

Strictly confidential

SMARTER GOVERNANCE

10 topical insights into risk oversight

September 2024



Supporting



Challenging



Delivering

bob **SEMPL**E


10 topical insights into risk oversight



North Carolina State, with the support of AICPA and CIMA, recently published their 15th edition of “The State of Risk Oversight”. It provides an overview of the current state of risk oversight practices based on data provided by 377 US organisations. This report summarises their 10 key areas of focus, overlaying insights from my own risk management experience with organisations in Ireland and beyond over the last 11 years. I hope it contributes to further enhancement of risk management – maximising the opportunities in strategic plans and minimising the uncertainties and hazards.

Bob Semple

Overview of Key Focus Areas

Issue	The Challenge
1. Volume and Complexity of risks	Risks are growing all the time
2. Risk management processes	Processes are still immature (after all these years!)
3. Risk and Strategy	Risk is disconnected from strategy
4. Risk Identification	Risks are not being identified sufficiently frequently – esp. strategic and emerging risks
5. Risk Scoring	Qualitative (5x5) scoring predominates – with resulting ambiguity/inaccuracy
6. Management Dashboards	Dashboards largely ignore KRIs
7. CROs and Management Risk Committees	Individual accountability is still underdeveloped
8. Board delegation of Risk to a Committee	Boards need to up their game on oversight
9. Pressure on Senior Management	Senior Managers face increasing governance expectations and accountabilities
10. Barriers to effective risk management	Real benefits of risk management are still not appreciated - or realised

The Challenge	Questions to ask
<p>1. Volume and Complexity of risks</p>	
<p>Factors such as:</p> <ul style="list-style-type: none"> • Interconnectedness of global markets • Geopolitical instability • Cyber and related threats • Climate change • Rapid technological advancements • Changes in supply chains • Process transformation resulting from use of AI • Evolving regulatory landscapes • Changing workforce dynamics • Surprises/ unanticipated issues <p>all contribute to making it harder for organisations to anticipate and manage risks effectively</p>	<ol style="list-style-type: none"> 1. How rapidly is our organisation’s business environment changing and how difficult is it for our leadership team to anticipate emerging issues? 2. What significant surprises have management and the board faced that they did not sufficiently anticipate? Why were we surprised by these occurrences? 3. How often does our management team or the board seem to be in “firefighting” mode that distracts our management team from important strategic initiatives? 4. What should management do to enhance the organisation’s preparedness to navigate a sudden, unexpected risk event? 5. How are recent geopolitical events (both nationally and internationally) likely to impact our business?
<p>2. Risk management processes</p>	
<p>A majority of organisations:</p> <ul style="list-style-type: none"> • say their organisation’s risk management oversight is not mature or robust • report not having a complete formal enterprise-wide risk management process in place <p>Just over a quarter of organisations have no enterprise-wide view of risks</p> <p>In short, most organisations’ risk management remains immature</p>  <p>The maturity level scale consists of five stacked boxes, each labeled 'Maturity Level' and containing a number from 1 to 5. Level 1 is red, level 2 is orange, level 3 is yellow, level 4 is light green, and level 5 is dark green.</p>	<ol style="list-style-type: none"> 1. If asked to describe “risk management” at our organisation, how would executives and board members respond? Would those responses be consistent? 2. In light of the risk environment for our organisation, how can we improve the maturity of our risk management processes to keep pace with our risk realities? 3. What major events have management had to suddenly address and why were those events not more fully anticipated by our risk management processes? 4. To what extent are our executives and board discussing and evaluating our organisation’s approach to managing risks? 5. Where is our organisation most vulnerable if we continue with our status quo approach to risk management?

The Challenge	Questions to ask
<h3>3. Risk and Strategy</h3>	
<p>Organisations struggle to integrate risk properly with their strategic plans</p> <p>Most organisations do not see the strategic advantage in operating mature risk management</p> <p>A majority of organisations fail to address risk issues in capital allocation decisions</p> 	<ol style="list-style-type: none"> 1. How can we better integrate risk management into our strategic planning process? 2. How can we better engage our risk experts with those making important strategic decisions? 3. How clear is the mapping of our enterprise’s top risks to our key business drivers and strategic initiatives? Which drivers or initiatives are most exposed to key risks? 4. How can we better move our understanding of risk appetite from “individually implicit” to “collectively explicit”? 5. When budget allocation decisions are made across the organisation, how can we better reflect the differences in risk conditions to inform our resourcing decisions?
<h3>4. Risk Identification</h3>	
<p>Most organisations identify new risks infrequently (sometimes only quarterly or, even, annually – despite the environment that points to very rapid changes in risk conditions)</p> <p>Few organisations devote sufficient time to ongoing monitoring and identification of new strategic risks</p> 	<ol style="list-style-type: none"> 1. How can we better identify emerging risks (and monitor the “risk velocity” of risks already in our register)? 2. How can we enhance our “horizon scanning” to ensure completeness of risk identification? 3. To what extent are the right individuals engaged in the process for identifying risks? Are we addressing third party risks sufficiently? 4. How can we incorporate “Devil’s Advocate” and similar techniques to overcome cognitive bias? 5. How can we measure and enhance “psychological safety” to protect against poor decision-making?

