RC25007 (W1006-024) June 7, 2010
Other

IBM Research Report

A Knowledge-based Decision Support Tool for Enterprise Risk Management

Nitin Nayak, Rama Akkiraju
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598 USA

Nagesh Mantripragada
IBM Global Business Solutions Center
Bangalore, India

Robert Torok
IBM Global Services
Toronto, Canada

Research Division
Almaden - Austin - Beijing - Cambridge - Haifa - India - T. J. Watson - Tokyo - Zurich

A Knowledge-based Decision Support Tool for Enterprise Risk Management

Nitin Nayak[1]*, Rama Akkiraju[1], Nagesh Mantripragada[2], Robert Torok[3]

[1]IBM Watson Research Center,
Hawthorne, NY 10532,

[2]IBM Global Business Solutions Center,
Bangalore, India

[3]IBM Global Services,
Toronto, Canada

ABSTRACT

Enterprise risk management (ERM) refers to a set of processes and methods used by organizations to manage their business risks. In this paper we present a knowledge-based, ERM decision-support tool to help identify, assess, prioritize, analyze and to design solutions to mitigate risks faced by organizations. This design tool is expected to be used both by business consultants as well as client organizations. Several ERM methodologies and tools have been presented in the past. Three key features differentiate our work from the prior-art. First, our knowledge-based ERM tool contains a rich repository of risk content organized for efficient search, and retrieval. This speeds up the risk, and root cause identification and helps conduct the risk assessment and analysis in a structured and consistent manner. Second, the classic and traditional qualitative and quantitative risk analytics are enriched with novel visualizations to help users query and view risk content. This provides useful insight in the context of the larger business environment. Finally, the tool supports the risk management life-cycle by integrating design-time activities with day-to-day risk monitoring and management. This encourages risk management at enterprise level rather than in silos and enables proactive management of risks. Feedback from beta test of this tool with ERM consultants at a large IT consulting company has been very positive and the tool is currently in use at the same company.

INTRODUCTION

Some common fallacies from past-era risk management strategies are that (a) risk management is only about financial risks (b) individual business units or organizations can independently manage their risks and (c) risk management is about managing risks to individual projects. Research and real-word risk events have proved these fallacies wrong. A recent CFO survey [1] conducted by a large IT consulting services company indicates that 87% of the risks to companies have non-financial sources. As for silo-based risk management, it is not only sub-optimal but can be dangerous to the enterprise as evidenced by the real-world incident at a world class automotive company, where uncoordinated risk mitigation strategies between the finance department and the research labs for reducing the cost of palladium metal usage within the automobile led to a billion-dollar loss in 2002 [2]. Additionally, while managing risks to individual projects is important, many risks span beyond individual projects and impact the enterprise as a whole. Some examples of enterprise-level risks include: fraud and bribery risks, talent management risks, socio-political and economic risks, natural hazards, etc. Considering all these factors enterprise risk management is receiving considerable management attention these days.

So what is Enterprise Risk Management? Enterprise Risk Management (ERM) refers to the processes and methods used by organizations to manage expected and unexpected events that may impact the achievement of their business objectives. ERM is broader than managing risks to one functional area or dealing with compliance issues alone. ERM seeks to overcome the silo-based approach associated with traditional risk management where different categories of risks are managed independently. We believe that ERM's approach should be:

- Integrated: ERM perspective spans all lines of business and is governed at enterprise level.
- Comprehensive: ERM's scope spans all types of business risks and across all business units, functions, processes, and systems.

[*] Corresponding author: Tel.: (914) 945-2902; E-mail: nnayak@us.ibm.com

- Proactive: ERM's approach is proactive where risks are identified, assessed, prioritized and risk responses designed and implemented to mitigate them.
- Strategic: In most organizations, ERM is part of strategic planning and focuses on risk events that impair the enterprise from fully achieving its objectives as well as the opportunities that may present themselves. ERM provides transparent, *risk-adjusted business performance management* integrated into the business.

