To Govern Well, Manage ENTERPRISE Risk

By John Mendzela

"Risk management" now receives high attention in most organisations. Central banks are no exception. Indeed risk management is often snappily promoted under the acronym "ERM" - Enterprise Risk Management.

But that acronym can be misleading. In fact many central banks are approaching enterprise risk management ineffectively. Two stories illustrate what goes wrong and how to get enterprise risk management right.

About ten years ago, I was individually interviewing each senior manager at a large central bank. The structured interviews were part of a scoping visit to gather information for the independent strategy and organisation review that the Governor had commissioned.

To begin, I explained the purpose of the interview and its confidentiality. Then I asked an open-ended question on familiar matters to get discussion started: "Please explain briefly your current role, how you came to take up that role, the resources you have, and the work of your department."

Interviews proceeded smoothly until I came to the Risk Management Department. The mid-career woman who had that job seemed upset, so it would be important to start on a relaxing note. We sat down across from one another. I sat in a friendly posture with pen in hand, made my introductory remarks, and asked my standard question: "Please explain briefly your current role, how you came to take up that role, the resources you have, and the work of your department."

"I will do that very briefly", she said curtly. "I was appointed head of the Risk Management Department last week. Before that I managed an economic forecasting unit, and I enjoyed that job. Now I have no staff, no plans and no tools. And I have no idea what risk management is about!"

What to do next? I leafed through my questionnaire. Further questions on her department were now irrelevant. And I did not want to dive into sensitive territory. I worked quickly through the last section on institution-wide topics, obtaining competent but terse answers. Then came the last page: "Is there anything that we have not spoken about, that I should consider when performing my review?"

© John Mendzela 2019

"Yes", she said firmly. "You need to understand that we have many excellent technical people, but not many people who understand organisation and management. And that needs to change before we can succeed in our future mission."

I reported the obvious deficiency in the central bank's approach to risk management to the Governor. But we had many fundamental problems of institutional governance and management to work on first. So I didn't have any further direct contact with the head of the Risk Management Department until some months later, when we met in a corridor. I said hello, and asked how her work was going now.

She was cheerful. "Very well thank you. I have two staff already, and the Department will be allocated more staff soon. We are communicating with other central banks, and adopting their systems for risk management. Our first task is to compile risk registers on all of the central bank's operational activities."

That story illustrates how many central banks have approached risk management:

- presume a new department is needed
- appoint someone with no relevant interest or expertise to head it
- copy what other central banks have done, without first exploring concepts or looking outside the central banking industry
- build a resource base for the new department
- start a bottom-up analysis with an operational perspective

That approach has predictable results – much investment, little return. Managers resent new systems they see as burdensome and unhelpful. Extensive analysis, documentation and risk mapping generates detailed reports that are not much used by managers and may not even be visible at the governance table. Much data is generated, but only limited information and little genuine knowledge. And some key data is likely to be false anyway – in the "make no mistakes" institutional culture that is common in central banks, hiding problems is more likely than accurate "incident reporting".

And worse, that operational emphasis misses the opportunity to create genuine enterprise risk management as a valuable governance tool.

What should be done differently?

© John Mendzela 2019

A few years later, another central bank asked me to help establish a risk management framework. I did not feel expert on that topic, but agreed as part of assisting the new Governor with a broader change programme.

I began with the most obvious question. Why was a new and specialised framework needed at all? Managing risk has always been part of any managerial role. This central bank had even specifically documented that in its job descriptions. So what was wrong or missing?

The answers elicited from discussions with a range of managers were not convincing. Yes, there were management problems and things sometimes went wrong in unexpected ways. But those deficiencies seemed to be specific problems in managerial skill and attention, not a fundamental gap that demanded a new framework.

I reported that to the Governor. He didn't disagree, but insisted that a new specialised framework must be developed. Why? Because the external auditors had identified the lack of a formal enterprise risk management framework as a "serious problem", and panicked the Board. Directors wanted something done, fast. Another central bank had already been approached for help. A process to develop operational risk registers was about to begin. And the external auditors were keen to get involved and sell their "expertise" in enterprise risk management.

I explained that enterprise risk management should be governance-oriented and top-down, not operationally-oriented and bottom-up. The external auditors and the "helping" central bank would take his central bank down entirely the wrong road. The Governor agreed. So he asked me to design something different, of high governance value.

