Operational risks in IT – time for the Board and management to wake up?

Two leading Nordic banks recently wrote-off £50m and £70m respectively having cancelled major IT programs due to internal resource constraints and insufficient capacity to manage and steer such ventures. A global Pharma suffered huge production problems following the introduction of an ERP system that had not been properly tested with losses amounting to £70m in six months. A leading university hospital postponed all surgical procedures due to IT disruptions. The list of operational risk related failure reported in media is longer.

There is little doubt that there is a need in many companies and government bodies to develop an insight and ability to identify and manage operational risks. This article describes how boards and senior managers in a relatively simple way can overcome and take control over existing shortcomings in the area of operational risk.

The failures mentioned above could have been avoided completely, or been limited, with a better model controlling and steering IT on a management level. In my opinion IT is often sub-optimally managed on C-level, causing both unnecessary and high operational risks – risks that Board directors and Executives are not aware of, hence causing this prisoner's dilemma.

IT governance and current shortcomings

Organizations that have introduced a Balanced Scorecard (introduced 20 years ago by Kaplan & Norton) often recognize the advantage of not measuring IT from a cost perspective alone. Which otherwise may be the case when the CIO reports to the CFO and is not a permanent member of the executive team.

CEOs that set specific goals for IT, based on indicators such as quality, availability in daily operations, delivery status on strategic projects and people dimension, are in my opinion, in a better position to manage IT. However, when C-level focus is on IT costs only, other problems tend to arise.

Managements and boards recognize that IT has a value and is of a strategic nature, but also perceive IT as difficult to understand and complex. If the CIO is not personally represented on the management board, and someone else represents IT, it is natural that the main focus will be around on cost rather than business value and risk optimization. The paradox is that the CFO 's will be responsible for the IT function is often also responsible for the company 's risk management.

Board members I speak with express frustration about IT are annoyed not to have control over IT. I have often heard comments such as: ''shouldn't we always do a proper risk analysis before deciding on major system changes? '', ''Why is it we can manage huge construction projects as planned but never succeed with an IT project?'' and ''what precise questions should I as Board director ask our CIO in order to properly understand the IT risks we actually sit with?''

Operational risk is defined as the risk of monetary losses as a result of faults and errors in process, technology or skills or due to external factors (after Basel II definition). Operational risk may also include other risks such as fraud, legal risks, physical risks, and environmental risk

When to consider making an operational risk analysis?
Boards with operational risk as a regular agenda item, organisations where operational risk management are a clearly defined management responsibility and companies where risks and risk index is part of the management reporting are likely to be far ahead compared to others.

In some situations one should always seriously consider a risk assessment:

- Before making any decision about major development projects, ERP projects, transformations, outsourcing or other strategic ventures
- As part of M&A due diligence processes
- As newly appointed Chairman, CEO, CFO or CIO
- Should the board feel unsure about the control of operational risks

Practical approach to operational risk control
There are ways to quickly improve risk mitigation and thus increase quality, which in turn can lead to cost reductions and improved control of both IT and operational risk. In an ideal situation, management, CIO and IT function work together to identify and reduce operational risks over time.

There are a number of ways to practically apply operational risk management. Formal models and frameworks such as COSO, ICFR and Basel directives, which are mandatory or more appropriate in some situations including large public companies and organizations in the financial sector.

SME:s and public sector will, in my opinion, benefit from a basic and more pragmatic methodology, which includes

- Identification of risks and risk areas
- Analysis, compilation and assessment of current risks
- Assessment of risk levels - if possible including financial implications
- Decisions about actions (activity plans and budgets)
- Decisions and introduction of performance management model and reporting
- On-going riskmitigering as part of daily operations

By analysing and identifying the organization's operational risks in areas such as in- and outgoing payments, information and IT security, suppliers, project management, IT processes, IT skills, environmental impact/CSR and attrition can relatively quickly lead to sufficient understanding of current risk situation and what need to be done.

After the analysis, the organization should mitigate risks on tactical level by reducing the most pressing and prioritized risks and make a plan for future risk reduction. In certain specific areas, such as IT security or process development, it may be wise to consult an independent specialist.

Finally, the organization should introduce a governance model and some basic and specific tools like a dashboard for risk mitigation and monitoring (see illustration). One should also, especially if there are several major risks, consider establishing a risk committee where CIO together with other executives, organizes and directs the work to manage and reduce the operational risks over time. The risk committee should ideally report to the Management team or even the Board once or twice per year.

Benefits from improved risk control

The upside is that Board and management can take control by following specific ratios (risk index) and set measurable goals for how much the CIO and other executives should reduce operational risks in the coming period. By shifting focus from IT costs alone management place itself in a position to steer IT towards a more effective delivery with reduced operational risks, higher quality and lower costs as a result.

Appendix – Example of risk mitigation dash-board

Styrkort för riskmonitorering

Sammanfattning av risk analysen visar att organisationen med specifika insatser kraftigt kan reducera de underliggande operationella riskerna

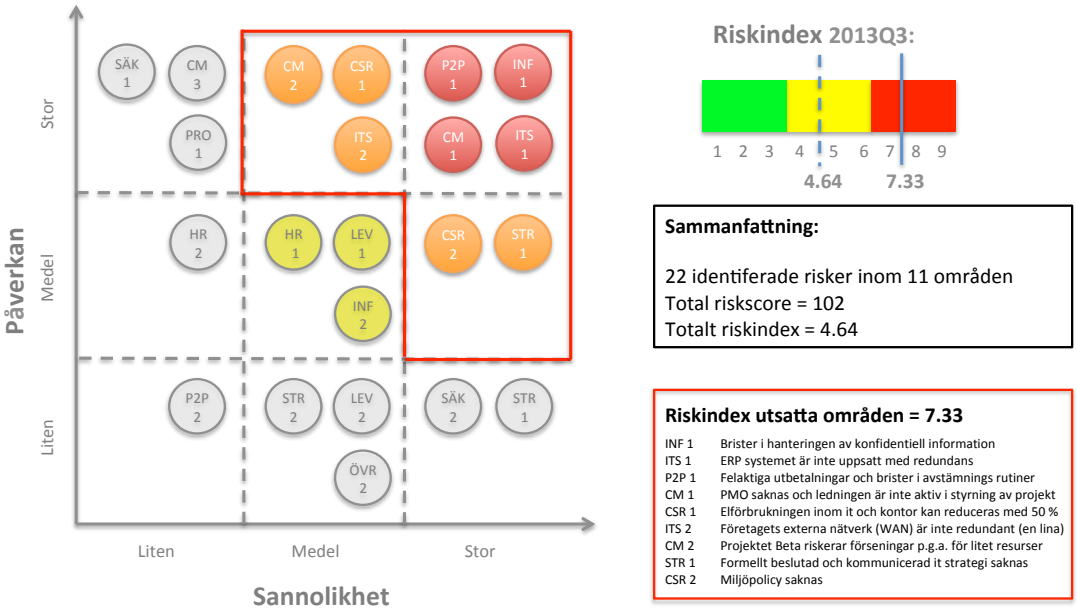

Illustration: Examples of risk mitigation dashboard

About the author: Björn Ovar Johansson works as interim cio and is the founder of Senior IT Executive in Sweden and the UK