ISSUE 85

protiviti®
Face the Future with Confidence

Board Perspectives
Risk Oversight

Positioning Independent Risk Management to Succeed

In many organisations, board risk oversight is enhanced when the board and executive management are supported by an effective independent risk management function. Positioning the chief risk officer (or equivalent executive) and the independent risk management function – which we refer to collectively as "CRO" in this publication – to deliver to expectations requires an understanding of how the CRO role can succeed.

The ultimate advocate for risk management in any enterprise is arguably the CEO. However, CROs are unique in that they are often expected to provide a voice that champions the protection of enterprise value at crucial decision-making moments when a given strategy, transaction or deal is under scrutiny or is likely to expose the organisation to unacceptable risk. If they do not, who will?

Effective CROs are concerned with what the institution may not know. They must occasionally offer a contrarian point of view; otherwise, the decision-making process may end up flawed by "group think."

Key Considerations

Not all CROs are alike. However, there are factors that offer a discussion framework for positioning the CRO (and independent risk management) to succeed. Below, we discuss six of these factors.

Inculcate an "everyone is responsible for risk" philosophy – If the board, senior management and operating personnel believe that the CRO is the only position within the organisation concerned with risk, the game is over before it begins. The organisation has a major source of dysfunction lying in the weeds.

Six Success Factors for Positioning Independent Risk Management

1. Inculcate an "everyone is responsible for risk" philosophy
2. Integrate risk into opportunity pursuits and decision-making processes
3. Clearly define the CRO position
4. Position the CRO to deliver to expectations
5. Undertake a strategic focus
6. Foster effective board communication

Unless managing risk is an organisational imperative, with all responsible personnel aware of and owning the risks their respective activities create, it is really difficult for any CRO to be successful. Ideally, front-line business unit, process and functional owners should also be risk owners, or the first line of defence when it comes to identifying, sourcing, managing and monitoring risk. The enterprise's risk culture drives the "everyone is responsible" view.

Integrate risk into opportunity pursuits and decision-making processes – The board needs to be assured that management has not allowed past successes to breed overconfidence. Tension within an institution between its market-making and control-related activities is inevitable and should be encouraged. Striking the appropriate balance between the two is fundamental to what a CRO attempts to achieve. It typically begins with formulating and documenting a risk appetite statement approved by executive management and the board and driving it down to an operational level. From there, risk considerations are incorporated into decision-making processes, performance evaluations, compensation decisions and the discipline of monitoring the impact of changes in the business environment on the risk profile.

When making key business decisions, management discusses and reviews risk scenarios that facilitate an understanding of the interrelationships and impacts of critical risks that are germane to an effective decision. "What if" scenario planning, stress testing and other tools are baked into strategy-setting, business planning and forecasting processes to visualise the effect of potential future events on the institution's revenues, costs, profits, cash flow and market share, and how the organisation can respond to or benefit from them. These activities require acknowledgement from the top that there should be prudent boundaries and limits to entrepreneurial value-creating activities and that high-risk ventures are pursued in a transparent manner with the full knowledge of executive management and the board.

Clearly define the CRO position – Two distinct CRO roles exist in practice. While there are variants, an understanding of these two roles provides a context for framing the positioning conversation:

- The **"champion"** CRO advances and enables the organisation's risk management framework and plays the roles of coordinator and integrator to ensure consistency in application across operating units and functions. The champion CRO plays such roles as educator (as a provider of insights); facilitator (of risk assessments and formalisation of risk mitigation plans); and consultant, communicator and reporter.

  Champion CROs often establish, communicate and facilitate the use of appropriate risk management methodologies, tools and techniques; support evaluations of enterprise risks; and provide transparency into the capabilities around managing the priority risks across the institution.

- The **"line of defence"** CRO undertakes the activities of the champion, but also is authorised to play a combination of other roles. These roles include evaluator; initiator; approver (of policies and risk response design); escalator (of significant issues to executive management, including the CEO, and, through appropriate channels, the board); vetoer (of activities affecting compliance with established internal policies); and arbitrator (of disagreements between operating and functional units affecting risk management).

  In this broader role, the CRO establishes and communicates the organisation's risk management vision, designs and implements an appropriate risk management infrastructure, implements relevant action-oriented risk reporting to the board and senior management, maintains a watchful eye for evidence of a dysfunctional risk culture, and reviews compensation plans to consider the possible impact of risk factors and compensation on behaviour.

