**Operational risks in IT – it is time for the Board and senior management to wake up?**

A university hospital postponed all surgical procedures due to IT disruptions in 2012, twelve months later another leading hospital cancelled their operations following a regional power failure where the hospitals battery back-up systems failed to kick in. It was concluded that proper testing was never conducted. Fortunately, no patients were injured in either hospital.

In 2012 a global pharmaceutical company suffered huge production problems following the introduction of a new ERP system that had not been properly tested with bottom-line losses amounting to £70m in the first six months after go-live.

Not all operational risk scenarios are this extreme – on a weekly or even daily basis we can read about IT glitches in most business sectors where disruptions cause unnecessary losses and, to make matters even worse apart from the media coverage, the consumer experience is rapidly spread and shared in social media damaging the brands reputation. Examples of some recent headlines;

- ''Supermarket giant insists that its systems have returned to normal after a technical issue just days before Christmas forces the cancellation of 400 online orders''
- ''Air traffic control technical 'glitches' fixed after a day of delays for plane passengers''
- ''The Government's IT failures know no bounds''
- ''Managers at RBS have red faces after second IT crash in less than a year annoys millions of customers''
- ''Google apologizes for 11 hours of Gmail issues affecting 29% of emails, blames dual network failure''

The list of materialised operational risks reported by media may seem endless. However, this is most likely only the top of an iceberg of inherent operational risk that will cause problems for customers and taxpayers on one hand and financial and other losses for private and public organisations on the other – at least unless management start to react proactively.

My point is that there is an urgent need for many organisations (private and public) to develop an insight, understanding and an ability to identify and manage operational risks. This article intend to describe how Boards of Directors and Executive management in a relatively simple way can overcome some of these issues and relatively quickly take control over existing shortcomings in the area of operational risk, hence avoiding negative press.

The failures described above could have been avoided completely, or at least been significantly reduced with a better model for controlling and steering IT on management level. In my opinion, IT is too 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.

A recent study published in Harvard Business Review 2011[1] shows surprisingly high numbers of out-of-control IT projects, so called Black Swans, which by definition can sink entire companies. Having examined over 1000 IT projects the research found that the average

[1] *Why Your IT Project May Be Riskier Than You Think by Flyvbjerg and Budzier*
*Published in: Harvard Business Review, Vol. 89 (2011), No. 9, pp. 23-25.*

overrun was 27%. However, an alarmingly 15 % of the projects studied was a Black Swan with an average cost overrun of 200 % and a schedule overrun of almost 70%.

**IT governance and current shortcomings**

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

Organisations 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 the C-level focus is on IT costs alone, other problems tend to follow.

Managements and Boards of Directors recognize that IT has a value and that IT is of a strategic nature, but they also perceive IT as difficult to understand and something complex. If the CIO is not personally represented on the management team, and someone else speaks and acts on the behalf of IT, it is natural that the main focus will be on cost rather than business value and risk optimization. The paradox here is that the CFO (if also being responsible for the IT function) often is accountable for the organisations overall risk management.

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

**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 Board of Directors or Executive Management makes any decision about major development projects, ERP projects, transformations, outsourcing or other strategic ventures – here an independent risk review should be performed
- As part of M&A due diligence processes
- As newly appointed and externally recruited Chairman, CEO, CFO or CIO
- Should the Board of Directors have serious doubt about the organisations ability to control its operational risks

**A 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 risk mitigation 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.

**Dashboard for Monitoring Operational Risk Index**

The analysis indicates that the organisation can significantly reduce inherent operational risks by taking proposed actions.

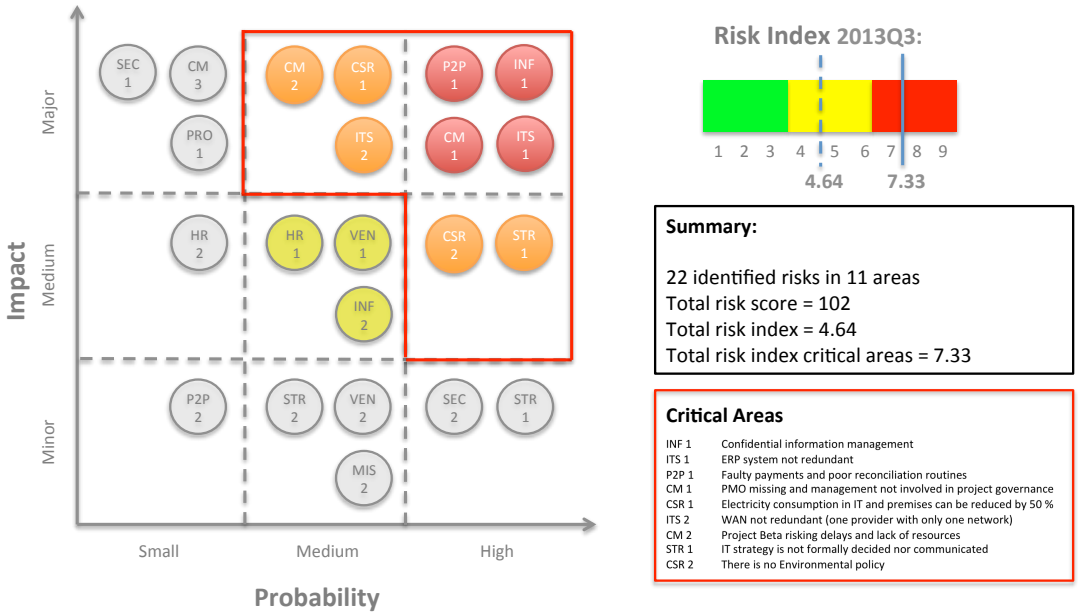


Illustration: Example of risk mitigation dashboard



*About the author:*
*Bjorn Ovar Johansson works as interim CIO and Senior Advisor with operational risk mitigation as specialism. He is the founder of Senior IT Executive in the UK and is a former CIO in Banking, Financial Services and Life Science sectors.*