The ISO 31000 Standard: a different perspective on Risk and Risk Management

An analysis from a security perspective

The biggest challenge for security managers is to demonstrate the value added by security. It is not an easy task for risk management to argue the return on security investment (ROSI), but it is certainly not a mission impossible. In many organizations with a lower maturity in security risk management the link between investment in security and the value added is not sufficiently explained and justified. Costs for security are therefore regarded as a necessary evil, mainly to meet legal obligations. In more mature organizations the link between security and the value added are well understood, therefore investments in security are related to the protection of value already created within the organization. But can security management also effectively create new value?

To answer this question the term “risk” needs to be clearly defined. If a risk is defined as a danger, a threat or discontinuity, then risks are seen as purely negative. With this logic the risk management costs are seen in the worst case as an inevitable and necessary evil, or in the best case as protection of the value already created in the organization. The decision to take action in risk management is often the result of a necessity (an incident or immediate threat), of unavoidability (we must do something) or efficiency (this seems the best way).

A *negative* approach to risk is rather narrow. To achieve objectives inherent risks are unavoidable, but this can also be positive instead of negative.

An event or incident with negative consequences may ultimately have a positive impact. The consequences of September 11, 2001 can still be felt today, including several negative consequences. There are however also positive consequences as a result of 9/11.

One of the consequences of 9/11 is the ‘securitization’ in the fight against terrorism. ‘Securitization’ is a concept that was introduced by the Copenhagen School and is a constructive approach to (international) security. The term refers to a process whereby policies are increasingly implemented in the field of national security including a wider application of security measures.

The laws, regulations and policies in counterterrorism policies are characterized by this broader approach.

Examples include the introduction of the International Ship and Port Facility Security Code (ISPS) and the Authorized Economic Operator (AEO). The European program for the protection of European and National Critical Infrastructure (EPCIP) concerns a new security system for the protection of critical infrastructure against terrorist attacks.

These measures will help to prevent that the threat manifests itself (discouragement / prevention) and prepare us to respond quickly and effectively in the event of a threat, however it remains difficult to determine the effect. We therefore need to have a broader look at risks in general and more specific at security risks.

The answer to the question whether risk can also create value is contained in a quote from William Shedd: “A ship is safe in harbor, but that’s not what ships are for.”

Ships are built to sail. Sailing ships realize goals and objectives. The objectives of manufacturers exporting goods, the objectives of shipping companies, importers, end consumers…

“Opportunity is Risk and Risk is Opportunity.”

There are risks with potential adverse consequences associated with sailing, but the objectives of the manufacturers, shipping companies, importers and end users cannot be achieved without taking any risk. During sailing the effects of the risk can be negative and/or positive.
In the example of the ISPS and AEO regulations companies who choose to comply with ISPS and AEO compliance also create numerous commercial benefits. ISPS promotes international trade and the AEO certificate delivers in addition to “supply chain security” a boost for international trade and a considerable saving in time during custom clearance, thus financial savings.

Speaking the same language

To assess the value of risk management one must speak the same language and use generally accepted definitions of risk and risk management. The ISO 31000 offers a basic vocabulary for risk and risk management definitions. The ISO 31000 standard for risk management defines risk as the effect of uncertainty on objectives. Risk management is defined as the coordinated activities to manage and control risks within an organisation.

This opinion opens up many possibilities: it is not possible to discuss risks without discussing objectives. Risk management should therefore closely linked to the protection of value and ultimately the creation of value. The contradiction between optimization of value and the (unavoidable) costs contributed to risk management is a paradox, only a seemingly contradiction.

Two other standards are linked to the ISO 31000 standard: ISO 31010 which provides an overview of risk management methods and the ISO Guide 73 in which 51 concepts of risk and risk management are defined (29 concepts have been incorporated into the ISO 31000). These two standards support the use of the same language.

Structure based on three pillars

The structure of the standard is based on three pillars: the principles, framework and process.

The text in the ISO 31000 standard is short, clear and relatively easy to understand. Nothing in the text is radically new and the principles describe good practices that are generally accepted. The framework is based on Deming’s ‘Plan-Do-Check-Act’ cycle and the process represents international best practices in risk management.

The Principles

The view of the principles is that risk management should firstly be focused at the creation of value and thereafter the protection of value.

Risk management should be an integral part of the organizational processes of an organization, be considered in the decision making process and explicitly take the factor of uncertainty in consideration.

Risk management must be systematic, structured and timely organized. Risk management is based on the best available information such as historical data, experience, feedback from stakeholders, observations, predictions and advice from experts ... Risk management is always tailor-made and considers human and cultural factors.

Risk management is transparent and does not exclude anybody, when appropriate there needs to be communication and feedback between internal and external stakeholders. Finally, risk management is dynamic and a continuous process of adaptation to change and improvement.
The Framework

It is essential that the framework is based on a mandate and commitment from top management. The design of a framework for managing risks in an organization is based on an understanding of the internal and external context of the organization (political, economic, social, technological, legal and environmental context).