The line of defence CRO may not be authorised to assume all of these roles, but clearly reaches beyond a champion CRO with escalatory and/or veto authority. The key is for the board and CEO to have a mutual understanding of the CRO's role and function. In heavily regulated industries, such as financial services, the line of defence CRO is likely the preferred option. If the focus is primarily on understanding and coordinating an organisation's fragmented risk management efforts and reporting on the state of risk management, a champion CRO might work.

Position the CRO to deliver to expectations – To serve as a second line of defence, a CRO must have sufficient stature with business-line leaders and across the organisation. Stature comes from the authority, compensation and direct reporting lines that command respect. In short, for business-line leaders to collaborate effectively with the CRO, they must view the CRO as a peer. This positioning is accentuated if the CRO:

- Reports to someone who has strong influence on the organisation, such as the CEO or executive committee (with administrative reporting to an appropriate C-level executive);
- Has direct access to a standing committee of the board (i.e., through dotted-line reporting);
- Engages in mandatory, regularly scheduled executive sessions with the board or a standing committee of the board;
- Provides periodic reports and escalates issues to executive management and the board;
- Has influence on compensation practices incenting the desired risk management behaviours; and
- Is sufficiently resourced with an adequate support staff.

Undertake a strategic focus – Consistent with the premise that risks must be owned by the lines of business and functional activities that generate them, the CRO generally operates in a strategic oversight role with authority vested by the executive committee (or a designated risk management committee), the CEO and/or the board (or a committee of the board). The CRO's focus must be on understanding enterprise risk, monitoring changes in the risk profile and aligning risk with the desired tolerances for risk.

Ideally, the CRO is accountable for enabling the efficient and effective governance of truly significant enterprise risks, and related opportunities, for the institution overall and its various lines of business. The board needs to ensure that there is an appropriate risk focus. Certainly, the CRO role should not be perceived as a check-the-box compliance function that forces the business to follow rules imposed on it, as opposed to linking risk and opportunity effectively when creating and protecting enterprise value.

Foster effective board communication – The CRO should have open and free access to the board (or a board subcommittee). For line of defence CROs, the board must be vigilant in ensuring that there is nothing constraining the CRO from reporting to it when significant risk issues arise. To that end, a formalised escalation process should exist, such as written procedures and agreements requiring escalation of any significant issues raised by the risk management function that are being argued by business-line executives, even in circumstances where the CEO resolves disputes between the first and second lines of defence.

Since we are not talking about a one-size-fits-all approach to the CRO role, we must acknowledge there are no "hard and fast" rules. Positioning the CRO function within the organisation is more than defining the role. The depth and breadth of the CRO's relationships with senior executives and business-line and functional leaders have a significant impact on the CRO's effectiveness and the sustainability of the position as it is defined. The stronger these relationships, the more effective the CRO will be in realising the intended value proposition. As expectations increase, the need for more sophisticated risk professionals grows.

Questions for Boards

If there isn't a CRO (or equivalent executive) and/or an independent risk management function in the organisation, the board may want to inquire as to why in the context of the nature of the entity's risks inherent in its operations. If a CRO exists, the board of directors may want to consider the following suggested questions:

- Does the CRO role and independent risk management function constitute an effective second line of defence? If not, should it?
- Does the CRO have access to the board or to a committee of the board?
- Are there signs of ineffective positioning of the CRO or the independent risk management function within the organisation? For example:
  - There is lack of clarity in the CRO role and how it interfaces with senior line and functional management.
  - Risk management is not valued as a discipline equivalent to opportunity pursuit.
  - The CRO is not viewed as a peer to business-line leaders.
  - There is no direct reporting line to the board.
  - The CRO is entangled in the minutiae of managing compliance and is seen as an obstacle to getting things done.
  - The CRO is constantly fighting turf issues with entrenched silos.
- Does the board leverage the CRO in obtaining relevant and insightful risk reports?

How Protiviti Can Help

Protiviti assists boards and executive management with assessing the risks inherent in the enterprise's strategy and business plans, either across the entity or at various operating units, and the capabilities for managing those risks. We help organisations identify and prioritise the risks that can impair their reputation and brand image and lead to failure to execute the corporate strategy successfully. We also assist CROs with improving capabilities for managing more complex market, credit, model validation and commodity price risks.