Risk Management and ISO 31000 in the Netherlands

Interview conducted for isotc262.org by
Dr. Frank Herdmann with

Andre Smulders,
Dutch delegate to TC 262

Ir. Andre (A.C.M.) Smulders CISSP is an expert in the field of cyber security with more than 14 years of experience in risk management in complex multi-stakeholder environments. Since 2005 he has worked at TNO as a Strategic Cyber Security Advisor for a variety of contractors in both public and private sectors. He is co-author of the publication "Networked Risk Management", has been the chair of different expert groups and is a speaker on national and international symposia.

isotc262.org: *Andre you were representing the Netherlands at the ISO/TC 262 meeting in October 2016 in Amman. Can you briefly introduce the Netherlands Standardization Institute (NEN), your national standardization organization, please?*

Andre: Royal NEN is the Dutch member body of ISO and CEN (the European Committee for Standardization). In total over 800 national standards committees are active, with in total over 5000 committee members. NEN is a professional non-profit business organization. NEN is an active contributor to ISO and CEN activities and manages a relatively large number of ISO working bodies. Besides standards development and standards sales activities, NEN also provides training and develops practical guides and web tools to promote and enhance the application of standards.

isotc262.org: *What is the impact of risk management and in particular ISO 31000 in the Netherlands?*

Andre: The interest in risk management in general is increasing because risk management is seen as an important management approach to react adequately to the changing business environment. These changes can evolve rapidly or even be disruptive. Also, governments apply risk management approaches more often to set priorities and provide a sound basis for legislation and regulations. More specifically risk management aligned with ISO 31000 gets more attention because of the risk-based approach in the new HLS-based ISO management systems standards such as ISO 9001 and ISO 14001.

isotc262.org: *Who are the key stakeholders of risk management in the Netherlands?*

Andre: A wide variety of organizations and businesses, including governmental agencies. As mentioned in the answer to the previous question, many organizations apply risk management for a wide variety of reasons. The specific application of ISO 31000 is less widely spread. It is mainly used as a general reference or framework or background information to assist the implementation of more specific risk management standards, e.g. in the field of environmental or OH&S management. ISO 31000 is sometimes seen as too generic to be of practical help. This is reflected in the membership of the Dutch mirror committee in which only a limited number of organizations are represented: consultancies, accountants and an organization that has a stake in information security.

isotc262.org: *What are the biggest obstacles for integrating risk management in all organizational activities for managers in the Netherlands?*

Andre: Risk management and risk based thinking is usually well integrated at top level management. However, integration into other organizational levels is not always achieved, for example when the risk management function is separated from the business functions whose risks they manage. This may cause a misalignment between objectives of the business and objectives of the risk management function. Consequently, this may lead to both inefficiencies and ineffectiveness in both the business as well as the risk management function. Aligning risk management with decision making within an organization helps to produce better decisions, supporting businesses to be more successful.

Another obstacle is that many organizations are part of supply chains or complex ecosystems. In approaches where security baselines, policies and other regulations exist that apply to all, conflicts may arise because organizations have different objectives and needs. Managing risks within a single organization differs from risk management across different organizations as one organization does not control the others. Additionally, in ecosystems there is a necessity for the capability to handle these different or even conflicting objectives. Well understood risk management can support organizations to develop this capability.

isotc262.org: *ISO 31000 quickly became one of the bestselling and most well recognized standards in ISO. What do you think about the future of the standard and how will it change to adapt to new challenges?*

Andre: By adding the relation with decision making, the ISO 31000 focusses on a better integration of Risk Management into the organization. I expect that the focus on a family of standards will provide additional guidance to organizations in managing risks in their ecosystems. This allows organizations to manage such risks, and better formulate their needs and/or requirements, and push risk management forward by increasing value to its users. It could also be an opportunity to provide a seamless alignment with HLS based management system standards.

isotc262.org: *What message do you want to give to the risk management community?*

Andre: Whereas organizations were once monolithic they are now part of complex ecosystems. Thinking about, and overcoming the obstacles mentioned before is a huge chance for the risk management community. It allows us to adopt an objectives oriented risk management approach that truly supports businesses as they change their objectives in our increasingly fast changing world.

isotc262.org: *What advice can you give to interested parties in the Netherlands who want to offer their input to the work of ISO/TC 262 and who should they address?*

Andre: You should get informed about the ways in which standards are created and managed – it is a world on its own. This helps to find the most effective ways to contribute. A first step would be to get in touch with NEN. At NEN Dick Hortensius is responsible for managing the Dutch mirror committee for ISO/TC 262. His contact details are:
e-mail: dickhortensius@nen.nl
phone: +31 15 2690 115

isotc262.org: **Thank you very much!**