BWise
BUSINESS IN CONTROL
A NASDAQ OMX COMPANY

Four Steps to incorporate risk management into your organization:
Getting risk handling right

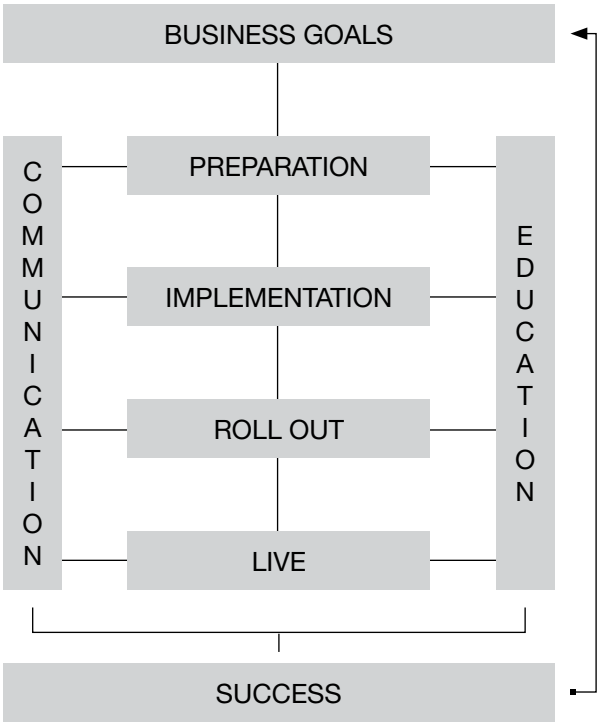

Figure 1.
Overall project methodology

Based on clear and realistic goals, best practices show a successful four phased approach, consistently supported by good communication and education (Figure 1). This article does not include the aspects of communication, education and handling change, although change management is a major critical success factor.

The four phased approach:

1. Preparation;
2. Implementation;
3. Roll out;
4. Live.

This document explains these four phases and how they assist in achieving risk management step by step at your company.. If related to the goals of a certain phase, specific critical issues are indicated.

BWise
BUSINESS IN CONTROL
A NASDAQ OMX COMPANY

Step 1
Preparation

This is the most important phase; it concerns all the milestones and targeted goals. The selection of a methodology and content, critical involvement of key employees and commitment to this plan by top management must all be realized for success.

Critical success factors

- Clear and realistic deliverables of this phase related to the overall project goals and scope
- A well-defined scope of risk management
- Appropriate risk management methodology and expertise (internal or externally hired)
- Current level of risk management knowledge and expertise in the company
- Decentralized flexibility in risk handling ('the deeper, the more details') and also secure corporate group risks (emphasize taxonomy, reporting schedules). Create acceptance by introducing risk management as a business supporting tool including centralized aggregated risk reporting
- Selection of key employees from staff and businesses and securing enough capacity for them to be sufficiently involved
- Good project and program management

Risk methodology workshops

The business goals must be set by the board of directors as a starting point. These goals should be the basis for risk workshops with key employees. Risk workshops will identify and classify the company's key risks and measures. There are different ways to identify risks.

1. Risk workshops based on a pre-conceived common risk framework
2. Free-format risk workshops based on the risk understanding of the business

The advantage of the free-format approach is it creates internal knowledge and awareness on risks. The lack of guidance by a pre-conceived framework may lead to poor quality and very different results across the organization. Proper training of facilitators will address those advantages and disadvantages. A side effect of introducing risk management is that it creates awareness for the urgency of risk management and continuously self improving initiatives for the entire company.

New to Risk Management?

If risk management is new to your organization the best way to proceed may be to hire and involve an outside consulting firm and define a pragmatic, high level, risk methodology tailored to your organization. Simply hiring a new risk manager for risk management duties has often proven to be unsuccessful. This new manager may not know the specifics of the company or its politics and has not received 'earned support' yet. Vital to the success of a new risk management initiative is not only the involvement of top management from the beginning, but also participation of a select group of key employees. They should be representatives from the departments in scope and your potential champions.

Process driven workshops to identify key risks

From prior experience BWise has found that for both approaches a process driven view delivers the best results and the following must be addressed with key employees

- Clear understanding of the defined business goals
- Shared understanding of the risk management methodology
- A common language to express and document anything risk-related
- Based upon the defined goals, outline the core processes which contribute to achieving these goals
  - Related to the goals, define the internal or external events which can occur and have an impact on these goals
  - If an event has a positive impact, it will be treated as an opportunity and will be managed by the business to take advantage of its potential (these positive events may be improving report information, delivering more specs or simplifying procedures)
  - If an event has a negative effect on achieving a goal, it must be treated as a risk
- Per process the identified risks' impact and likelihood must be considered and agreed upon by the group. Each risk can now be plotted in a risk map. Based on the risk appetite for the company as a whole or per division each risk in the red is a risk which could seriously harm the achievement of business goals
  - All risks over the risk appetite line should be addressed by the business. For example, adding the responsibility of these risks to certain employees, changing policies and procedures or adding risk information to standard management reports
- The next step involves attempting to find the risk response for high impact risks. Four different risk responses are possible
  - Terminate (Avoid) - eliminate this related business activity, because you cannot do anything to minimize the risk
  - Transfer (Share) - possibility of insuring or 'outsourcing' the risk
  - Take (Accept) - you cannot do anything to mitigate this risk, you just accept it as it comes
  - Treat (Reduce) - define controls that can mitigate or neutralize the effect of these high impact risks if they occur

Governance structure

In addition, management must define a governance structure to embed risk handling; including policies and procedures, escalations, reporting lines and risk handling responsibilities and authorizations. Larger and multinational businesses should give extra attention to aggregate risks from decentralized entities up to the corporate level (risk roll-up).

