Risk Management

ARTICLE SERIES - 2020 / 01

Vestinex

Photo by Loic Leray on Unsplash

Risk Management

Critical component of business resilience

Today's complex and constantly changing organisational environment creates significant business risk that poses genuine and real challenges for management. Risk propagates in a variety of forms including but not limited to strategic risk, operational risk, financial risk and Information Technology risk all of which can impact your organisation if not well understood, analysed and mitigated through appropriate measures and controls.

What is Risk Management?

So what exactly is risk and what does it truly mean to risk manage?

In our experience, this question posed to any level of management within an organisation results in responses that are varying and wide ranging. There is of course no single accurate answer to this question. What is a risk to one person may be considered an opportunity to another. Therefore, the only true measure of risk is the person or organisation themselves, formed by what they perceive, based on their knowledge of the organisation, experience in that particular industry and the environment in which the organisation operates.

At a base level risk is "*any situation which has the potential to adversely impact the normal operations of the organisation*". Many organisations make risk management far more complex than is required. This is largely the result of not having a thorough understanding of risk nor truly understanding the application and purpose of risk management processes.

Risk Management therefore is the discipline through which to identify, assess/understand, analyse, mitigate, control and report on potential threats and impacts to the organisation. This is required by the organisation in order to determine the selection of appropriate treatment strategies designed to avoid, eliminate, transfer or accept the risk in the context of the organisations operations.

Contextualisation of Risk to the Organisation

To properly manage risk, practitioners and organisations must first critically understand their operational environment. Practitioners must have the ability to assess, analyse, determine root cause, prioritise and implement effective strategies to mitigate identified risks. Failure to understand both the operational environment and the risks faced by the organisation leads to an inability to control the risk and the potential to adversely affect the organisation and its operations.

Contextualisation of risk to the organisational environment is critically important to confirming an accurate assessment of the risk.

Generic risks relevant to one organisation may not be applicable to another, and hence a one size fits all solution is not a realistic solution or approach. On the above basis it stands to reason that a thorough understanding of the organisation, its strategies, objectives, functions, people, processes and technology must be known and understood by risk practitioners as part of the risk management process in order to prepare an accurate assessment.

Risk Methodology and Process

Whilst there are varying methodologies for the completion of risk assessments the primary elements of any of those methodologies contain the following:

- **Identify** – Identify the risks and threats to the organisation from internal and external sources. Identification should cover all areas of the organisation such as strategic, operational, data/information, people, process etc.

- **Assess / Evaluate / Analyse** – Assess the identified risks in the context of the organisation including the determination of the root cause, likelihood or the occurrence of the risk, consequence of the risk occurring and rating the risk in accordance with the organisational risk profile and risk appetite

- **Mitigate / Strategise** – Determine relevant mitigation actions and strategies to avoid, transfer, mitigate or accept the identified risks

- **Implement / Monitor** – Implement the selected mitigation/ treatment strategies and implement continuous monitoring to assess the ongoing effectiveness of the strategy

- **Report** – Regular reporting on new and emerging risks and the current status of previously identified risks to senior management and the board

Root Cause Analysis

A significant issue with the completion of many risk assessments is the failure by practitioners to analyse the “root cause” of the risk or more literally speaking, understanding and treating the core elements that generate the risk. If the root cause is not mitigated many risks can be generated from a single common cause. Treating the risk symptoms without identifying and treating the root cause does not rectify or mitigate the risk. Conversely, treating the root cause has the potential to mitigate multiple risks directly or indirectly.

Assessment of Likelihood, Consequence and Rating

Many organisations attempt to blindly adopt recognised industry standards, create and use standard criteria for the specifications of likelihood and consequence leading to the assessment of risk rating. Use of generic specifications such as that depicted within the AS/NZS ISO31000:2018 Risk Management standard whilst an excellent base guideline do not take into consideration the context of the organisation, and require contextualisation to the organisation for effective use.

Risk practitioners should understand the operational environment and develop criteria for each level of Likelihood (Very Unlikely -> Almost Certain) and Consequence (Negligible-> Catastrophic). This is a critical requirement as the criteria upon which these levels are based is individual to the organisation especially in the area of Consequence. Similarly, consequence should be measured by organisations across a number of categories such as Financial, Reputation, Regulatory, People etc. and specific criteria across each category defined.

