So, I'm a new public sector Chief Risk Officer. What the hell do I do now?

All that power and glory, but a thick fog surrounds you. Here are 50 questions to ask in your first 100 days.

In response to the recommendations or observations of several reviews, Chief Risk Officers (CROs) have proliferated in Canberra over the last few years. There remains no enduring legislative or regulatory requirement for a Commonwealth public sector entity to have a CRO.

In some sectors, for example financial services, the role of a CRO is mandated, well defined, well understood, and the requirements to be one clear. In the public sector, the role is more ambiguous and often established with little consideration as to what it is exactly intended to achieve in practice.

Often a Chief Financial Officer, Chief Audit Executive, Chief Operating Officer, or other unsuspecting senior executive wakes up on an otherwise normal day and finds out they are a public sector CRO.

Many of the well-meaning and otherwise accomplished people who find themselves with this job title are professionally and organisationally ill-equipped to discharge its responsibilities. This is not my judgement, but their own, conveyed to me by the numerous public sector CROs I've worked with and supported over many years.

So, how do you oversee and shape the management of opportunity and uncertainty for a potentially multi-billion-dollar department?

This brief article doesn't tell you what you need to implement or change. That's up to you and will be different in every organisation. It does though provide some thoughts on the attributes of a good CRO (public sector or otherwise) and some questions to ask as you ease into the role.

Ten attributes of an effective CRO

A CRO doesn't need to be an expert in the science and art of risk management. Like all senior executives, they must build and leverage the capability of their teams and supporting networks. However, I believe there are a set of enduring qualities that will determine how well an individual is able to be a CRO:

1. The **role and accountabilities** of the CRO should be clearly defined and understood – by the organisation's management and staff, relevant parliamentarians, and boards or committees.
2. A CRO should have unfettered and unfiltered **access** to the most senior management, boards and committees.
3. The CRO should have **visibility** of and the ability to **critically review** all risk across the organisation and those shared with stakeholders.
4. A CRO should understand the organisation's business and be seen as a **credible** strategic advisor and enabler.
5. A CRO, through the authority of their position or their personal qualities, should be able to **challenge and influence** decision making across the organisation.
6. To encourage disclosure, a CRO should be **trusted** by all levels of staff and management.
7. A CRO should be **unencumbered** by significant risk in their own portfolio to reduce the risk of self-review.
8. A CRO should have an appropriate **appreciation and understanding** of the value of risk management and the key attributes of risk arrangements and frameworks.
9. A CRO should have the **discretionary capacity and assigned resources** to fulfil the role.
10. A CRO should **not be routinely distracted** overseeing minor compliance concerns or intervening in the management of the transient risk of the day.

To test the merit of the principles above, swap CRO for CFO and swap risk for money.

Of course, not every one of these attributes is applicable to every individual or organisation. Some people can star or flounder regardless of how many are met. Given that almost all public sector CROs today are double or triple hatted, some of these attributes are aspirational from the get-go. It is the extent to which that compromises your ability to undertake the role that matters.

50 questions to ask

For someone in a new senior role, being equipped with good questions is often more valuable than being given advice. Some questions a new public sector CRO might ask follow:

How is the CRO role defined, understood and resourced?

Unlike in other sectors, there is no mandate or common expectations for public sector CROs. Often, they are appointed without a clear articulation as to what they are expected to achieve or do.

1. What are the expectations and accountabilities of your position? What is the view of the Accountable Authority and/or Board (as relevant)? Where is this documented?
2. What are the authorities of your position? In particular how does the CRO's authority extend across and into other roles that have a strong focus on risk? (e.g. CSO, CISO, WHS, business continuity etc). Where is this documented and is it understood across the organisation?
3. How many of the ten attributes described above do you and your position exhibit? Given other competing roles you might

have, how much of your time and energy can you devote to being the CRO?

Does your organisation know why it does 'risk management'?

Why does your organisation do risk management? It's an investment made in competition with other priorities. Is the purpose clear?

4. Are the principles and intended outcome of your organisation's risk management arrangements clearly defined? Why do you do it? Is there a strong and succinct policy statement, endorsed by the accountable authority that says it is to be done and why?

5. Does this policy reflect the unique role and operating environment of your organisation, and the expectations of the government of the day?

Your risk management framework

All Commonwealth entities are required to have a risk management framework - a documented approach to the management of risk.

6. Can you draw the elements of your organisation's risk management framework on a single sheet of paper? Do they fit together as a system, or are they a collection of largely independent pieces?

7. Does your framework reflect the latest versions of relevant standards and regulations? When was it last reviewed or updated?

8. Are the risk management roles and responsibilities of others in the organisation clearly defined and understood?

Risk appetite and tolerance

Risk appetite and tolerance are the natures and amount of risk your organisation is prepared to accept to achieve its objectives. Without such an appetite, the organisation will be paralysed by risk aversion and minimisation.

9. Has the organisation articulated its appetite and tolerance for different natures of risk? How was this compiled and how recently was it reviewed?

