Goal Oriented Enterprise Risk Management

Applies to:
Governance, Risk and Compliance, Best practice and benchmarking, Organizational change management. For more information, visit the Governance, Risk, and Compliance homepage.

Summary
Managing risks at wrong places is the inherent risk of/in any risk management function. Unfortunately, in reality this risk often occurs!

While risk management is often considered to be largely applicable to financial sector, I strongly believe, it is equally important (and proves beneficial too) to other industries as well. As most of my experience has been with IT, in this article, I've laid out the flaws, frequently overlooked key attributes of an effective risk management and a practical approach to overcome them.

Could be risky not to go through this article!

Author: Vinay HK
Company: SAP AG
Created on: 20 August 2008

Author Bio
Vinay is a Risk Manager in the global GRC risk management team responsible for the board area of Global Service and Support.

In his earlier roles, he has been a Quality lead, Lead auditor for ISO systems, Test lead and a Developer. His interests include topics in the area of Compliance, Risk management, Security, Business continuity, Operations and Process reengineering.

Vinay swims, hikes, reads and drinks beer in his free time.
# Table of Contents

Motivation............................................................................................................................................................ 3  
Typical Flaws | As-is in Risk Management: ........................................................................................................ 3  
The Goal Oriented Enterprise Risk Management: ............................................................................................. 4  
Epilogue.............................................................................................................................................................. 7  
Related Content.................................................................................................................................................. 8  
Copyright............................................................................................................................................................. 9
Motivation

Managing risks at wrong places is the inherent risk of/in any risk management function. Unfortunately, in reality this risk often occurs!

While risk management is often considered to be largely applicable to financial sector, I strongly believe, it is equally important (and proves beneficial too) to other industries as well. As most of my experience has been with IT, in this article, I’ve laid out the flaws, frequently overlooked key attributes of an effective risk management and a practical approach to overcome them.

Typical Flaws | As-is in Risk Management:

The current risk management practice overlooks many critical details. Most important of them being:

1. Too much focus on the operational risks - a case of not stitching in time and fighting with 9!
2. Lack of continuity of risks - the risks of material impact are often not continued to the operational level
3. Lack of monitoring - the risk information not being up-to-date
4. Lack of involvement of key, authoritative and accountable people
5. Reporting happens largely on operational level and does not get appropriately aggregated to the enterprise level
6. Incorrect articulation in reporting to Management
7. Misuse of tools available for risk management. A myth that using a tool for managing risks will enable Orgs to take better decisions
The Goal Oriented Enterprise Risk Management:

Goals are the single most important attribute for any Enterprise and naturally, the senior management. Needless to say that the risk management has to be goal oriented too. Below are the basics of such a model.

1. Goals:

“If you want to live a happy life, tie it to a goal, not to people or things” No prizes for guessing the genius from whom this came from (Albert Einstein).

Call it Goals/KPIs, but they have to be the cornerstone of every risk assessment. Every risk that is identified has to be necessarily mapped against a goal (to a goal at the enterprise level or at an LoB level which would have cascaded from the top).

2. Network:

Build a strong community of key people in various LoBs who have an insight into their Business and get the buy-in. One is likely to stumble if this community turns away. The Enterprise will have to break the barriers and have to come together and collaborate.

Involvement of the stakeholders down the value chain is necessary for the assessments done at a higher level. For example, it is always recommended to have the people from testing/release management in a risk assessment done during start of development to avoid problems later on.
3. **Follow a process:**

Play safe! Not following a defined process approach is a risk by itself. Make sure you mitigate it. It could be that you use one of “n” models/frameworks available for reference or build your own tailored approach.

Set individual steps in the process and establish tangible deliverables at each process step. Without deciding on the deliverables, it is highly likely that you trigger a cumulative negative value addition as you progress.

