 as the standard for the practice of risk management in the United States, and it has also been adopted by other governments, including Australia. ISO 31000 practices include consultative workshops; control identification and verification; targeted surveys; and
direct staff engagement in order to identify and control risks. The application of these guidelines can be customized but are expected to provide a common approach to managing any type of risk, including both external and internal ones.

Third, there is the COSO Enterprise Risk Management (ERM) – Integrated Framework. This was first issued in September 2004 and provides a set of risk management standards for businesses (COSO 2004). It expands on internal control processes, hoping to provide a more robust and extensive focus on risk in order to better align risk appetite and strategy; enhance risk response decisions; reducing operational surprises and losses; identify and manage multiple and cross-enterprise risks; and seize opportunities for improvement. The updated COSO ERM framework published in 2017, provides “a framework for US federal boards and management in entities of all sizes.” It highlights the importance of considering risk in both the strategy-setting process and in driving performance (COSO 2017).

Due to these somewhat competing and over-lapping systems, risk management programs in the US are often extensive but often limited to specific business lines or managed on an isolated agency by agency basis. In most agencies, risk management is included in functions like “Strategic Planning” and “Budget.” This is intended to strengthen responses and future risk preparedness, especially in emergency and crisis prevention scenarios, but integration is still lacking in many agency management activities which differ in terms of the kinds of risks controlled for, and the level of engagement of stakeholders. And, as this description highlights, they tend to emphasize the identification and mitigation of external risks.

4.2. The United Kingdom: gradual construction of a coherent internal risk policy regime

In UK, the risk management process is also structured along with textbook principles (HM Government 2020). It is a system that focusses on:

1. Risk identification and assessment – how to determine and prioritize how risks should be managed in an organization
2. Risk Treatment – the selection, design and implementation of risk treatment options in order to support achievement of intended outcomes and manage risks to an acceptable level.
3. Risk Monitoring – the design and operation of integrated risk monitoring, and
4. Risk Reporting – timely, accurate and useful risk reporting is done to enhance the quality of decision-making and to support the organization in meeting their responsibilities.

The Treasury publishes primary reference and overviews of good practice for corporate governance in central government departments (generally referred to as “the code”) (HM Treasury 2017). This guidance on various aspects of corporate governance is contained in publications such as, Managing Public Money, the Audit and risk assurance committee handbook (HM Treasury 2016), the Ministerial Code, the Civil Service Code, the Code of conduct for board members of public bodies (HM Treasury 2019).
When it comes to external risks, this system is fully operational. There is strong crisis management and emergency planning framework in the UK which features a six-stage process (Plan, Rehearse, Implement, Maintain, Evaluate, Recover) for responding to external risks (Government Communication Service 2018). For managing internal risks, however, the situation is different. And while the UK does have a single national strategy of risk management, like the US it too is de-centralized and exists mainly in the form of Treasury guidelines which individual agencies and managers are expected to follow in their own ways.

Unlike the US, however, when it comes to internal risks the British system does highlight these and expects them too to be subject to risk management activities. Thus in its report on Management of Risk (HM Government 2020) the Treasury notes that “inherent risks” exist in policy and governance and that these require whole-system-thinking, aligned incentives, positive relationships and collaboration. These are expected to exist alongside relevant technical knowledge to support multi-disciplinary approaches.

UK Treasury codes set out best practices in this area, suggesting that matters of internal risks, for example, should be the central focus of the organization’s board, and not simply a committee matter. And it suggests that all boards should be supported by an “audit and risk assurance committee.” It further mandates that the committee should consist of a suitably experienced non-executive board member (the chair of the committee); an internal audit service (operating to Public Sector Internal Audit Standards); and sponsor teams of the key ALBs. Similarly, the code mandates that a board’s regular agenda should include scrutinizing and advising on risk management and that such Boards must enough information and resources to efficiently set the organization’s risk appetite while maintaining “a clear framework of governance and risk management” within the organization.

Audit and Risk Assurance Committees in specific government agencies are expected to support the Boards to meet these obligations. Such committees are expected to be established in all Executive departments, Non-Departmental Public Bodies and other ALBs and are to undertake the task of internal audit, risk mitigation, work with the External Auditor, and deal with organization’s financial and reporting issues.

In fact to stress the significance of these risk factors the UK government code suggests maintaining two separate committees with following responsibilities:

i. an audit committee – with focus on assurance arrangements over: governance, financial reporting, annual reporting, accounts, including the governance statement;
ii. a risk assurance committee – with a focus on ensuring the are resources for adequate and effective risk management.