10. How is this translated across the organisation so it can be understood and implemented in practice? For example, how is the risk appetite practically reflected in your risk framework and processes?

Risk in strategic and corporate planning

Strategic risks are those that threaten or enable the strategic choices your organisation makes. They are different from otherwise big, but operational, enterprise risks.

11. How does your organisation identify and assess uncertainty in its ability to achieve its strategic priorities? How is strategic planning and the assessment of risk aligned?

12. How are such strategic risks discussed by the executive team and Boards/committees? Is the conversation one of steering into the future and navigating uncertainty, or just one of listing big things that can go wrong?

Your Board

Some public sector organisations have Boards or some other form of external governance. These have a critical role in risk management, but often they don't get the information they need and have risk management views counter to the executive management.

13. If your organisation has an external governance body, is their role in risk management clearly defined and understood?

14. What reports do they want and what reports do they get? How is Board reporting tailored and focused to ensure the right conversations are had?

The executive risk conversation

Most public sector agencies have a diverse range of internal executive and consultative committees and forums. Some have a 'risk committee of management', an executive forum focused on discussing strategic, enterprise and other significant risks. Such a committee acts as a cross-organisation risk staging post before concerns get to the top-level executive committee or the audit committee.

15. How is risk discussed in the executive meetings, forums and committees you attend? Is it informal or structured? What is the rhythm - is a rolling discussion of key risks a standing agenda item?

16. Do you (as CRO) attend the right committees, or only by invitation? How do you pick up on risk issues that aren't being 'pushed' to you? How do you 'pull' risk information from colleagues or business units who may not know what they don't know?

17. If you do (or don't) have a risk committee of management, was this a considered decision? If you do, is its mandate and accountabilities clearly defined and understood?

18. How strong and consistent is the messaging from the top on the importance of good engagement with risk? Would people consider it one of your organisation's priorities?

Commonwealth Risk Management Policy

The Commonwealth Risk Management Policy was released in 2014 to provide principles-based guidance for relevant Commonwealth agencies to meet the risk management expectations of the Public Governance, Performance and Accountability Act. The Policy is binding on non-corporate entities, and advisory for corporate entities.

19. Does your risk management framework clearly describe how you comply with the nine elements of the Policy?

20. When was this alignment last reviewed or assured?

Core risk process and language

You will likely need several risk processes within your organisation – each focused on a specific need. However, there should be a core process and language that each is derived from.

21. Risk terms are used very differently between organisations. Does your risk framework include a clear and comprehensive glossary? Are risk terms and concepts defined consistently across the many documents in your organisation?

22. Pretend you are a more junior staff member who's been asked to quickly conduct a risk assessment of a small project. Close your door, and without help, can you efficiently find (and understand) the things you need to complete this task?

Risk profiles across the organisation

A risk profile is a set of risks often stored in a risk register. You probably have a diverse range of risk profiles being "maintained" across your organisation (for example, strategic, enterprise, divisional, branch, project and special purpose (e.g. WHS or Information Security)).

23. Can you draw a diagram showing the risk profiles being maintained in your organisation on a single piece of paper?

24. Can you explain how this structure came about, and the functions, boundaries and the inter-relationships between each profile? Is it logical and fit-for-purpose?

25. Is the organisation managing the right risks? Skim some of the profiles – are they

just lists of the usual things that can go wrong?

26. How does the organisation systematically work to understand the inter-dependencies or common concerns across these otherwise individual risk profiles? How do we pull the signals from the noise?

Portfolio, Program and Project (P3) risk arrangements

Most organisations have programs and projects – transient or bounded change management activities. They often don't align against your organisational structure and have risks different from business as usual.

27. How do your programs and projects identify, assess, document and manage their risks? Do you have well established and consistent P3 risk governance arrangements?

28. How does the organisation understand the risk at the boundaries of projects and business as usual? How do you stop things falling in the cracks between them?

29. Does the organisation understand the total risk of all of its projects and the ultimate risk to the realisation of the benefits they were intended to achieve?

Special purpose risk systems

Complex organisations require specialist risk systems to comply with specific external or policy requirements. Examples of such systems include workplace health and safety, business continuity, physical security, information security and fraud control. Unfortunately, the practitioners of these disciplines can hide behind their own jargon, priorities and processes. This robs the executive of the ability to see and compare diverse risks across the organisation.

30. How do your subsidiary risk systems feed up into your enterprise risk arrangements? How do they translate their concerns and needs into a common frame so that priorities can be established, and investment decisions made?

Embedding and operationalising risk management

Risk management can't be a stand-alone activity. For best effect, the identification and assessment of risk should be embedded into other business processes. Examples include procurement, recruitment, program management and policy development.

31. Can you see evidence that risk judgments made as part of other business processes are consistent and proportionate?

32. Do you have a consistently implemented process for capturing, analysing and sharing the results of your organisation's successes, failures and near misses? Is your management of risk continuously improved by the collective experience of your organisation?