I wasn't confident. But I got started. I began by preparing a set of "Questions and Answers on Enterprise risk management" to get Board and management thinking along the right lines (an updated version appears later in this article). I was especially keen to make any new framework positive in flavour, and to focus on the central bank as a holistic and enduring institution. In fact the key breakthrough came to me as a simple question: "If I was a Board member here, and I wanted to feel confident that the central bank was well-placed to succeed in its mission now and in the future, what positive statements about the institution would I need to be assured of?"

The heart of the new framework became a simple one-page report that considered each of ten dimensions of the institution in turn. Sequence was important. The analysis began with reputation -- often rightly described as any central bank's most important asset. What is the target

© John Mendzela 2019

outcome for our reputation? How can we express that in a few positive statements that we can objectively verify? Our list was simple:

- *The Bank is seen as an honest, competent and trustworthy institution by all key stakeholders*
- *External parties who interact with the Bank do so with confidence in its integrity and capability*
- *The Bank is seen to operate under worthy leadership and within an appropriate culture*
- *The Bank meets, and is seen to meet, all relevant professional and organizational standards*
- *Staff feel positive about being part of the Bank and align their behaviour with the Bank's values*

Nine more dimensions followed, applying the same approach to the central bank's statutory mandate, governance, funding, capability and management practices. The analysis ended with change management.

The simple starting point of a one-page report to the Board was a great relief for everyone. Analysis proved remarkably easy. The resulting scorecard led naturally to consideration of actions to check the ratings and improve those that were too low. How can we verify our internal view on each statement? And where we are not confident that those test criteria are being met, what should we do next?

Managers felt motivated, and quickly identified specific change initiatives. For example, to check on reputation, external stakeholders could be independently surveyed, compliance with professional standards could be more systematically checked, and alignment of behaviour with values could be built into performance appraisal. Risk "owners" were identified for each institutional dimension. To drive and coordinate progress without extensive cost and bureaucracy, a new position of Risk Management Adviser was created, reporting to the Deputy Governor (a Board member). Crucially, that was a sole-charge position, not a new department.

The result wasn't perfect. A suitable new appointee was hard to find, and the first appointment was not a success. Strong attention from the Deputy Governor and the Board was not always achieved. But conceptually, the new enterprise risk management framework stood the test of time and contributed to valuable institutional change. Later unification of risk management with strategic management led to better-integrated governance and management at that central bank.

Wider opportunities for the central banking industry emerged too. Over the next few years, I generalised that specific experience to develop a

© John Mendzela 2019

framework for assessing institutional excellence in any central bank or financial regulator. Diverse central banks have applied that ***INEX***^{SM} framework at various levels: as a comprehensive assessment, as a guide to institutional change priorities, or as an ongoing and simple enterprise risk management tool for Board and management. (See the explanatory video on institutional excellence and the ***INEX***^{SM} framework at http://www.mendhurst.com/central-banking/)

Central banks that move beyond departmental business planning to develop functionally-driven strategic plans can achieve further benefits from re-thinking their risk management. Typically, risk management came along after strategic planning and management had already been established, or risk management was developed as a distinct activity carried out by different people. In those circumstances, the governance linkage between strategic management and risk management requires extra effort and is likely to remain too weak.

Instead, strategic management and risk management can be simplified and integrated by driving risk management from a functional basis. A single high-level risk profile can be developed for each external function, to reflect environmental factors and the degree of intended strategic change for that function. For internally-oriented functions such as human resources management and information technology, risk management can apply the ***INEX***^{SM} framework diagrammed below, to achieve holistic and institutional perspectives rather than a technical orientation. A single strategic monitoring and risk management report can then be developed to make governance oversight clearer, more effective, and more efficient.

Where from here? Like any governance activity, “ERM” needs to be simple but profound to be effective. How to move forward depends on what already exists. Change needs will fall into two broad categories:

- Central banks that already have extensive systems and resources for strategic management and operationally-oriented risk management will need to think afresh, to retain what adds net value and reform what does not. Obstacles and perhaps even resistance to change will inevitably arise, so strong Board-level sponsorship will be essential.
- Central banks that have not yet invested heavily in systems and resources for strategic management and risk management are luckier. They can start right, to achieve good returns in improved governance and management from relatively small investments.

In either case, circulating and discussing the text on “**ERM – Questions and Answers”** that follows would be a good starting point!

