

ERM yourself

A proper enterprise risk management programme must be implemented from the top down, while a captive insurance company can enable a more robust ERM process, if properly managed, says Temple University's Michael Zuckerman

How do ERM programmes work and how have they evolved in recent years?

An enterprise risk management (ERM) programme requires recognition that exposures to loss and adverse events do not occur in a silo. So why manage them as if they are? An adverse event has a cascading impact affecting the entire organisation. For example, a factory explosion results in the loss of a plant, equipment and bodily injury. The loss will also disrupt the organisation's supply chain, interrupt operations, make it difficult to recruit and retain skilled employees, increase expenses, and reduce revenue and profit, which in turn impacts on corporate value, possibly increasing the cost of capital.

Ultimately, there will be negative consequences for a firm's reputation, which may cause the downward spiral towards lost market share and even bankruptcy. At the end of the day, ERM is about building a resilient organisation.

A successful ERM programme must, therefore, begin with the board of directors holding the senior managers responsible for driving the ERM process across the organisation. The process must address all risks, including the upside and downside. And it must foster a risk culture characterised by strong risk-based communication across the enterprise, including regular reporting to the board on material risks, and how they are being addressed.

To do this, risks must be properly identified and assessed at the strategic and operational level. A firm must understand its appetite and tolerance for risk. And it must use tools to enable risk prioritisation, and establish risk owner accountability to ensure that risk is being properly managed across the organisation. Risk identification and assessment is the critical component of ERM. It goes without saying that this requires strong data management skills.

This process sets the ERM agenda and creates the focus on measuring residual risk, or in other words, identifying the opportunities to improve risk mitigation for those identified significant risks. A captive insurance company can enable a more robust ERM process, if properly managed.

How would a company incorporate cyber risk within an ERM programme? What are the challenges specifically with cyber?

The ERM programme must absolutely address cyber risk. It is a material risk from which good things can flow if managed properly, otherwise it could have disastrous consequences if mismanaged. The cyber exposure, if mishandled, will damage corporate value and possibly trigger a shareholder suit against the directors. The cyber ERM programme must provide for a strong threat detection system, IT security/loss prevention and cyber risk financing, which should consider employing a hybrid approach using a captive insurance company and commercial insurance and reinsurance. Finally, an exceptional post-breach response programme is crucial.

What are the features of a successful ERM programme?

For an ERM programme to be successful the board needs to understand the firm's significant risks and how they are being mitigated. There should also be a strong enterprise-wide risk identification and assessment process. It is important to understand the firm's stakeholders and the risks associated with these relationships. Effective ERM communication should be in place across the enterprise and an efficacious risk information management policy should be used to assess and manage risk, as well as a focus on managing residual risk, and risk financing.

A successful ERM programme will also need a resilient organisation that is able to address what it does not yet know and finally, it will use a transformative captive insurance company that enables an organisation to meet its strategic objectives.

What other risks can companies use an ERM programme for?

All risks must be addressed by ERM. The question is what material risks could be partially funded in a captive insurance company. The answer to this question, of course, is that the captive should be used to fund any risks that are predictable, usually high frequency and low to moderate severity. The goal is to employ a hybrid strategy to fund a portion of this exposure to the extent that the variation of retained actual losses from expected losses can be managed by proper capitalisation and funding of the risk within the captive. The highly volatile portion of this risk can then be transferred to the reinsurance market.

What does the future of ERM look like for captives?

It is very bright. We are seeing a modest increase in the amount of specialised risks like cyber, supply chain and terrorism being partially funded in a firm's captive insurance company. Again, if the captive is properly managed, according to best practices, it will raise the visibility of risk management within the enterprise. **CIT**

Michael Zuckerman
Assistant professor
Temple University

