

# *SMARTER GOVERNANCE*

## *10 key questions about risks*

August 2023



*Supporting*



*Challenging*



*Delivering*

## 10 key questions about risk

Too often, the Risk Register is regarded as an administrative overhead, a burden on the business which detracts from value rather than adding. And, worse, it puts the focus on the incomplete documentation of the risk instead of smart actions to manage it.

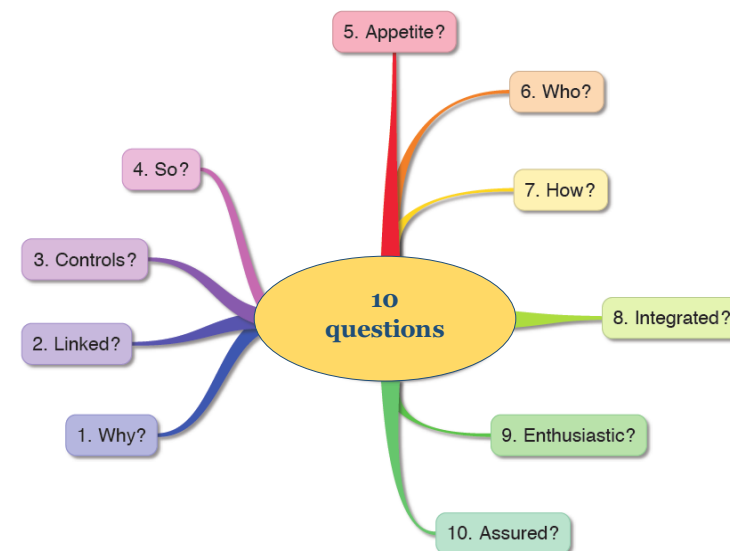
This appendix briefly describes ten questions to rectify this state of affairs. If you amend your risk descriptions, having successfully answered all ten questions, you will find yourself in a position to realise significant benefits – previously unavailable. But, be warned! This takes effort! You will need to challenge, to probe, to test unstated assumptions, to decide who is the right person for planned actions, and to align your actions with a collectively agreed risk appetite.

What’s in it for you? Simply put, realising your objectives faster, at least cost, exploiting opportunities to good effect – all aligned to a ‘sweet spot’ of risk, personally and for your organisation.

Good luck!



### Bob Semple

Question	The Challenge
1. Why?	Risks are poorly described
2. Linked?	Risks are disconnected from everyday operations
3. Controls?	Controls are poorly defined
4. So?	Practical consequences are not identified
5. Appetite?	Risk appetite is poorly defined or applied
6. Who?	Individual accountability is poorly managed
7. How?	Planned actions are not SMART
8. Integrated?	Risk management is not integrated in everyday operations
9. Enthusiastic?	Inadequate training / support is provided
10. Assured?	There is no systematic assurance about successful management of risk



Question	The Challenge	How to tackle it
<p><b>1. Why?</b></p>	<p><b><i>Risks are poorly described:</i></b></p> <p>Aspects that typically cause difficulty include:</p> <ul style="list-style-type: none"> <li>• Describing the risk at too high a level (for example “Non-availability of services”)</li> <li>• Not separating completely separate risks (for example “Fraud or Error”)</li> <li>• Describing the consequence of the risk rather than the risks itself (for example “IT breakdown”)</li> <li>• Not probing deeply enough to reveal the underlying issue(s)</li> <li>• Distinguishing what is controllable versus uncontrollable</li> </ul>	<p>Use root cause analysis to get underneath the stated risk by asking “Why?” repeatedly (usually 4 iterations are effective).</p> <p>If you can’t explain the risk to a stranger in 30 seconds and get his undivided attention, you need to refine your analysis (or, possibly, drop the risk)</p> <p>(More detailed guidance on defining risks and an explanation of the 5 Whys (root cause analysis) is available on request).</p>
<p><b>2. Linked?</b></p>	<p><b><i>Risks are disconnected from everyday operations:</i></b></p> <p>Risks are not related to corresponding strategic or operational objectives and, therefore, are not seen as important.</p> <p><b><i>“The only two certainties in life are death and taxes - everything else is uncertain (a risk!)”</i></b></p>	<p>Explicitly relate identified risks to strategic and operational plans.</p> <p>In practice, this can be done in 2 ways:</p> <ol style="list-style-type: none"> <li>1. Starting with strategic and operational objectives, identify the impact of uncertainty on these objectives (risks), or,</li> <li>2. Perform a SWOT analysis to surface the risks of greatest concern; then link those concerns back to strategic and operational objectives</li> </ol> <p>Better still, do it both ways to make sure your analysis is complete.</p> <p>Another useful approach is to consider risks under three categories:</p> <ol style="list-style-type: none"> <li>1. Preventable</li> <li>2. Strategic</li> <li>3. External</li> </ol> <p>See HBR article: <a href="https://hbr.org/2012/06/managing-risks-a-new-framework">https://hbr.org/2012/06/managing-risks-a-new-framework</a></p>