4.3. The commonwealth of Australia: a fast learner

Unlike the US and more similar to the UK, in managing external risks and emergency preparedness the Australian Government Crisis Management Framework is another example of a simple, centralized and government-wide management scheme. It
provides ministers and senior officials with guidance on their respective roles and responsibilities and sets out the arrangements that link ministerial responsibility to the work of key officials, committees and facilities (AU Dept. of the Prime Minister and Cabinet, 2017).

Commonwealth policy sets out nine elements of an agency’s Assurance Review Framework (AU. Dept. of Finance 2017), which are expected to guide the establishment and operation of an appropriate system of risk oversight and management. These elements are:

i. Establishing a risk management policy;
ii. Establishing a risk management framework;
iii. Defining responsibility for managing risk;
iv. Embedding systematic risk management into business processes;
v. Developing a positive risk culture;
vi. Communicating and consulting about risk;
vii. Understanding and managing shared risk;
viii. Maintaining risk management capability; and
ix. Reviewing and continuously improving the management of risk.

This extends to both internal and external risks but in managing internal risks, an important characteristic of the Australian Government, unlike in the UK and US, is that its internal risk management system is uniform and evenly distributed throughout each agency’s organizational structure.

The Commonwealth resource management framework (AU Dept. of Finance 2019) governs how officials use and manage public resources. The PGPA Act 2013 is the cornerstone of this framework which states that the accountable authority must establish and maintain an appropriate system of risk oversight and management for the entity, and an appropriate system of internal control for the entity to ensure public resources they are responsible for are properly managed. The PGPA Act provides flexibility to establish those systems and to create an operating environment that supports the proper use and management of public resources.

Under this framework, the “Risk and Internal Control” covers the risk management framework as well as compliance reporting and internal control systems (AU Dept. of Finance 2020).

These tasks include reporting on compliance, fraud control, audit committees, reporting to Joint Committee of Public Accounts and Audit (JCPAA), Model Accountable Authority Instructions, and Australian Government Assurance Reviews. These latter include Implementation Readiness Assessments (IRA), Gateway Reviews Processes and Assurance Reviews Processes.

The system is still de-centralized, however, as all the Divisions, Branches, and Sections within an agency are supposed to maintain local “risk assessment” with their own section. The same is true for all levels down to Projects, Programmes, and Portfolios as well. Beyond that level, separate thematic risk assessments are also carried for special topics like security, fraud, and safety. For such topics, separate risk assessment procedures often using specialized methods are employed.
Within the broader Australian Government, there are also some agencies that manage a category of risk on behalf of the whole government. The Australian Signals Directorate is one such agency that assesses Government information security risks, and is assigned with the task of treating them according to the Australian Government Information Security Manual (the ISM). The manual includes information on security measures and functions similar to risk management measures for the government, although specific to security issues.

4.4. Analysis

This review of three leading OECD countries shows that progress has been made toward the management of internal or inherent risks but sometimes in an ad hoc and decentralized way. Table 1 compares risk management process in USA, UK and Australia.

In the UK, risk assessment only became a governmental matter at the end of the twentieth century after getting high public attention due to a series of major policy disasters (Dunlop 2017). The timelines of UK government publications shows that as more researchers and scientists become involved in the risk analysis processes, after this time and increased the more attentive Government became to risk management issues in its existing protocols. Most innovations happened during the first half decade of the 21st century, when major transformations took place (Grant 2009) and risk assessment developed as an integral part of the government policies. After this initial period constant improvement was observed in the subject of risk assessment both in governmental organizations and scientific communities; a process which continues today but which still prioritizes external over internal sources of risk.

Table 1. Risk management process in USA, UK and Australia compared with the general risk management cycle.

