Somewhat later than planned, the ISO 31,000 risk management standard update was released in February 2018. When addressing this, there are two findings, which stands out:

- The 2018 edition is better than the former 2009 edition
- It is an update – it is not a complete change of the approach to risk management. Hence if you are already in line with the ISO 31,000 standard, there may not be any need to change your overall approach

This leaves the ISO 31,000/2018 (ISO) well ahead of the updated COSO standard despite the almost quantum leap the 2017 update has been given since the 2004 edition.

ISO is based on a reduced set of nine core principles which is a strong and effective approach to standardising risk management. Recognising that all companies and organisations are unique in one way or another, one principle (# 3) states that risk management must be tailored to the individual organisation. As such, there is no "one size fits all", and hence any attempt to create a standard based on standardized processes and governance structures is ineffective.

These nine principles constitute the foundation of ISO risk management – and if/when an organisation builds its risk management approach, systems, processes and structures around these – they will be highly likely to have an effective and efficient risk management which truly add value and competitive advantage vis a vis lagging competitors. Importantly, one principle includes a push for continuous improvement.

The standard emphasizes that risk management must be an integral part of decision making. This was also stated in the 2009 edition but appears to have been largely ignored by risk managers and executives/boards across the globe. Common risk management practices are still reactive safety measures on already made decisions rather than an element of proactive decision support.

In the 2018 this "integrated in decision making" is stated repeatedly and is hence very hard to continuously ignore. To me, this is a fabulous lever for risk professionals, which they can use in their discussions with top management and boards as to how to develop and improve the handling of risks – be it positive or negative risks of the company.

I can only encourage risk professional who are not involved in decision making to vigorously use the updated ISO as leverage to get involved in strategic planning, sales & operation planning, resource allocation, budgeting – and other business processes, which make decisions under uncertainty … as all decision processes do.

This means that risk managers should look at any decision process, and address how that includes uncertainties (if at all) – and how can the risk profession add value to that approach. This will enable risks to be taken deliberately, intelligently and on an informed basis.

In any organisation there are multiple categories of risks taken, and here ISO in my perspective fall somewhat short in recognizing these. I agree, that by the end of the day, it all comes down to some element of decision making – but the systematic and often highly efficient approach many companies have to standard risks such as currency volatility, credit risk, employee safety, natural disasters, IT operational safety, manufacturing errors, etc. is not tangibly handled in ISO – which appears to focus on the risks taken by business decisions from strategy to day-to-day management.

However, this somewhat falls in line with the fact that the ISO 9000 standard, which over years is gradually moving into becoming a Total Quality Management (TQM) approach now explicitly requires risks and opportunity management being embedded in processes.

Hence – the two ISO standards may appear to "collaborate" where operations and standard risks are being embedded in the company TQM approach, and risk management is focused on decisions.

This may very well be a deliberate and good development – especially as multiple business analyses indicate that 80% of all major risks hampering companies are driven by (bad) decisions or poor strategizing. Despite this – too many companies and organisations – do not have explicit processes and tools to systematically identify and address the uncertainties and risks taken by decisions. Furthermore, it appears that the higher the level of management involved (and the higher potential impact), the less systematic is the risk management.

As stated – the update is an update. Yet, to many companies, the full application of this will lead to a significant improvement of the value risk management provides for the company.

Such an increase is highly needed for organisations if they are to persevere in the world ahead. Changes happens today more often and with bigger impact than ever before. Extrapolating this means that changes today happen less frequently and with less impact than ever in the future that lies ahead. To survive and prosper – organisations must mentally leave the concept of risk management as they know it and implement a culture and approach of intelligent risk taking. Such an approach is fully in line with the updated ISO 31,000/2018 standard.

Hans Læssøe
AKTUS
hl@aktus.dk
www.aktus.dk