Question	The Challenge	How to tackle it
<p><b>3. Controls?</b></p>	<p><b><i>Controls are poorly defined:</i></b></p> <p>Typical challenges include:</p> <ol style="list-style-type: none"> <li>1. The design of the control does not address relevant control objectives for the identified risk (such as: accuracy, completeness, authorisation, audit trail etc)</li> <li>2. The control as designed is appropriate but is not, in reality, being operated or evidenced (for example, a well-designed bank reconciliation that is not being completed or reviewed on a timely basis)</li> </ol> <p>Often, the so-called controls in risk registers are better classified as the controls that managers:</p> <ul style="list-style-type: none"> <li>• would like to be in place (but were never there in the first place), or,</li> <li>• think are in place (except they are not actually operating as hoped)</li> </ul> <p>A further challenge is mixing up current versus proposed controls (and taking comfort before proposed controls are successfully implemented)</p>	<p>Apply professional scepticism:</p> <ol style="list-style-type: none"> <li>1. explicitly link the design of the control to the control objectives required to address the risk (ask if the risk were about to become an incident, would the control described be effective in preventing it?)</li> <li>2. seek evidence that the control is operating effectively (for example, by reference to a key performance indicator which has been set appropriately and is being monitored effectively)</li> <li>3. separate current controls from proposed controls</li> </ol> <p>PwC provide a useful guide on factors to consider in optimising controls: <a href="https://www.pwc.co.uk/assets/pdf/towards-controls-optimisation.pdf">pwc.co.uk/assets/pdf/towards-controls-optimisation.pdf</a></p>
<p><b>4. So?</b></p>	<p><b><i>Practical consequences are not identified</i></b></p> <p>In the same way that so-called ‘risks’ need to be peeled back to root causes, stated consequences need to be probed to fully appreciate their ultimate impact.</p> <p>Generally speaking, consequences can be identified at two levels:</p> <ul style="list-style-type: none"> <li>• Concrete adverse outcomes impacting the organisation such as: financial loss, injury/death, breakdown/interruption, and,</li> <li>• The ensuing damage to reputation.</li> </ul> <p>The test is to be able to express the consequence bluntly – in a way that elicits a desire to remedy it promptly.</p>	<p>Ask “So?”, repeatedly, to identify the concrete outcome as well as the resulting damage to reputation.</p> <p>The following link provides an approach to measuring impact by reference to performance measures already in place: <a href="https://paladinrisk.com.au/risk-tip-3-developing-consequence-matrix/">paladinrisk.com.au/risk-tip-3-developing-consequence-matrix/</a></p>

Question	The Challenge	How to tackle it
<p><b>5. Appetite?</b></p>	<p><b><i>Risk appetite is poorly defined or applied</i></b></p> <p>Risk standards typically require a statement on the system of internal control, which imposes obligations on the Board (or “those charged with governance”) to describe processes used to identify business risks and to evaluate their financial implications, including the use of a statement of risk appetite.</p> <p>While most are used to managing risk implicitly, this requirement to manage risk explicitly (including the use of a statement of risk appetite) is challenging.</p> 	<p>Examine the statement of risk appetite and ask yourself:</p> <ul style="list-style-type: none"> <li>• are the actions described in the risk register sufficient to reduce the risk to the level specified in the statement of risk appetite? (for example, if there is a stated risk appetite of ‘Zero’ or ‘Adverse’ for cyber risk yet the risk register records the assessed level as 4x4 with few proposed actions?)</li> <li>• are managers and staff really familiar with the details of the statement of risk appetite (the collective, explicit statement on risk ) or are they actually applying their own (individual, implicit) understanding of risk appetite?</li> </ul> <p>There is good advice available on how to describe risk capacity and risk appetite by reference to limits and triggers.</p>
<p><b>6. Who?</b></p>	<p><b><i>Individual accountability is poorly managed:</i></b></p> <p>The 3 essential elements in completing any task are to establish and communicate:</p> <ul style="list-style-type: none"> <li>• Responsibility – a crisp definition of the task at hand</li> <li>• Authority – confirmation that the required resources are available (people, budget, data, IT, time etc)</li> <li>• Accountability – how and when the individual will be held to account is clear</li> </ul>  <p>Frequently, these elements are not properly catered for (either by the person assigning the task or by the assignee, who, unwisely, agrees to take on the task))</p>	<p>Several responses help address this challenge:</p> <ul style="list-style-type: none"> <li>• Agree who the ‘Executive Owner’ is for each risk</li> <li>• Separately identify the ‘Operational Owner’ for each planned action</li> <li>• Explicitly check that Responsibility, Authority and Accountability are appropriated addressed for each planned action</li> <li>• For complex cases, determine if a more formal approach (using, for example, RACI analysis) is appropriate</li> </ul> <p>(Further details of RACI analysis available on request)</p>

