Editorial

IT & Risk Management

Ronald Koorn
editor-in-chief

As Ulrich Beck wrote 25 years ago, we're living in a risk society. Although the slogan 'no guts, no glory' holds true for start-ups and other innovative initiatives, overall our economy is permeated with a risk-averse culture.

In practice, (IT) Risk Management usually suffers from several shortcomings, such as:

- No link between risks to (strategic/tactical) objectives and goals: the focus remains predominantly on operational risks, without a direct relationship to the achievement of goals;
- Static approach: emerging risks and major uncomfortable threats ('the elephant in the room') are often left out of risk assessments;
- Mono-disciplinary perspective: the inter-relationships between risks and the psychological aspects of Risk Management and mitigation are often ignored;
- Qualitative evaluation: as statistical figures on likelihood and impact are becoming available, a quantitative approach to Risk Management can be a valuable addition to weighing and prioritizing risks better;
- Absence of Key Risk Indicators (KRIs): KPIs are everywhere, but KRIs are rarely used for monitoring risks and/or for performance management purposes;
- Lack of effective tooling: the old-fashioned top 10 lists, two-dimensional risk maps and extensive spreadsheets are still 'king';
- No overall framework: all areas within Governance, Risk, Security, Compliance and Auditing (GRSCA) inside and outside of IT are using different frameworks and tooling;
- Two-dimensional risk mapping: traditional risk assessments measure the likelihood and impact (2 dimensions), but omit to take risk connectivity and risk velocity in consideration (4 dimensions). As a consequence, missing are structural breaks ('tipping points') and the pace with which a risk can adversely impact your organization;
- Technocratic exercise: ultimately risks are driven by behaviour, most risk management processes can benefit from incorporation of the human factor and risk culture;
- Etc. (I presume that you as the reader can think of other methodical issues with Risk Management).

In summary, there are sufficient Risk Management areas to improve upon and to read about in this issue of *Compact*.

This *Compact* edition focuses on IT & Risk Management, which can be read two-fold:

1. **Risk Management for IT:** no IT projects or operations without risks, therefore we have included articles on data migration, IT assurance and privacy (because of the upcoming deadline of May 2018 for compliance with the General Data Protection Regulation – no one could have missed that);
2. **IT for Risk Management:** how can IT support the Risk Management function and processes? The articles on GRC Tooling, SAP S/4HANA, Horizontal Monitoring and dashboards in this *Compact* will elaborate on IT solutions for addressing Risk Management challenges. The latter two articles are primarily aimed at the healthcare sector, but will be applicable to other sectors as well.

As we issued a special *Compact* edition on Cyber Security last year (2016/3), we have excluded cyber security subjects.

Besides articles on Blockchain and autonomous vehicles, in the next *Compact* issue (2017/4) you will find additional articles on Risk Management. The next issue will contain articles on Dynamic Risk Assessments, SAP Process Controls, Smart Controls and Third Party Risk Management.