© John Mendzela 2019

Enterprise Risk Management (ERM) – Questions and Answers

What is enterprise risk management?

A top-level definition from Wikipedia says that “Enterprise risk management (ERM) includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives, assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring process.“

Wikipedia also notes that ERM is evolving. It quotes one expert comment that “the point of enterprise risk management is not to create more bureaucracy, but to facilitate discussion on what the really big risks are.”

Of course more specific and more technical definitions abound. There are plenty of methodologies and consultancy offerings on the market, often claiming to represent “best practice”. But the top-level definition rightly emphasises that the methods and processes of the chosen ERM framework must help achieve the organization's particular objectives.

Central banks differ from most other organisations, and also differ significantly from each other. So for any individual central bank, the challenge is not to copy the practices of others but to instead develop an approach to enterprise risk management that is “right practice for us” – sound general practices that are customised to suit that central bank’s particular circumstances.

And whatever approach is chosen, it’s vital to recognise that risk management is not something brand-new, but something that has always been part of everyone’s job. Aim to emphasise and improve what is already being done, not replace it.

Why is enterprise risk management important for central banks?

Absent or poor enterprise risk management will, sooner or later, lead to serious organisational failings. For a commercial business, that means major losses, going bust, being taken over or just dwindling away. That will have impacts on stakeholders– owners, employees, customers, suppliers and funders – but probably not much effect on the economy as a whole. Other enterprises will take its place.

© John Mendzela 2019

Central banks are however institutions, in the true sense of that word. Each central bank is a unique cornerstone of its national economy. And economies are increasingly interconnected globally. So serious failings at a central bank will have much wider impacts.

It's important however to distinguish between the routine technical activity of managing risks to avoid failure in specific activities and true enterprise risk management. Enterprise risk is more fundamental and enduring than any particular or immediate operational risks. If the central bank as an institution remains relevant and capable, it is likely to perform its policy, regulation and operational roles well. But if that institution is outdated, misaligned or just plain incapable, it is most unlikely to succeed. So enterprise risk management primarily means managing institutional risks.

What are central banks doing about enterprise risk management?

In most cases, too little of the right things and too much of the wrong things. A traditional presumption still operates that technical competence is all that really matters. So technical excellence and policy decisions receive high attention and investment, but managing enterprise risk to achieve and maintain institutional excellence is misunderstood or misdirected.

That misdirection is visible even in terminology, where central banks tend to talk about ORM – operational risk management – rather than ERM. And the techniques and tools applied by the risk management departments that many central banks have established take a bottom-up approach. Typically they develop extensive and localised "risk registers" for each area of operations, and generate detailed reports that encourage the Board and top management to think in compartments. Enterprise risk management is piecemeal and left to specialist support departments: HR, IT, finance and internal audit.

How can we change that balance?

To make enterprise risk management a reality, start at Board level.

1. Recognise that risk management in general and especially enterprise risk management is part of the Board's most fundamental governance role. So design of the entire framework should begin at the Board

© John Mendzela 2019

table, focusing on a strategic and long-term picture. Analysis should proceed top-down, not bottom-up.

2. Ensure the Board views the central bank's activity as integrated service delivery to stakeholders, rather than a collection of technical tasks carried out by specialist departments. Involve the entire board in enterprise risk management, not just the Audit Committee or some other specialised group. Expect Board members to act as part of a collective body governing the entire institution, not as overseers of individual portfolios.

3. Design reporting and discussion processes that keep the Board focused on the big risk management picture for the institution as a whole. Encourage "simple but profound" questions that question the status quo and challenge internal preconceptions or dogma.

4. Delegate the detail. Establish systems that keep accountability for managing operational risks with the responsible managers, and escalate to the Board only when failures are likely to have a major impact or display systematic patterns.

Doesn't that demand new management systems?

For routine finance and operations, no. Central banks typically have well-established internal audit and control systems, and mechanisms to follow up operational problems or control failings. In my experience, financial losses and operational errors typically arise not from weak systems, but through failure to operate controls well or from exception situations that could and should have been contemplated in advance. Mechanisms for learning are also sometimes too weak. But risk management for routine finance and operations can usually be improved just by enhancing existing internal audit and control systems, and ensuring organisational culture and manager attitudes support those systems. New systems to "manage risk" are rarely needed.