Question	The Challenge	How to tackle it
<p><b>7. How?</b></p>	<p><b><i>Planned actions are not SMART:</i></b></p> <p>The SMART acronym (Specific Measurable Attainable Realistic Time-bound) is easy to understand but can be difficult to apply.</p> <p>If proposed actions to address risks are not clearly stated, there is a real danger that the required mitigation will not take place in time, effectively or at all.</p> <p>Classic weaknesses include:</p> <ul style="list-style-type: none"> <li>• Long-winded/vague proposed actions – not being specific</li> <li>• Mixing up current controls versus proposed controls</li> <li>• Assigning the task to more than one person (or to a Committee/Team)</li> <li>• Not specifying a clear deadline for completion (or, worse, specifying ‘Ongoing’)</li> <li>• Not specifying a clear ‘output’ (which demonstrates successful completion of the task)</li> </ul>	<p>Specify each proposed action:</p> <ul style="list-style-type: none"> <li>• With a clear task (ideally starting with an action verb/imperative)</li> <li>• Who is to do it</li> <li>• By what date</li> <li>• With a clear ‘output’ or deliverable</li> </ul>
<p><b>8. Integrated?</b></p>	<p><b><i>Risk management is not integrated in everyday operations</i></b></p> <p>Managers instinctively manage risk implicitly rather than explicitly. One of the biggest risks associated with the Risk Register is that it is perceived to be separate from day to day work – a bureaucratic obligation rather than the single most important aid to achieving strategic and operational objectives.</p> <p>Two practical impediments to effective risk management in this regard are:</p> <ul style="list-style-type: none"> <li>• Lack of integration of risk management (especially the risk register and the actions contained therein) into day to day working, and,</li> <li>• Inability to share the insights from other parts of the organisation</li> </ul>	<p>A variety of responses are possible:</p> <ul style="list-style-type: none"> <li>• Implement a dedicated risk management system (rather than rely on a spreadsheet)</li> <li>• If possible, integrate the risk management system as part of a workflow solution</li> <li>• Design and operate Key Risk Indicators</li> <li>• Monitor and follow-up overdue planned actions</li> <li>• Monitor and report ‘near misses’</li> <li>• Promote a culture of ‘psychological safety’ (see page 40)</li> </ul>

Question	The Challenge	How to tackle it
<p><b>9. Enthusiastic?</b></p>	<p><b><i>Inadequate training / support is provided:</i></b></p> <p>Implementing risk management (or any new topic) requires three aspects of learning to be addressed:</p> <ul style="list-style-type: none"> <li>• Knowledge and understanding</li> <li>• Practical tools</li> <li>• Confidence and enthusiasm</li> </ul> <p>Individual training needs can vary substantially; if not addressed, unmet training needs can severely impact the success of risk management.</p>	<p>Formally assess training needs and design and deliver appropriate training.</p> <p>Practical approaches include:</p> <ul style="list-style-type: none"> <li>• Providing one-on-one assistance to each risk owner in documenting their highest risk to the standard required using a challenge-response ('Socratic) approach</li> <li>• Including risk management objectives in each manager's/individual's annual performance targets</li> <li>• Establishing Communities of Practice to share insights</li> <li>• Review of risks at Management Team and at Board level</li> </ul> <p>The following link provides an interesting case for risk management training: <a href="https://www.protechtgroup.com/blog/the-importance-of-risk-training">https://www.protechtgroup.com/blog/the-importance-of-risk-training</a></p>
<p><b>10. Assured?</b></p>	<p><b><i>There is no systematic assurance about successful management of risk</i></b></p> <p>Keeping an appropriate balance between the detailed processes on the one hand, and the 'big picture' on the other, is difficult.</p> <p>Boards often express concern about incomplete identification of significant risks, uncertainty about who is to address them and failure to tackle identified risks quickly enough.</p>	<p>Use formal 'Assurance Mapping' to deliver the comfort required</p> <p>Introduce a "Four Assurances" confirmation which requires the following assurances to be provided (by the CEO to the Board, and by Managers to the CEO):</p> <ol style="list-style-type: none"> <li>1. I have an up to date listing of the top risks in my area of responsibility</li> <li>2. I have devised appropriate action plans for these top risks (consistent with the statement of risk appetite)</li> <li>3. I am ensuring that planned actions are being completed satisfactorily, on time</li> <li>4. I have identified anything else you need to know about risk</li> </ol> <p>The following link describes Assurance Mapping: : <a href="https://www.icaew.com/technical/audit-and-assurance/assurance/assurance-mapping">https://www.icaew.com/technical/audit-and-assurance/assurance/assurance-mapping</a></p>

---

## Contact

*m:* +353 86 810 6434

*e:* [bob@bobsemple.ie](mailto:bob@bobsemple.ie)

*w:* [www.bobsemple.ie](http://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 2023. All rights reserved. Not for further distribution without the permission of Bob Semple.