How does one get started with ERM? Many companies wrestle with how to get started with enterprise risk management. Some companies own risk management tools but have not used them because they do not where to begin. Several ERM methodologies and tools have been proposed in the past [3] [4] to help companies get started. Most ERM methodologies in practice are very similar to each other and start with understanding the organization's business objectives and then provide approaches for identifying, assessing, prioritizing risks and conducting detailed analysis of prioritized risks to design a set of risk response actions followed by implementation of risk monitoring solutions. Several vendor tools are also available for risk monitoring and management [5] [6].

Our ERM methodology and tool builds on these existing methodologies. In particular, our tool integrates multiple risk-related perspectives such as business objective, business process, organizational hierarchy and functional areas so companies can get a holistic view of their ERM environment and make informed decisions about how to mitigate the risks with the eventual goal of increasing shareholder value. In addition, we introduce a novel knowledge-based approach to enterprise risk management. Our knowledge-based approach is designed to both improve the business consultant's productivity as well as the quality of the deliverables through reuse of existing knowledge from a wide variety of sources. Additionally, the tool suite and the associated content helps to rapidly build the skills of new consultants thereby helping to grow the service delivery organization. From a client's perspective, the reuse of existing ERM knowledge helps to accelerate ERM engagements as well as reduce their costs. We also hope that once the engagement is completed, clients will choose to take ownership of the ERM repository and tools that have been populated with client-specific information and use it regularly within their strategic planning cycle.

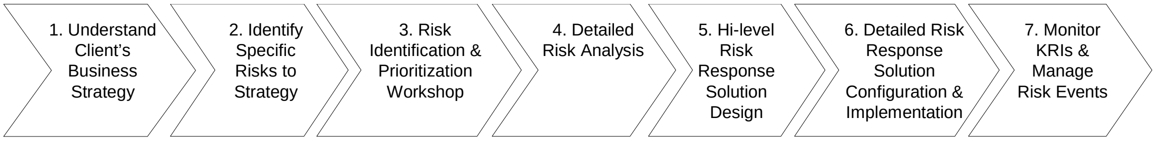
Our main contributions in this work can be summarized as follows.

- First, our knowledge-based ERM tool contains a rich repository of risk-related content organized for efficient search, and retrieval. This speeds up the risk and root cause identification and helps conduct the risk assessment and detailed analysis in a structured and consistent manner.
- Second, the classic and traditional qualitative and quantitative risk analytics are enriched with novel visualizations to help users query and view risk-related content. This provides multiple perspectives and useful insight in the context of larger business environment.
- Finally, the tool supports the risk management life-cycle by integrating design-time activities with day-to-day risk monitoring and management. This encourages risk management at enterprise level rather than in silos and enables active management of risks.

The rest of the paper is organized as follows. We present an overview of our ERM methodology in Section 2. Section 3 provides details of our knowledge-based ERM decision-support tool and discusses how it can be used within a client engagement. We conclude in Section 4 with a discussion on the enablers for acceptance of the ERM tool suite within the business consulting and client communities and on further exploration areas.

ERM METHODOLOGY

Similar to other traditional ERM methods [3] [4], our ERM methodology also encompasses all aspects of risk management, including the identification of particular risks and opportunities relevant to the organization's objectives, assessment of the likelihood and magnitude of impact of these events, the determination of a risk response strategy and its enterprise-wide deployment, monitoring for signs of the occurrence of events and the crisis management to handle such events should they occur. However, as noted in the Introduction section, we enrich this methodology with an ERM knowledge repository and the associated decision-support tool with novel visualization techniques. Figure 1 shows the traditional ERM methodology and the various steps involved in it. An overview of the various steps in the ERM method is provided below in this section. An overview of the decision-support tool is presented in Section 3.


1. Understand Client's Business Strategy
2. Identify Specific Risks to Strategy
3. Risk Identification & Prioritization Workshop
4. Detailed Risk Analysis
5. Hi-level Risk Response Solution Design
6. Detailed Risk Response Solution Configuration & Implementation
7. Monitor KRIs & Manage Risk Events