| Risk management processes | USA's risk management structure | UK's risk management structure | Australia's risk management structure |
|--------------------------|--------------------------------|-------------------------------|--------------------------------------|
| Risk identification      | • Control environment          | • Risk identification and assessment | • Establishing the risk management policy |
|                          |                               |                               | • Establishing risk management framework |
|                          |                               |                               | • Defining responsibilities |
|                          |                               |                               | • Embedding risk management into business processes and systems |
| Assessment               | • Risk assessment             |                               | • Developing a positive risk culture |
|                          |                               |                               | • Establishing communication and consultation about organization’s risk |
| Mitigation               | • Control activities          | • Risk treatment               | • Understanding and managing shared risk |
|                          | • Information and communication |                               | • Maintaining risk management capability |
|                          |                               |                               | • Reviewing and continuously improving the management of risk |
| Review                   | • Monitoring                  | • Risk monitoring              | • Risk reporting |
|                          |                               | • Risk reporting               |                                      |
The corporate governance structure in USA, on the other hand, is highly focused on internal control and financing, while risk management is a joint function of the department’s financial officer, the office of Inspector General and staff, along with guidelines from OMB’s Circular, GAO’s Green Book and other programmes. The result is a patchwork of risk assessment and management processes. Agencies generally follow the Government Performance and Results (GPRA) and the GPRA Modernization Act (GPRAMA) and produce annual performance reports to report their strategies, goals and operations to the Congress. But currently, agencies do not (and are not required to) have an independent risk management framework as in the UK or Australia.

The risk management system in the Australian government is the most developed. Today, assessment of both external and internal risks is an important part of governance in Australian agencies. Throughout the corporate structure, risk management regulations are strongly embedded and responsibilities assigned to every layer of management. The main responsibility, however, falls on management Board members who are required to establish risk and audit committees to focus on risk to organization’s overall working and environment. Audit committee meetings are also joined by Australian National Audit Office (ANAO), which makes “risk management and assessment” a regular exercise. In some agencies, external (private) companies are also invited to provide risk support and help improve the risk assessment process. All the agencies act as per the PGPA Act and base their risk management framework on international standards or national standards.

5. Conclusion: existing risk management regimes and their focus on external risk

Dealing with risks requires hard choices to be made both in policy formulation and implementation. Policy volatility or the propensity for policies to fail, is affected by both external and internal factors. Although the former may be better explored in policy literature, the latter has also seen important work such as Hatvani 2015; Kiliç, Kuvat, and Boztepe 2021; Vijayakumar and Nagaraja 2012.

There is therefore a need to “design in” correctives such as stricter accountability mechanisms, verification and monitoring plans right at the outset of policy-making to ensure these are locked in and left in place while a programme or policy matures (Plaček, Půček, and Ochrana 2018; Vine and Sathaye 1999). As many governments have come to realize recently, without better internal risk management, it is difficult to offset policy risks. That is, there is just as much of a need to better assess and address the internal risks of failure right at the outset when a policy is first considered, as there is with the more familiar “external” risks (Falco 2017; Taylor et al. 2019).

In response, in practice, many governments have begun to create guidelines and agencies to systematically anticipate and mitigate these kinds of risks. But as the three cases set out above show, this process has been very uneven and varies by jurisdiction. Robust (internal and external) risk management is vital for the government for meeting their critically important missions and each of the case study governments recognized this.
External risk management has attracted high attention after catastrophic incidences like natural disasters or man-made situations like security threat and, most recently, health-related crises and pandemics but internal risks remain problematic and require more research and implementation in practice. And this is true not only in developing or under-resourced governments but also in the wealthier and generally better organized OECD countries.

Notes
1. ISO 31000:2009 is now replaced by ISO 31000:2018 (ISO, 2018) which also provides guidelines on managing risk faced by organizations.
2. Partnerships established between departments and arm’s-length bodies (ALBs) are also governed by similar codes of good practice. These ALBs are organisations that deliver a public service, are not ministerial government departments, and operate at a greater or lesser distance from Ministers. The term can include non-departmental public bodies (NDPBs), executive agencies, non-ministerial departments, public corporations, NHS bodies, and inspectorates (House of Commons, 2014).

Disclosure statement
No potential conflict of interest was reported by the author(s).