Shared risk

Shared risks are those big complex risks with no natural owner. Responsibilities for their management can be shared across agencies, jurisdictions, and with the private sector and the community. As your organisation will only have a bit-part in its shared risks, it can be tempting for officials to turn a blind eye.

33. Review your risk registers and profiles. Are the risks predominantly inwards looking or based on the objectives of your organisation alone?

34. How does your organisation formally consider its shared risk environment? Do you ever take a holistic view of the risks you have a role in, but without looking solely at the implications for yourselves?

Risk management training and competence

We all manage risk every day - we do it every time we cross the road. But, to do it consistently in a professional context requires people understand the organisation's attitude to risk taking and the systems and processes that can support them make appropriate risk decisions.

35. How do people in your organisation onboard with how 'you do risk'? This includes junior recruits and senior lateral hires. Is it comprehensive, compellingly and consistently delivered? Casually ask a couple of recent recruits in the coffee shop about how risk is managed in the organisation…

36. What through-career training and mentoring in risk management do you provide – junior, supervisory, senior executive and specialist? How well is this aligned to your current risk management arrangements, or is it generic and off the shelf?

Recognition and rewards

People do what they are recognised and rewarded for. It is a powerful motivator of good and bad behaviours. This includes how people perceive, communicate and manage risk.

37. How is engagement with risk considered in your staff performance management or appraisal arrangements? Is it explicit or just another optional implicit consideration?

The central risk team

Most organisations have a central risk team. They maintain your risk arrangements and support the executive and business units think about risk in a consistent manner.

38. Do you have the right people? How competent and compelling is your risk team? Do they understand risk management as a discipline and also the business of your organisation? Are they professional risk people embedded (and invested) in your organisation, or are they organisation staff in temporary risk roles?

39. Is there an effective push and pull system that enables your risk team to both inject themselves <u>and</u> be drawn-in to the right conversations? Ask your colleagues if that is working or not.

40. How is your risk team upskilled, challenged and measured? What are their performance expectations and how are these benchmarked or set?

41. Do you have a network of risk champions or an internal risk community of practice to model good risk management and support their peers?

Risk Culture

Risk culture is those values, practices, beliefs and perceptions that shape how your staff manage risk on a day to day basis. The majority of your organisation's risks won't find a home in a risk register and it is these elements of risk culture that determine how well they are managed. Risk culture is a subset of your broader organisational culture.

42. Do we understand (and define) what risk management values, practices, beliefs and perceptions we want our people to have?

43. How do we work to achieve the risk culture we want? Have we ever explicitly tested our organisation's risk culture? Do we understand the priority changes that need to be influenced or shaped?

Audit and Assurance

Risk management is both a goal and an enabler of good governance.

44. If your organisation has an Audit Committee, Audit and Risk Committee or internal auditor is their role in risk management clearly defined and understood? Where does their role and accountability begin and end?

45. What is the connection between your audit and assurance activities and the risks you assess? How are critical risks and critical controls targeted for audit? What is the standing process to trigger this?

46. If there are overlaps between your risk and audit teams and functions, how have you acknowledged and managed the opportunity for self-review risk?

Use of consultants and advisors

Consultants and external advisors can bring important expertise and independence to your risk management arrangements. However, they can also introduce inconsistency and conflicting approaches if not carefully orchestrated.

47. Are parts of your organisation independently hiring consultants to advise or support them manage risk? If so, why? Is this for good reason, or does it reflect a need for better coordination or improvement in your internal risk management capability?

Risk information management

A Risk Information Management System (RIMS) is an information management system for risk profiles and risk data. In theory, they can simplify and consolidate the capture and reporting of risk information across the organisation. They may be integrated with other governance and planning tools.

48. Do you have a dedicated RIMS? If so, why? What is it doing for you and what does it cost? What is the take-up of the RIMS and when was satisfaction with the system last tested?
49. Does the RIMS implement your organisation's own risk management framework, or are there compromises imposed by its design? Were you forced to implement the risk management approach the RIMS needed?
50. Spend some time randomly looking through the system. How up to date are the entries? How comprehensive are they? Does the system encourage and capture the outcome of good risk discussions or is it just a drop-down selection compliance exercise?

Summary

This article doesn't try and tell you the risk arrangements you should put in place. That's up to you and your team, and of course will vary between organisations. It does though equip you with some questions to ask as you explore the role. Critically considering the answers (or lack thereof) you receive will allow you to develop your 12-24 month transition or transformation plan.

First published 5 November 2020, v1.0

Sal Sidoti has over 30 years' experience working with public and private sector organisations across Australia and further afield. He works with his clients providing tailored risk management advisory services that support decision making in practice. Approaches that go beyond cut-and-paste compliance and death by spreadsheet. Sal is the Director and Principal Consultant of Crafted Solutions Pty Ltd. He is home based near Canberra, Australia.

https://au.linkedin.com/in/sjsidoti
enquiries@craftedsolutions.com.au

Title illustration courtesy of Motoki Tonn via Unsplash