Broadly speaking, risk management of operations and routine finance requires just three things:

1. Strong business processes, documentation and controls
2. Capable and respected internal audit
3. Culture and incentives aligned with risk management goals

© John Mendzela 2019

What about major investment operations? Isn't a "Middle Office" essential?

Yes and no. Central banks certainly face major financial risks such as exchange rate movements that need to be managed or at least monitored. But special structures are not in themselves an answer. For example, a "Middle Office" dominated by those in charge of market operations may just be false comfort. And I have frequently encountered "Investment Committees" that through their membership or overly technical orientation provide no effective governance oversight at all. One central bank considering structural change in this area benchmarked against five different central banks and found five entirely different organisational structures, each of them apparently effective.

So information flows and culture matter far more than structure. Some formal mechanism to manage major financial risks is essential, but that should be seen as just a specialised part of managing operational risk. Governing major financial flows is likely to demand a "Funding Committee" that operates from governance level, receives independent information flows, and is NOT dominated by technicians or technical agendas. And that committee's scope should extend over all aspects of strategic funding and balance sheet management, not just foreign reserves.

What about policy and regulation risks? Aren't they different to operational risks? Shouldn't the Board be directly considering them?

Discussion about "policy and regulation risk" can be misleading. For a central bank, developing and implementing policy and regulation are really just inherent parts of operations. They comprise specialised business functions that central banks perform. The technicalities are different and greater than in more concrete operations, but the governance and management challenge – including risk management – remains the same.

Policy and regulation work in central banks should not be seen as "unique" or "special", or be exempted from the disciplines that should apply to all business processes. For example output definition, performance standards, work process documentation, "kaizen" (continuous improvement) techniques, activity costing and even independent audit can and should be applied to policy and regulation work.

© John Mendzela 2019

In particular, too much compartmentalisation of specialist activity – often referred to as “working in silos” – limits governance oversight and undermines risk management. Systemically, that can be remedied through an appropriate mix of structure, documentation, review and audit. The right organisational culture also plays a crucial role.

And yes, the Board is likely to play a more intensive role in policy and regulation oversight than it does in other operational matters. Exactly how that happens will differ between central banks. But that Board role in those functions, including consideration and management of the specific risks of a range of options, is different from governance and risk management of the central bank as an enterprise.

© John Mendzela 2019

What should information flows in an institutionally-oriented enterprise risk management framework look like?

At the top level of management and the Board table, just a single page. For example, after applying the ***INEX***^{SM} dimensions of institutional excellence, a Board member might receive a colour-coded table like this:

Dimension	Target Outcome	Achieved?	Verified by?	Comments
1. Mandate	• Clear and cohesive? • Feasible to achieve? • Accepted by stakeholders? • Not compromised by mandates of other entities? • All activities mapped to it?		CB statute External advice External surveys Chart of functions and outputs	Overlap with bank supervision entity still unclear Performing a few historic activities outside mandate
2. Governance	• Stakeholders represented? • Demonstrable capability? • Professional governance standards visibly met? • Clear roles and boundaries for Board and Governor? • Timely, complete and clear information to Board?		Institute of Directors guidelines Director CV's Board charter Standardised Board report formats	Benchmarking not complete No Board evaluation process Reports are still too detailed and overly technical
3. Funding	• Accounting done to full international standards? • Capitalisation sufficient to cope with most shocks? • Profitability adequate to support normal operations? • Budgeting and costing systems by function? • Capitalisation enforceably protected or guaranteed?		External audit Scenario analysis Annual budget Distribution provisions in CB statute	Net equity <2%! Profit too low to fund operations and rebuild capital Budgeting and costing only annual, and only by department No multi-year distribution policy
4. Culture				
5. Reputation				
6. Capability				
7. Organisation				
8. Management				
9. Communication				
10. Review				
11. Change Management				
12. Crisis Management				

© John Mendzela 2019

For the first three dimensions, this example states and scores five criteria for achievement of target outcomes. It identifies how that score has been verified, and comments on specific issues and improvement routes. The result suggests that

- deficiencies in mandate are relatively minor and probably manageable over the medium term
- governance risks need significant attention, but the problems seem well understood with action underway
- major risks are apparent in funding. The CB balance sheet has been "hollowed out". Capitalisation is inadequate and not protected. Internal financial management seems poorly developed

The example does not refer to any particular central bank, but it does identify issues in those early fundamental dimensions that are likely to be similar across most central banks. The later dimensions in the table are likely to be much more customised and specific. For example, the target outcome for culture is likely to reflect history, national culture, institutional maturity and other factors. And the reputation target for a mature central bank in a developed economy is likely to differ significantly from the target for a central bank in an emerging economy. Capability, organisation and management targets will all need tailoring to specific institutional circumstances. Targets for the final dimensions may need to remain relatively rudimentary until earlier dimensions are scoring well.