Enterprise GRC (ERM) platforms

Organizations should support professional risk handling by selecting and implementing a risk management platform solution. The following is needed for a successful selection:

- A proper set of requirements, including and foremost in the area of reporting
- An outline of the related workflows of executing risk management
- An understanding of authorizations within the defined governance structure
- Technical or IT constraints/requirements

When actually purchasing a solution, the business should request a proof of concept or a demonstration with real company data. Check the references of the solution vendor, and perform an on-site visit of the vendor. The business should also make an estimate of how many users and supporting employees will ultimately use the solution.

BWise
BUSINESS IN CONTROL
A NASDAQ OMX COMPANY

Step 2
Implementation

The acceptance of risk management has already begun by involving key employees from the departments at the earliest moment in this project. Best practices show that you should continue to involve key employees in the project.

Implementation plan

The actual implementation of a risk management technology solution typically has the following set up:

- Scoping and Project Plan - fine tuning project requirements, defining the project organization, planning, available capacities and deliverables per project phase
- Actual start of the implementation
- Risk methodology workshop results are translated into configuration possibilities. Initial workshops should be used to train key employees with the possibilities and use of the supporting risk solution. Using a software solution will actually help drive standardization and uniformity across the organization
- Report requirements are finalized and approved, roles are defined and corresponding work and authorizations are clear
- Extra attention should be given to the definition of risk frameworks (i.e. risk universe or risk taxonomy), the business objectives, the processes, risks and controls
- Measures and controls must be defined. Do not underestimate the difficulty of defining controls. Define inherent risks and residual risks, this sets the foundation for the business's risk and control matrix
- After configuring and testing of the solution, relevant data can be loaded

Step 3
Roll Out

The roll out phase is the final step before a business goes live with the solution. Best practices have revealed a few key points to consider.

1. Secure application and technical support before you start the actual roll out. Be aware of potential IT infrastructure issues. The business is linking this new system to its existing IT network.
2. Train staff appropriately. Use real business cases during introductions. Use custom made e-learning support and userfriendly documentation.

3. Adjust or expand the risk framework for more local detailed requirements including more local risks and controls, but make sure the basic framework and centrally defined corporate risks are not altered.

4. Do not go live with a “big bang” approach. Embrace a slowly expanding approach. Think big, start small, and then scale up. This leaves room for learning, quick wins and fine tuning of the framework, and does not create large exposure from the start.

5. After further roll outs are implemented and checked, then enterprise risk management is on its way. Vital deliverables of the project are now being produced, including reporting at all levels to monitor progress, control testing, issue tracking and auditable evidence.

Step 4
Live

At this time, monitoring reports and aggregate risk reports are being produced. These results will begin to support local and corporate management in getting a grip on all relevant risks, including the risk of non-compliance of the entire company.

At the start of the roll out, a "change board" should be created made up of key employees. The change board should secure the standards and taxonomy of the framework, manage all change requests and treat requests as potential improvements.

Each request must be judged if it is applicable to single or multiple entities, departments or individuals. When the last group has begun using the solution, corporate wide risk management has really commenced.

BWise
BUSINESS IN CONTROL
A NASDAQ OMX COMPANY

Change Management

Due to the high-level approach we have taken with this document, change management is not addressed here. Change management is important, especially in a decentralized company.

An overview of 12 critical success factors for such a project is shown in figure 2.