1. **Understand Client Business Strategy**: The method starts with understanding the client's business objectives and any existing or proposed business strategies to meet these business objectives. The actual design of the business objectives and business strategies is outside the scope of our ERM method and is assumed to be provided as input by the client. However, analysis of the business objectives and business strategies from the perspective of risk management is within the scope and in fact one of the main deliverables from our ERM method. In Section 2 we describe how using our decision-support tool one can examine the business objectives, visualize how well the company is doing against the desired targets using various heat maps and gain understanding of where the company is, what the underperforming areas and the associated risks and opportunities are.
2. **Identify Specific Risks to Strategy**: In our approach, anything that can prevent the client from meeting their business objectives is considered a business risk. This all encompassing approach is important to move away from the silo-oriented mentality of traditional risk management wherein only those risks are included and analyzed that the specific business function is familiar with and feels empowered to control. By casting the net for risks far and wide, the ERM approach provides a more holistic and broader enterprise-level view of risks. Many of these risks can be identified by searching through the ERM content in our ERM knowledge repository and via interviews with client executives and subject matter experts. Along with the identification of risks any supporting data should also be collected to help with downstream steps of the ERM methodology. The result of this step is a set of risks that are considered pertinent to the client's business objectives.
3. **Risk Assessment and Prioritization**: Risk is assessed in terms of the likelihood of a risk event and its financial impact upon occurrence. Both the risk likelihood and impact are assessed along a four-point qualitative scale that is defined by Low, Medium_Low, Medium_High, and High. For each client, the qualitative scale is calibrated to suit the client's perception of risk event frequency (e.g. number of events per year) and financial impact (range of monetary loss associate with each level of the scale. For example, Low being loss below $250 thousand and High being loss above $10 million, etc.). For each risk that has been identified as pertinent to the business objectives, the risk exposure is assessed based on interviews with client executives and subject matter experts. This assessment is completely subjective and its value can be improved by surveying multiple business people knowledgeable about the risk and using averages and variances to assess the quality of the information. Such surveys can be either conducted via interviews, online surveys, or also in workshop settings wherein experts from multiple parts of the business are invited to participate. The result of this step is a shortlist of prioritized risks that are considered important enough to be analyzed in greater detail.
4. **Detailed Risk Analysis**: The list of prioritized risks is expected to be small which should allow for detailed analysis of these risks from several perspectives. Most techniques for risk analysis, especially in the financial industry, focus on quantitative approaches that require use of loss data distribution, but these may not always be available easily for all business risks. Hence, we propose the use of combination of qualitative and quantitative analysis to provide business executives with a good understanding of their ERM environment as well as specific risks. Examples of the qualitative risk analyses include the standard root cause analysis, ERM environment analysis, ERM coverage analysis, and ERM heat map analysis. Examples of quantitative risk analysis for ERM investment decision-making include cost-benefit analysis of various risk controls as well as generating an optimal portfolio of risk controls for maximum risk reduction under given budgetary constraints. More details of these risk analyses capabilities are provided in Section 3 when we discuss our ERM tool suite capabilities..
5. **High-level Risk Response Solution Design**: The high-level risk response solution approach consists of two levels: choosing a risk response strategy and defining the organizational, systems, process aspects of the risk response strategy implementation. Depending on the client's risk appetite and estimated residual risk values after implementing some risk mitigation solution, the risk response strategy can be to either completely avoid the risk, accept the risk, share the risk with third parties such as insurance providers or joint venture partners, or mitigate the risk by reducing the likelihood of risk event, reducing its impact or both. Once the risk response strategy has been selected for each risk, this is followed by summarizing and creating risk response projects based on the information gathered during the previous steps. This information includes a shortlist of prioritized risks, designated organizational risk ownership, identified root causes, reused existing risk controls, new risk mitigation projects identified, key risk indicators to be tracked, and role-based risk ownership for managing

various risks. These elements make the structure of the high-level risk response solution which provides the input to the next step in the ERM methodology.

