Industry Forum
Business Excellence Through Inspired People

Risk Management

The future has always been uncertain, prone to surprise us. We all learn to live with this condition with more or less success. Where large sums of money are at risk a more systematic approach has grown up. One example is audit where a risk based approach has been adopted. Auditors examine those parts of the organisation whose operation could have serious consequences in future. The priority is to scrutinise the areas where the potential negative impact is greatest.

The whole insurance industry is another example of risk management that everyone is familiar with. The key idea here is risk sharing to reduce the potential cost to individuals.

Risk management also has been developed as a body of knowledge and practice in the investment community. The key idea is the distribution of possible profit outcomes for a particular project or programme. If this distribution is understood then it will be easier to take action which reduces the likelihood of a negative outcome. If this perspective is used routinely then an investment business will secure better overall returns.

It is now widely recognized that the current business environment has shifted in directions which make risk management more pertinent. VACU is the acronym which summarises the current environment as more volatile, ambiguous, chaotic and uncertain. A number of different trends have come together to make this state of affairs ranging from geopolitics to the rapid spread of digital tools and techniques.

In 2009 the International Standards Organisation issued ISO 31000 covering principles and practices of risk management which is aimed at any organisation of any size in any sector. The standard is intended to help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.
ISO 31000 cannot be used for certification purposes, but does provide guidance for internal or external audit programmes. Organizations using it can compare their risk management practices with an internationally recognised benchmark.

Business services organisations are offering an increasing range of products to help firms strengthen their risk management capability. For example Deloitte suggest an effective capability will engage senior management, have a strategic focus, have a risk sensing function which includes the use of sources external to the firm, use a mix of digital and human elements, have quantitative outputs and produce time series data. The UK training market is developing with, for example, two day introductory courses to risk management now available.

SMMT Industry Forum Ltd
2680 Kings Court, The Crescent, Birmingham Business Park, Birmingham, B37 7YE
T +44(0)121 717 6600 F +44(0)121 717 6699
www.industryforum.co.uk enquiries@industryforum.co.uk twitter @smmtif

Industry Forum
Business Excellence Through Inspired People

Health and safety at work involves certain legal obligations in respect of the workforce but is not for the most part seen as a strategic aspect of business. Nonetheless risk management is a core function and in the UK the Health and Safety Executive make available free online an excellent set of resources, tools and techniques. There is probably in most organisation some capability to use such tools effectively at operational level. The challenge is to develop that capability so that it can operate at strategic level.

Military and security planning is another domain where there is good experience of risk analysis. For example the fundamental process is to first identify an asset and a threat to it. The next stage is to review the existing level of protection to identify the vulnerabilities. Prioritizing vulnerabilities provides the basis for a work programme.

For many organisations the new global standard on digital payment security will also be a useful resource. This is version 3.1 which was released in April 2015. The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, JCB, and China UnionPay. The standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.
It was created to increase controls around cardholder data to reduce credit card fraud via its exposure. Validation of compliance is performed annually, either by an external Qualified Security Assessor that creates a Report on Compliance for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire for companies handling smaller volumes.

There is some evidence that firms are reluctant to implement the standard because of its complexity and expense. Also there is worrying evidence that senior managers in the UK routinely take unnecessary risks in project management even though project complexity is increasing thanks to digitalisation. For example in project management it is well established that quality, cost and timeliness are hard to optimise as a totality. Typically it is safer to specifically select which of the possible pairs are the priorities for any given project. However reviews of project failures in the UK still find that the most common cause of failure is the unrealistic targets set by senior management at the start of the project.

Almost everyone has heard of SWOT analysis as part of strategic planning and clearly any alignment of weakness and novel threat will be a big priority in strategic risk management. Many people are also familiar with the environmental scanning framework, PEST, covering political, economic, social and technological domains. This is frequently extended to cover legal and environmental and also sometimes ethics and demographic. These extension raise the question of how risk is segmented in strategic risk management.

ISO 31000 uses a risk management process which consists of the three steps: Establishing the Context, Identification and Assessment. Establishing the Context means that all the possible risks are identified and the possible ramifications are analyzed thoroughly. The best segmentation of risk for a particular firm should be clarified in this phase. It is worth remembering that risks could be either internal or external - possible internal risks might be employees of the company or operational inefficiency in a certain process.