ORCID
Michael Howlett http://orcid.org/0000-0003-4689-740X

References
AU. Dept. of Finance. (2017). Australian Government Assurance Reviews - Rescue Management Guide No. 106.
AU Dept. of Finance. 2019. “Managing Commonwealth Rescues.” Government. https://www.finance.gov.au/government/managing-commonwealth-rescues.
AU Dept. of Finance. 2020. “Implementing the Commonwealth Risk Management Policy (RMG 211).” Managing Commonwealth Rescues. https://www.finance.gov.au/government/managing-commonwealth-rescues/implementing-commonwealth-risk-management-policy-rmg-211.
AU Dept. of Finance. 2017. “Australian Government Assurance Reviews – Rescue Management Guide No. 106.” https://www.finance.gov.au/publications/resource-management-guides/guidance-assurance-reviews-process-rmg-106
Aven, T, and O. Renn. 2010a. “Risk Management.” In Risk Management and Governance, 121–158. Berlin, Heidelberg: Springer.
Aven, T, and O. Renn. 2010b. Risk Management and Governance: Concepts, Guidelines and Applications. Vol. 16. Springer Science & Business Media.
Baumgartner, F. R, and B. D. Jones. 2002. Policy Dynamics. Chicago: University of Chicago Press.
Boin, Arjen, Paul ’t Hart, Eric Stern, and Bengt Sundelius. 2005. The Politics of Crisis Management: Public Leadership under Pressure. Cambridge: Cambridge University Press.
Boin, Arjen, and Paul ’t Hart. 2010. “Organising for Effective Emergency Management: Lessons from Research1.” Australian Journal of Public Administration 69 (4): 357–371. doi:10.1111/j.1467-8500.2010.00694.x.
Burnaby, P., and S. Hass. 2009. “Ten Steps to Enterprise-Wide Risk Management.” Corporate Governance: The International Journal of Business in Society 9 (5): 539–550. doi:10.1108/14720700910998111.
COSO. 2004. “Enterprise Risk Management — Integrated Framework.” https://www.coso.org/Pages/erm-integratedframework.aspx

COSO. 2017. “Guidance on Enterprise Risk Management.” https://www.coso.org/Pages/erm.aspx

Deloitte. 2009. “Take the Right Steps – 9 Principles for Building the Risk Intelligent Enterprise.” https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/Board%20of%20Directors/in-gc-putting-risk-in-the-comfort-zone-nine-principles-for-risk-intelligent-enterprises-noexp.pdf

Dunlop, Claire A. 2017. “Pathologies of Policy Learning: What Are They and How Do They Contribute to Policy Failure?” Policy & Politics 45 (1): 19–37. doi:10.1332/030557316X14780920269183.

Falco, Gregory. 2017. Constraint Tree Analysis: A Method to Evaluate Threats to Technology Policy Goals. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2939209.

FATF. 2021. “Guidance on Proliferation Financing Risk Assessment and Mitigation.” http://www.fatf-gafi.org/publications/financingofproliferation/documents/proliferation-financing-risk-assessment-mitigation.html.

Feldman, Yuval. 2018. The Law of Good People: Challenging States’ Ability to Regulate Human Behavior. Cambridge UK: Cambridge University Press.

GAO. 2014. “Standards for Internal Control in the Federal Government. GAO-14-704G.” https://www.gao.gov/assets/gao-14-704g.pdf

Government Communication Service. 2018. “Emergency Planning Framework.” https://3x7ip91ron4ju9ehf2unqrm1-wpengine.netdna-ssl.com/wp-content/uploads/2020/04/Emergency-planning-framework-1.pdf

Grant, Wyn. 2009. “Intractable Policy Failure: The Case of Bovine TB and Badgers.” The British Journal of Politics and International Relations 11 (4): 557–573. doi:10.1111/j.1467-856X.2009.00387.x.

Hardy, K. 2010. “Managing Risk in Government: An Introduction to Enterprise Risk Management.” IBM Center for the Business of Government. http://enterrasolutions.com/media/docs/2013/09/RiskinGovernment.pdf

Harvey, G. E. 2012. “The Process of Risk Management: Important Steps to Take.” Petroleum Accounting and Financial Management Journal 31 (1): 77.

Hatvani, E. N. C. 2015. "Risk Analysis and Risk Management in the Public Sector and in Public Auditing." Public Finance Quarterly 1 (7): 7–28.

HM Government. 2020. The Orange Book - Management of Risk – Principles and Concepts. London: HM Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF.

HM Treasury. 2016. Audit and Risk Assurance Committee Handbook. London: HM Treasury. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/512760/PU1934_Audit_committee_handbook.pdf.

HM Treasury. 2017. Corporate Governance in Central Government Departments: Code of Good Practice. London: HM Treasury. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609903/PU2077_code_of_practice_2017.pdf

HM Treasury. 2019. “Guidance Code of Conduct for Board Members of Public Bodies June.” Gov.UK. https://www.gov.uk/government/publications/code-of-conduct-for-board-members-of-public-bodies/code-of-conduct-for-board-members-of-public-bodies-june-2019

Hopkin, P. 2018. Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. Kogan Page Publishers.

Hoppe, Robert. 2018. “Heuristics for Practitioners of Policy Design: Rules-of-Thumb for Structuring Unstructured Problems.” Public Policy and Administration 33 (4): 384–408. October 1. doi:10.1177/0952076717709338.