6. **Detailed Risk Response Solution Configuration & Implementation**: The risk response solutions designed are then implemented using various projects and are setup for monitoring on an ongoing basis. The monitoring itself can manifest as role-based risk dashboards for risk owners that display the current values of various KRIs along with trends, threshold values, etc. The information collected and decisions made during the previous steps can be used to automatically configure risk monitoring applications from various independent software vendors (ISVs). Additionally, the high-level design can also be used to configure various audit solutions that allow the auditors to keep tabs on risks, interview risk owners, and in short leverage the thinking that went into high level risk response solution design.
7. **Monitor Key Risk Indicators (KRI) & Manage Risk Events**: Our notion of ERM goes beyond the risk mitigation aspects to also include the activities that occur during and after a risk event. Beyond the operational risk monitoring which is the responsibility of role-based risk owners, the effectiveness assessment of the KRIs being tracked, the organization risk ownership, and the risk mitigation controls implemented is an important step in the continuous improvement of the ERM environment. The organizational learning from tracking new risks, understanding changes to the business objectives and business strategy and its implications to the risk prioritization, KRIs, organizational ownership, etc. is a critical part of enabling ERM best practice.

A KNOWLEDGE-BASED DECISION-SUPPORT TOOL FOR ERM

The methodology as shown in Figure 1 is quite commonplace. We believe our differentiation lies in (a) our ERM knowledge repository, (b) the multiple perspectives and visualizations we provide in our decision-support tool for conducting risk analytics and (c) the lifecycle approach to risk management enabled in the tool. Together, these features improve the quality of risk assessment and analysis while improving the business consultant's productivity. Our ERM tool suite design is modular and consists of several integrated components as shown in Figure 2. Our tool suite takes business objectives, existing controls, organizational structure, and process hierarchy models as inputs for various analyses. The knowledge repository contains rich risk content and provides various insights that are qualitative in nature. The Risk analysis workbench combined with business case analysis tools provides insights based on both qualitative and quantitative analyses. We describe some of the components in detail in the remainder of the paper.

ERM MODELER

This module shown in Figure 2 supports steps 2 and 3 in the ERM methodology shown in Figure 1. It allows the user to create templates for various ERM elements such as risk, root cause, key risk indicators and metrics, risk controls, etc. Client-specific content is then captured in template to create new instances of these ERM elements. The ERM modeler also allows the user to model relationships amongst various ERM elements, which we believe are just as important as defining the details of an individual ERM element. Examples of relationships include a risk and

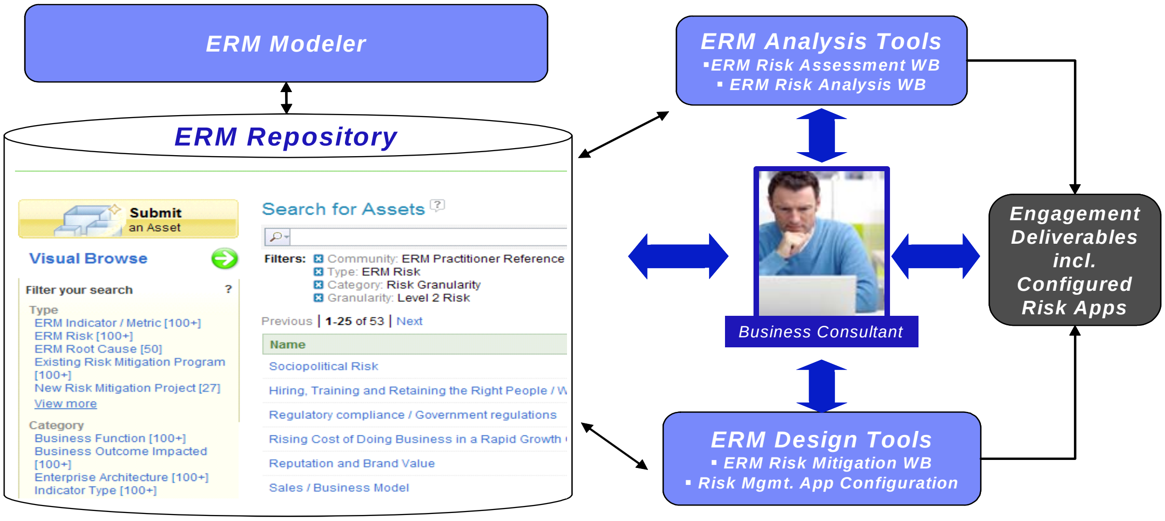
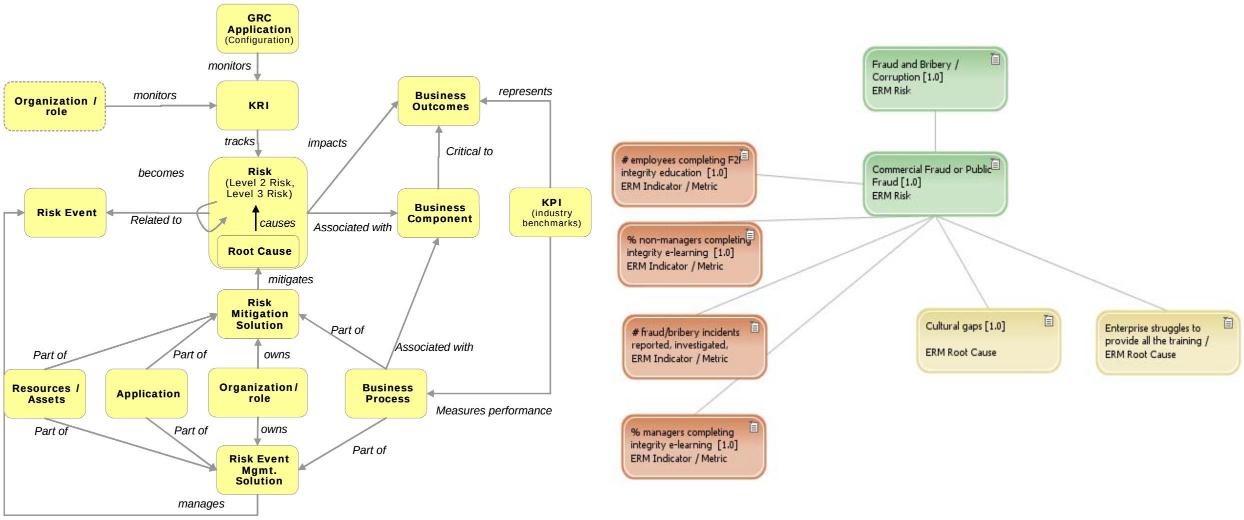

