

On high alert

Solutions to managing security-related risk

Security, or rather the lack of security, results in a variety of effects that lead to uncertainty with respect to the achievement of societal and organizational objectives. The use of the term “security” implies that there exists the threat of risk – whether from terrorism, cyber-security or identity threat – and that dire measures need to be taken in order to secure society from these threats.

Following the publication of ISO 31000:2009, *Risk management – Principles and guidelines*, the management of risk has moved from a focus on financial, operational, market, employment, insurance and reputational risks to a broader approach based on the effect of uncertainty on the achievement of organizational objectives.

A consequence of focusing on the effect of uncertainty on objectives is that the management of security risk has moved from the shadows into mainstream management. A risk-based approach to security draws the attention of the organization’s board and top management. It also results in transparent decision-making with respect to risks that threaten the ongoing sustainability and resilience of an organization. It also requires that appropriate accountabilities and responsibilities are assigned at each and every step of the management process, and that all security risks have an owner.

The involvement in, and management of, security risk by top management ensures that the control and treatment of events, often outside the experience of an organization, are properly addressed. The end goal is to provide the best outcomes for the achievement of the organization’s objectives. Security risks are identified, assessed and treated as part of the overall management of organizational risk, resulting in greater understanding of the need for the organization’s investment in security related treatment.

The formal inclusion of security risk is a vitally important part of an effective organizational approach to the management of risk that should fit seamlessly into an organization’s management system. It introduces a new element: the concept of someone deliberately introducing an

exposure to potential harm and seeking actively to bypass existing controls. The potential consequences of security risk also need to be addressed in the organization’s plans for managing disruption-related risk so as to ensure that the required capability, resources and knowledge are available and accessible to support the achievement of these key objectives.

*ISO 31000
is a must-have
solution for all.*

An effective enterprise risk management system (ERM) will ensure that security-related risk is interlinked with all other risk management activities being addressed (e.g. safety, environmental, marketing, reputation, regulatory, financial, etc). It must be clearly understood that the only differences in approach relate to the application of discipline specific knowledge and skills that relate to each risk area – the overall principles, framework and process remain the same.

While many security risk activities may be conducted by specialist areas, many will also be conducted as part of the way other organizational units routinely address their risk exposures (e.g. managing employment-related security risks should be a fundamental human resources accountability whilst information technology (IT) related security risk should be an accountability of IT management).

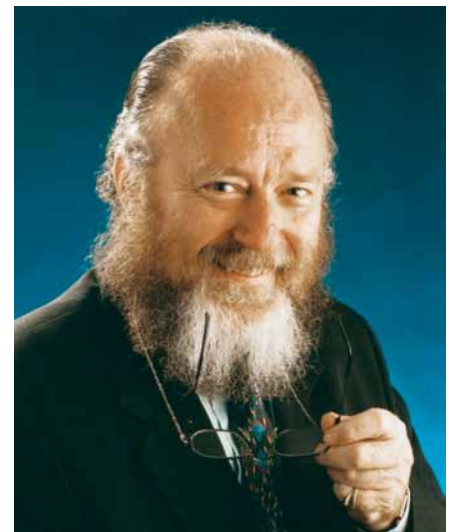
The management of risk is critical to effective decision-making that ensures strategy and controls are more appropriately applied. It provides an interface between such decision-making and the implementation of key functions, processes and

infrastructure, which are required to achieve organizational objectives.

The management of security risk requires those accountable to have a thorough understanding of the risk management principles, framework and process first and foremost. This must be complemented by a thorough understanding of the specific security disciplines. In the current environment, security within society or an organization cannot be left isolated from all of the other management processes and systems.

Security should encompass issues such as strategy, governance, ethical conduct, safety and organizational performance. For the management of security risk to be successfully integrated into the fabric of society and organizations, it must become an integral part of how they operate by becoming as fundamental as financial and human relations management, communication and decision-making skills.

ISO 31000 is a must-have solution for all organizations and the whole of society. It provides best practice guidelines to effectively manage security-related risk, and in so doing, maximizes opportunities and minimize threats for the benefit of all. ■



Kevin W. Knight AM*
Chair of the ISO working group that developed ISO 31000:2009.

* Member of the General Division of the Order of Australia.