This process will allow risk practitioners and general staff alike to accurately determine a true risk rating based on sound and defensible assessment criteria. Over time these criteria can and will change, and organisations, especially those in fast to market environments, must review and update the criteria and hence risk ratings regularly.

Contextualisation of the risk matrix is similarly important, as it is based upon the criteria established for likelihood and consequence. In some instances contextualisation of the matrix itself can better support the risk processes. Hence, organisations should carefully consider the suitability of generic matrices before their blind application.

Design and Implementation of Mitigation Strategies

Once the organisational risks have been identified, assessed, analysed and rated (or prioritised) stakeholders need to identify and implement viable, cost effective strategies that mitigate and control the risk to the business.

Careful consideration must be given to the types of strategies implemented to reduce the risk to an acceptable level. The greater the level of risk to be reduced, potentially the more costly for an organisation the strategy will be to implement. It is often the case that a relatively easy to implement strategy such as a policy can be effective in the mitigation of risk at a low cost.

Prior to the development of any risk strategy practitioners should determine the type of strategy or control that is to be implemented. There are four key treatment types which are Avoidance, Transfer, Mitigate or Acceptance.

The selection of the treatment options will dictate the type of strategy or control that is implemented by the organisation to reduce the level of risk to an acceptable level. Avoidance strategies include strategies that control the risk by removing the source of the risk (i.e. not completing a particular business transaction). Transfer strategies include items such as Insurance to transfer the entire or at least some portion of the risk to another party (i.e the insurer). Mitigation strategies are those that implement a control environment designed to reduce the level of risk to an acceptable level whilst achieving the business objectives. Finally, Acceptance of the risk level by the organisation is a valid treatment option if no other strategy or control is available (i.e external risk factors outside of the control of the organisation).

Regardless of the treatment strategy selected all must be carefully examined and considered by the organisation. The primary strategies should be those that allow for the achievement of the business objectives whilst minimising risk to the organisation and may be a single control strategy or more likely a suite of controls working together for the common goal.

Oversight, Governance and Control

Risk is an ever changing and fluid manifestation of modern organisations. As such, risks to the organisation its functions and its operations are constantly changing due to being affected by internal and external factors. Practitioners need to ensure that risks are not only assessed but are regularly reviewed as part of the organisations Governance and Control framework. It is essential to the ongoing management of risk that an oversight function by the Senior Management of the organisation and the Board (where relevant) is implemented and that risk is placed high on the corporate business agenda. Failure to do so can lead to regulatory , compliance, reputation and financial implications from which the business may not recover.

The adage "*it takes 20 years to build a reputation and 2 minutes to destroy it*" has never been a truer statement when it comes to risk management.

Professional Biography

Jason is the Director and Principal Consultant for Vestinex Pty Ltd and has over 26 years in the areas of Fraud Investigation and Prevention, Risk Management, Information Technology Audit and Security and Business Continuity / Emergency Management planning. Jason has formerly held investigation and advisory roles within Government and professional service firms. Jason holds a Diploma of Policing, Certificate IV in Government Fraud Control and Investigation, Certificate IV in Training and Assessment and a Bachelor of Science in Computing Science (1st Class Hons). Jason is also a licenced private investigator in NSW.

E: jason.Plumridge@vestinex.com.au

M: 0417 703 638

About Vestinex Pty Ltd (“Vestinex”)

Vestinex Pty Ltd is a professional business services provider based in Sydney, Australia. We pride ourselves on being a boutique provider which places us in a position of being able to provide a range of valued added business services to our clients as part of an integrated client focused team. This approach enables Vestinex to assist our clients to achieve their strategic and operational goals and achieve success in their business operations. We measure our success by the role we play in our clients success. Vestinex promotes to each and every one of our clients our motto of “Establish, Control, Succeed”.

- *Establish – A sound basis of policy, structure, planning and culture which breeds success and trust within the organisation with clients, customers and the market*

- *Control – Define and operate a comprehensive control, compliance and management function to ensure that business operations are effective, efficient and key risks across the business are managed appropriately*

- *Succeed – Success is borne out of solid management, engaged employees, trust in the market and strong leadership*

Website http://www.vestinex.com.au

Twitter: @vestinex

Facebook: https://www.facebook.com/Vestinex