The achievement rating should as far as possible be determined by objective evidence, ideally with involvement from an independent external party. Although some element of subjectivity is inevitable, the use of a colour-coded scale should identify for the Board where improvement to achieve agreed target outcomes is most urgent. Appropriate actions and projects can then be generated.

What detail might exist below such a top-level report will vary. Operational, financial and "policy" risks should be delegated and managed with no routine Board attention, just a "red alert" system to escalate serious or systematic failings. Specific initiatives to remedy identified deficiencies in enterprise risk management can proceed under project disciplines with Board or governor sponsorship and monitoring.

Does the scope and capability of internal audit need to change?

Perhaps not greatly. In many central banks, internal audit has already reoriented from traditional compliance activity towards risk-based

© John Mendzela 2019

prioritisation of internal audit work programs. It then becomes routine and natural for managers and internal audit to collaborate in identifying, managing and controlling operational risk. But often there are opportunities to increase the value added by internal audit:

- audit cross-functional business processes, not just “departments”
- end the outdated distinction between traditional audit and “ICT audit”. Today, virtually all business processes involve IT. Some internal auditors will specialise more highly, but all need high ICT capability
- avoid competition or duplication between internal audit and risk management. They are aligned and complementary disciplines
- don’t “stretch” internal audit beyond its inherent competence. Audit of some policy and operational activities will require specialist external expertise. And internal audit cannot reliably assess governance quality, management skill frameworks or technical training needs

How should strategy and risk be linked? Can they be governed and managed in a single framework?

Intuitively, strategy and risk have always been two sides of the same coin. Setting strategic priorities and making strategic decisions should only occur with an intense awareness of their associated risks. And implementation of strategy should automatically include appropriate measures for managing and mitigating risk. But longer-established formal processes for strategic planning and management and the (usually) more recent formal processes for risk management are often not well linked. Governance bodies find it difficult to fully appreciate, balance and trade-off the benefits and risks of alternative options.

As noted earlier, opportunities exist to integrate functionally-oriented strategic planning, monitoring and management with governance-oriented risk management. A simple and unified view across strategy, operations and risk will mitigate the inherent tendency for departments, managers and technical detail to drive institutional thought and action. The Board can govern all external and internal enterprise activity more effectively, and with less time and effort.

The definition we started with emphasised that enterprise risk management is an evolving discipline. What is its future direction?

No-one can answer that question comprehensively (though some might claim to!). But we can identify some clear trends, to thoughtfully follow:

© John Mendzela 2019

- Accept that traditional audit and control concepts should contribute to thinking about risk management but not dominate it. Outcomes, not procedures, matter most. Thinking on risk management should have broad scope and future focus, and challenge the status quo. The right sort of "Risk Management Adviser" or office, probably operating from within the "Strategic Management" function, can help
- Place less reliance on formal tools, structures and controls. Create an institution-wide culture of risk management awareness
- Appreciate the limits of quantification. Some "black swans" – extreme or unprecedented events - cannot be predicted or planned for with statistical tools or analytical frameworks
- Widen scope to recognise human behavioural impacts. One obvious example is that even the best technical cybersecurity cannot succeed if people within the organisation act carelessly or thoughtlessly. But our human brains and emotions also play more subtle tricks, such as encouraging us to ignore or underestimate "grey rhinos" – the risks inherent in what is familiar
- Shift emphasis from prevention of foreseeable events to prompt mitigation of unpredictable challenges. Seek to build responsiveness and resilience. A spirited and innovative culture will have more value than a formal crisis or continuity plan
- Think beyond organisational boxes. Managing increased interconnectedness between different risks requires cross-fertilisation and teamwork, internally and with external parties

And remember that to genuinely achieve enterprise risk management, it's that first word that matters most. Focus on institutional risk, start with the Board table, and keep your "ERM framework" simple.

© John Mendzela 2019