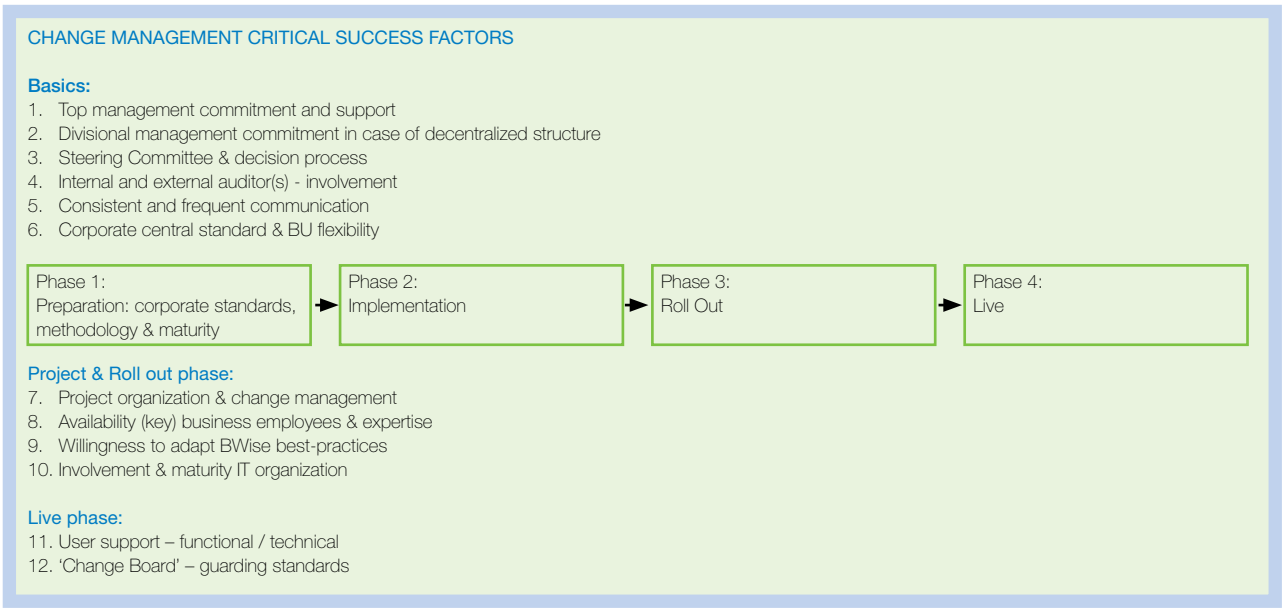

Figure 2.
Overview of Critical Success Factors

About BWise

BWise, a NASDAQ OMX company, is the global leader in Enterprise Governance, Risk Management and Compliance (GRC) software. Based on a strong heritage in business process management, BWise delivers a truly integrated and proven GRC platform.

With this platform, BWise supports an organization's ability to track, measure, and manage key organizational risks in one integrated system. By doing so, BWise helps customers to truly be in control by sustainably balancing their performance and financial and reputational risks. BWise enables customers to increase corporate accountability; strengthen financial, strategic and operational efficiencies, maximize performance, and better understand risks. Using BWise, organizations are able to comply with regulations such as Sarbanes-Oxley, ISAE3402/SAS-70, PCI, Solvency II, Basel II and III, Dodd-Frank, ISO-standards, European Corporate Governance Codes and many more.

BWise provides for the GRC needs of hundreds of customers worldwide, across all industries. Customers include adidas, AEGON, Ahold, AngloGold Ashanti, Connexxion, Health Alliance Plan (HAP) of Michigan, LeapFrog, Liebherr, Marathon Oil, Southern Company, Swiss Life, and Transcontinental. BWise has offices in the Netherlands, United States, Germany, France and the United Kingdom. For more information, visit www.bwise.com.

BWise® GRC Platform

BWise offers multiple role-based software solutions for Risk Management, Internal Control, Internal Audit, Compliance & Policy Management, IT GRC and Sustainability Performance Management. Each solution derived from the BWise integrated Governance, Risk management, and Compliance Platform supports the end-to-end process of a given role.

Gerard Parker Chief Risk Officer (Risk Management)		BWise® Risk Management Professional	BWise® Risk Management Advanced
Michael Bauer Corporate Group Controller (Internal Control over Financial Reporting)		BWise® Internal Control Professional	BWise® Internal Control Advanced
Ann Green Internal Auditor Internal Audit (IA)		BWise® Internal Audit Professional	BWise® Internal Audit Advanced
Jackie McLaren Compliance Officer (Compliance & Policy Management)		BWise® Compliance & Policy Management Advanced	BWise® Compliance & Policy Management Advanced
Damian Thomson Chief Information Security Officer (IT GRC)		BWise® IT GRC Professional	BWise® IT GRC Advanced
Kim Lee VP Corporate Sustainability (Sustainability Performance Management)		BWise® Sustainability Performance Management Professional	BWise® Sustainability Performance Management Advanced

BWise
BUSINESS IN CONTROL
A NASDAQ OMX COMPANY

Contact Information

BWise Headquarters
Rietbeemdenborch 14-18
5241 LG Rosmalen
P.O. Box 321
5201 AH Den Bosch
The Netherlands
Tel: +31 (0)73 - 6464911
Fax: +31 (0)73 - 6464910

BWise, Inc.
1450 Broadway, 38th Floor
New York, NY 10018
USA
Tel: +1 212-584-2260
Fax: +1 212-730-6918

BWise Germany GmbH
Kaiserswerther Strasse 115
40880 Ratingen
Germany
Tel: +49 (0)2102 420 663
Fax: +49 (0)2102 420 62

BWise
19, boulevard Malesherbes
75008 Paris
France
Tel: +33 (0) 1 55 27 37 28
Fax: +33 (0) 1 55 27 37 00

BWise
1 Bell Street
Maidenhead
Berkshire, SL6 1BU
United Kingdom
Tel: +44 (0)1628 421750
Fax: +44 (0)1628 421501

Disclaimer