From this a policy statement must be developed, responsibilities defined, risk management integrated into the organizational processes of the organization, the available resources for managing the risk identified and the internal and external reporting process outlined.

Once the framework has been established the implementation of the framework and the process follows. The framework should be monitored and evaluated continuously to ensure continuous improvements.

The Process

The risk management process also starts with a good definition of the internal and external context of the organization, but only in more detail. The basis of the process consists of the following steps: risk identification, risk assessment and risk evaluation. Following on the risk evaluation the next step is risk treatment during which various options and/or combinations of options are probable namely; avoiding the risk, acceptance or increase in the risk based on opportunities, removing the source of the risk, responding to the likelihood or consequences of the risk, sharing the risk with other parties... During all the stages there should be appropriate communication between internal and external actors and continuous monitoring and fine-tuning of the process.
International Consensus

The ISO 31000 standard was published in November 2009 after receiving approval from more than 75% of the ISO Member States. The ISO standards were established through an international consensus of definitions and practices with the aim to improve communication and coordination on the basis of a single validated document.

The standard was developed by a working group of 60 experts from different sectors (industry, health & safety, quality) representing 30 countries. The ISO 31000 may therefore be considered as the global reference for a broad group of stakeholders.

An umbrella standard

An umbrella for more than 60 ISO Standards

The ISO 31000 acts as an "umbrella" for more than 60 standards in the area of risk management. The ISO 31000 standard provides a general framework in which to organize the risk management processes. The European Committee for Standardization (CEN) identified approximately 60 standards referring to the management of risks. These standards have been aligned with the ISO 31000 standard or are in the process of been aligned in future versions.

Some examples:
- ISO 9000: Quality management systems
- ISO 14000: Environmental management
- European Directive ATEX – work allocation in an explosive atmosphere
- ISO 22000: Food safety
- ISO 22301: Business continuity
- ISO 27000: Information security management system (ISO 27001)
- ISO 39001: Road traffic safety management system
- ...

▲ Umbrella: The ISO 31000 standard can be used by private and public organizations of any size, industry, or sector.
Optimit Security Risk Methodology (OSRM)

Optimit’s Security Risk Methodology was developed independently of the ISO 31000 standard but is largely based on the same principles, framework and processes. At the end of 2012 the OSRM was aligned with the ISO 31000 standard, mainly on the basis of terminology.

The OSRM consists of 12 structured security processes and 101 sub-processes, further hierarchically structured in more detailed security management activities. The methodology was developed with the aim of identifying, assessing and evaluating risks, the planning and implementation of risk management measures and auditing of these measures in view of continuous monitoring and review.

The 12 main processes are:
- Security risk assessment
- Strategy and planning
- The human factor
- Physical security
- Access control
- Intrusion detection
- Fire protection
- Camera surveillance
- Manned guarding
- ICT Security
- Alarm & Crisis management
- Security audit

Voluntarily application

The title of the ISO31000 standard (Risk management, principles and guidelines) clearly states that it is a guideline and not a legal obligation. The added value lies in the voluntarily application. The ISO31000 standard allows organizations to customize various components of the framework and the process to their specific needs.

The aim of the ISO31000 standard is not to prescribe a new risk management system. The purpose is rather to integrate risk management into the overall management system. Organizations are invited to critically evaluate and test their risk management process against the guidelines and principles of the ISO31000 standard.

Certification

The objective of the ISO 31000 is not to certify organizations. Only individuals are able to obtain ISO 31000 certification. Individuals can follow a training program and take a certification examination. The examination process complies with the requirements of the ISO/IEC 17024 standard that prescribes the certification process for individuals worldwide. The holder of an ISO31000 certificate proves that he/she has obtained the necessary knowledge and skills to apply the standard in order to protect value and ultimately to create added value.

Wider application

The ISO31000 standard can be applied to any public or private organization and group or individual. Public and private organizations in all sectors, including any format or activity and challenged with any kind of risk can use the ISO 31000 standard as a tool for decision making. The ISO 31000 standard has been translated into 23 languages.
Summary

The internationally accepted ISO 31000 standard offers an alternative view on risks and risk management. This article provides an analysis from a security perspective. The biggest challenge for security risk managers is to justify the value added by security. It is not an easy task for risk management to argue the return on security investment (ROSI), but it is certainly not a mission impossible. An event or incident with negative consequences as a result may ultimately have a positive impact. Could effective security management also create new value? Yes it can, because the seemingly contradiction in optimizing and securing critical value is a paradox. The ISO31000 standard supports this view through a different and broader view on risk and risk management, while acting as an umbrella over more than 60 risk management standards. Optimit’s Security Risk Methodology (OSRM) is aligned with the ISO31000 standard. The ISO31000 standard is applicable to public and private organizations, regardless of the size of the organization or the specific sector in which the organization is operating, and applies to all kind of risks. The application of the ISO31000 standard is not mandatory. The purpose of the standard is to certify individuals and not organizations. Individuals will be able to apply their knowledge and comprehension of the standard after receiving training, taking an examination and obtaining an ISO31000 certificate.