4. **Org structure:**

Risk management function is best placed with the Chief Operating Officer or a central team which is very close to the COO’s office. This ensures that the function has the access to almost all the information that matters to an enterprise and opens a wide opportunity to cascade responses/mitigation plans down the organization. The function should in turn have representatives in various LoBs.

5. **Strategic risk management:**

Once the Organization is up and running on its goals, the next natural process step would be to devise strategies to realize the goals. Risk assessments should happen on these strategic decisions and carried forward to operational risk management.

It is imperative that all the key stakeholders from all related (even at the end of the value chain) LoBs are involved at this phase.

6. **Continuity:**

The identified risks and its corresponding responses should be carried all along the value chain. No matter it gets delegated/transferred/accepted/mitigated. In the above context, the results of the strategic risk assessments shall have their tentacles spreading into operational risk management and should not be overlooked.

Tool based risk management will help to link the risks wherever the activity (which realizes the strategy and eventually the goal) goes.

7. **Operational risk management (ORM):**

Here we come to the rock bottom of the process chain. It will be these granular processes/projects that will be finally responsible for acting on the responses for the risks and have to be carefully monitored. For example, this could be as simple as a risk assessment done during testing of a new Service pack planned for release.

ORM is best integrated with the QM function of the particular LoBs. The QM function should ideally interact with the centralized risk management function to carry forward all the relevant risks to their LoB and act accordingly.
8. **Validate risks:**
Always have the risks and responses validated by an accountable manager. This should apply for all risks/responses that get cascaded at different levels in Organization. The risk validator should have a broad view of the enterprise goals and the way it relates to her/his LoB in the Organization. Typically, these key people could be heads of various LoBs.

9. **Continuous monitoring:**
Having the risks updated at equal intervals of time will not only bring visibility on to the table but also open up efforts for further efficient and effective execution. The updates will not only keep the information current but also invites the 4 eye principle (validation) of having someone else also see and verify whether right actions are been taken at right times.

10. **Reporting:**
   a. **Frequency of reporting:**
      Is best done every quarter and if a tool is implemented, should be exploited to the fullest extent to ensure least manual effort
   b. **Consolidation**
      Consolidate risk reporting with many other reports that get circulated within each LoBs. Avoid reinventing the wheel, instead, collaborate and consolidate
   c. **Aggregation at different levels:**
      The risks will always have to be reported bottom up. Each risk aggregated bottom up shall present information of enormous value at the top. Aggregation in turn should be done on 3 levels:
      1. Goals
      2. Compliance
      3. Estimated risk exposure

If the reporting doesn’t fall into one of the above categories, it is unlikely that the report will fetch senior management’s attention.

Typical statements in a risk report could be:
1. Goal of “x” of opportunities in FY 2008 is unlikely to be met. The expected # of opportunities is 35% less than the goal
2. Customer satisfaction index is likely to be 20 percentage points below the target
3. An expected loss of “xx” million Euros on failing to abide contractual requirements
4. Risk of non compliance to ISO/Sox certification in Q4 2008
Epilogue

Efficacious risk management, like all other functions, demands a definite commitment from all the stakeholders involved. It is necessary for every risk management function to scope the areas which has to go through this process to avoid over-engineering and costly risk assessments. After all, one should not turn every stone around!
Related Content

Worth visiting:


Article - GRC Risk Management: https://www.sdn.sap.com/irj/sdn/go/portal/prtroot/docs/library/uuid/0043a8ab-bdae-2910-d8bc-cf4abd4d6bed

For more information, visit the Governance, Risk, and Compliance homepage.
Copyright

© 2008 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, System i, System i5, System p, System p5, System x, System z, System z9, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, Informix, i5/OS, POWER, POWER5, POWER5+, OpenPower and PowerPC are trademarks or registered trademarks of IBM Corporation.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

These materials are provided “as is” without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall not be liable for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials.

SAP does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third party web pages nor provide any warranty whatsoever relating to third party web pages.

Any software coding and/or code lines/strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.