Howlett, Michael. 2020a. “Dealing with the Dark Side of Policy-Making: Managing Behavioural Risk and Volatility in Policy Designs.” Journal of Comparative Policy Analysis: Research and Practice 22 (6): 612–625.
Howlett, Michael. 2022. “Avoiding a Panglossian Policy Science: The Need to Deal with the Darkside of Policy-Maker and Policy-Taker Behaviour.” Public Integrity 1–13. doi:10.1080/10999922.2021.1935560.

Human Rights Watch. 2021. “World Report 2021.” Human Rights Watch. https://www.hrw.org/world-report/2021.

Hussain, Z., W. Khan, and J. Z. Khan. 2018. “Job Safety Analysis and Risk Assessment A Case Study Of Frontier Ceramics Ltd.” https://www.researchgate.net/profile/Zahid-Hussain-5/publication/328723240_Job_Safety_Analysis_and_Risk_Assessment_A_case_study_of_Frontier_Ceramics_Ltd/links/5bddd05da6fddc3a8d9b3e67/Job-Safety-Analysis-and-Risk-Assessment-A-case-study-of-Frontier-Ceramics-Ltd.pdf

ISO. 2018. “ISO 31000:2018 Risk Management Guidelines.” https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

Jacobs, Alan, and R. Weaver. 2010. Policy Feedback and Policy Change. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network.

Kılıç, B. İ., Ö. Kuvat, and E. Boztepe. 2021. “Measurement of the Effectiveness of Internal Audits in Public Sector.” In Contemporary Issues in Public Sector Accounting and Auditing. Emerald Publishing Limited.

Leong, Ching, and Michael Howlett. 2021. “Policy Learning, Policy Failure, and the Mitigation of Policy Risks: Re-Thinking the Lessons of Policy Success and Failure.” Administration & Society 44: 009539972110653. doi:10.1177/00953997211065344.

Leong, Ching, and Michael Howlett. 2022. “The ‘Inherent Vices’ of Policy Design: Uncertainty, Maliciousness and Non-Compliance.” Risk Analysis.

NIST. 2018. “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.” SP 800-37 Rev. 2. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

Pandemic Prevention Institute. 2021. “Ending the Current Covid-19 Pandemic and Preventing Future Global Disease Outbreaks Requires Fast, Accurate Data.” The Rockefeller Foundation (blog). https://www.rockefellerfoundation.org/pandemicpreventioninstitute/.

Persson, J., and L. Mathiassen. 2010. “A Process for Managing Risks in Distributed Teams.” IEEE Software 27 (1): 20–29. doi:10.1109/MS.2009.157.

Pierson, P. 1993. “When Effect Becomes Cause: Policy Feedback and Political Change.” World Politics 45 (4): 595–628. 1993. doi:10.2307/2950710.

Pierson, Paul. 1992. “Policy Feedbacks’ and Political Change: Contrasting Reagan and Thatcher’s Pension-Reform Initiatives.” Studies in American Political Development 6 (2): 359–390. doi:10.1017/S0898588X00001012.

Plaček, Michal, Milan Pucek, and František Ochrana. 2018. “Identifying Corruption Risk: A Comparison of Bulgaria and the Czech Republic.” Journal of Comparative Policy Analysis: Research and Practice 21 (4): 366–384.

Pwc. n.d. “Risk Management and Compliance. Risk Assurance.” Services. https://www.pwc.com/me/en/services/risk-assurance/risk-management-and-compliance.html

Taylor, Christopher M., Elaine A. Gallagher, Simon J. T. Pollard, Sophie A. Rocks, Heather M. Smith, Paul. Leinster, and Andrew J. Angus. 2019. “Environmental Regulation in Transition: Policy Officials’ Views of Regulatory Instruments and Their Mapping to Environmental Risks.” The Science of the Total Environment 646: 811–820. doi:10.1016/j.scitotenv.2018.07.217.

Vijayakumar, A. N., and N. Nagaraja. 2012. “Internal Control Systems: Effectiveness of Internal Audit in Risk Management at Public Sector Enterprises.” BVIMR Management Edge 5 (1): 1–8.

Vine, Edward, and Jayant Sathaye. 1999. “The Monitoring, Evaluation, Reporting and Verification of Climate Change Projects.” Mitigation and Adaptation Strategies for Global Change 4 (1): 43–60. doi:10.1023/A:1009651316596.