The Challenge	Questions to ask
<h3>5. Risk Scoring</h3>	
<p>Most approaches used to prioritise risks are more qualitative than quantitative</p> <p>Too often there is inconsistency in how individuals apply a 5x5 scoring approach leading to under- and over-scoring of risks (individually and relatively)</p> <p>Few organisations report key risk indicators (KRIs) that management can use to monitor shifts in risk conditions over time.</p>	<ol style="list-style-type: none"> How can we better protect against: <ol style="list-style-type: none"> under-scoring of risks (thus exposing the organisation to unwanted potential harm), and, over-scoring of risks (resulting in needless remediation/excess cost) How can we refine our scoring matrix for impact and likelihood? (e.g. by reflecting risk velocity, level of preparedness, interconnectedness to other risks etc) How can we embed the use of KRIs – for example, by using them in setting personal objectives for executives? To what extent are differences in risk prioritisations (management v. board) discussed to get a more balanced risk perspective? What enhancements to our management dashboard do we need to make to effectively track changes in risks over time (i.e., key risk indicators)?
<h3>6. Management Dashboards</h3>	
<p>A majority of organisations:</p> <ul style="list-style-type: none"> do not prepare a formal written report about top risk exposures for senior management review do not schedule agenda time at management meetings to discuss key risks do not explicitly address risk issues as part of each board paper summary sheet 	<ol style="list-style-type: none"> What style of reporting would be most effective with our executive leadership and the board of directors? How does the information about top risks communicated to management and the board help in making strategic decisions? How can we better generate robust discussion and dialogue about risk? What enhancements can we make to reporting of risks using visualisation? How can we better link risk reporting to strategic objectives?

The Challenge	Questions to ask
7. CROs and Management Risk Committees	
<p>More organisations than ever before are appointing a CRO, but the delineation of responsibilities versus with the first line of defence is often blurred</p> <p>A majority of larger organisations have a separate risk committee but they often feel overwhelmed by the volume of information they are asked to review</p> <p>The emphasis in most organisations is still on the description of risks instead of tightly managing implementation of the mitigating actions to reduce residual risk in line with risk appetite</p>	<ol style="list-style-type: none"> 1. Who “owns” the design and implementation of our organisation’s approach to risk management? Is that the most effective person? 2. Is the individual responsible for leading our organisation’s risk management process at the right level within the organisation? Does that individual have access to our CEO and board? 3. Should we fold consideration of risk into the business of the executive/senior management team agenda instead of addressing it in a separate committee? 4. How can we use “deep dive reviews” to better understand how middle management is managing risks? 5. Do we have the right leaders engaged in overseeing the enterprise portfolio of risks on an ongoing basis? Are we continuing to manage risks at a granular level while reporting them on an aggregated basis?
8. Board delegation of Risk to a Committee	
<p>Most boards of directors have delegated responsibility for overseeing management’s risk management processes to a Board Committee (typically the Audit (and Risk) Committee or a dedicated Committee)</p> <p>Most boards pinpoint a specific meeting to discuss top risk exposures facing the organisation (rather than retaining risk as a standing agenda item for every meeting)</p> <p>Except for financial services organisations, only about one-quarter of organisations have formally articulated their risk appetite</p>	<ol style="list-style-type: none"> 1. Would individual board members be able to consistently and accurately describe management’s risk management process? Do they ‘own’ risk? 2. How does our board of directors evaluate the effectiveness of management’s risk management processes? 3. Is board discussion about risks sufficiently robust and is there a consensus understanding of the most important risks to the organisation? 4. How does the board of directors validate the appropriateness of management’s identification of top risks? Does the board compare management’s report of our top risks to external sources about top risks facing other organisations? 5. How does the board determine the levels of risk appetite among key stakeholders for different risks facing the organisation?

The Challenge	Questions to ask
9. Pressure on Senior Management	
<p>Expectations, particularly from boards of directors and their audit committees, are increasing for more senior executive involvement in risk oversight for their organisations.</p> <p>Part of that increased interest is triggered from unanticipated risk events that have impacted the organisation. (Over one-third of organisations believe the organisation needs to enhance its approach to business continuity and crisis management).</p> <p>Emerging best practices and corporate governance requirements are also incentivising greater engagement of senior leaders in risk management activities.</p>	<ol style="list-style-type: none"> 1. How well do we understand the risk oversight expectations of our key stakeholders (especially our customers) and how well are we meeting those expectations? 2. How are best practices related to enterprise-wide risk governance changing? 3. What vulnerabilities in our risk management process have been revealed by recent unexpected events affecting our organisation or peers in our industry? How well do we track incidents/issues and “near misses” and do we learn enough from them? 4. How robust is our organisation’s business continuity plan and is it well understood across the organisation? 5. What does our organisation need to do to be better prepared to navigate an unexpected crisis? When is the last time the board conducted a desktop simulation of a crisis to check the readiness of the board?
10. Barriers to effective risk management	
<p>Leaders are often reluctant to change how their organisation approaches risk management because they fail to see the need for change, or they don’t have individuals to lead the effort.</p> <p>There are still too many people at the top of the organisation who do not see the benefits of good risk management. Perceptions that there are more important competing priorities that require senior executive attention other than risk management is at the top of the list in regard to barriers limiting risk management progress.</p>	<ol style="list-style-type: none"> 1. How have we identified and addressed the cultural barriers that are limiting commitment to more effective risk management? 2. What additional incentives (and penalties) can we implement to remove the barriers to realising greater benefits from effective risk management? 3. How do we need to adapt our approach to risk management to take account of rapid changes in the volume and complexity of risks facing the organisation? 4. What additional training should we deliver to senior executives and board members? 5. How comfortable are we to be lagging advanced risk governance practices?

Contact

m: +353 86 810 6434

e: bob@bobsemple.ie

w: www.bobsemple.ie

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No republication or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, Bob Semple does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© Bob Semple 2024. All rights reserved. Not for further distribution without the permission of Bob Semple.