ERM Modeler
ERM Repository
Submit
an Asset
Visual Browse
Filter your search ?
Type
ERM Indicator / Metric [100+]
ERM Risk [100+]
ERM Root Cause [50]
Existing Risk Mitigation Program [100+]
New Risk Mitigation Project [27]
View more
Category
Business Function [100+]
Business Outcome Impacted [100+]
Enterprise Architecture [100+]
Indicator Type [100+]
Search for Assets
Filters: Community: ERM Practitioner Reference
Type: ERM Risk
Category: Risk Granularity
Granularity: Level 2 Risk
Previous | 1-25 of 53 | Next
Name
Sociopolitical Risk
Hiring, Training and Retaining the Right People / W
Regulatory compliance / Government regulations
Rising Cost of Doing Business in a Rapid Growth
Reputation and Brand Value
Sales / Business Model
ERM Analysis Tools
▪ERM Risk Assessment WB
▪ ERM Risk Analysis WB
Business Consultant
Engagement Deliverables incl. Configured Risk Apps
ERM Design Tools
▪ ERM Risk Mitigation WB
▪ Risk Mgmt. App Configuration

Figure 2. A component view of our ERM decision-support tool

its related root causes, a root cause and its related risk controls, a risk and its related key risk indicators, etc. Figure 3 shows the ERM model comprising of various ERM elements and associated relationships. In order to understand the client's ERM environment, the ERM modeler allows the user to graphically visualize the ERM model. Additionally, the ERM Modeler has a web-based user interface thereby allowing multiple team members to remotely access the ERM content and work collaboratively to create ERM content. An example of such an ERM model is shown in Figure 3. It showcases a risk (employee committed fraud and bribery risk) for a fictional company in an emerging market for which two root causes have been noted (1. cultural gaps between the parent company and its emerging market subsidiary, and 2. lack of proper communication and training of company's values to its employees). Some of the metrics used for measuring this risk (# of fraud incidents in the past 2 years) and the effectiveness of the risk response solutions (# of employees, managers completing business ethics education) are also shown in the picture. Only a small portion of the overall risk network for 'employee committed fraud and bribery' risk is shown in Figure 3 for illustrative and readability purposes.



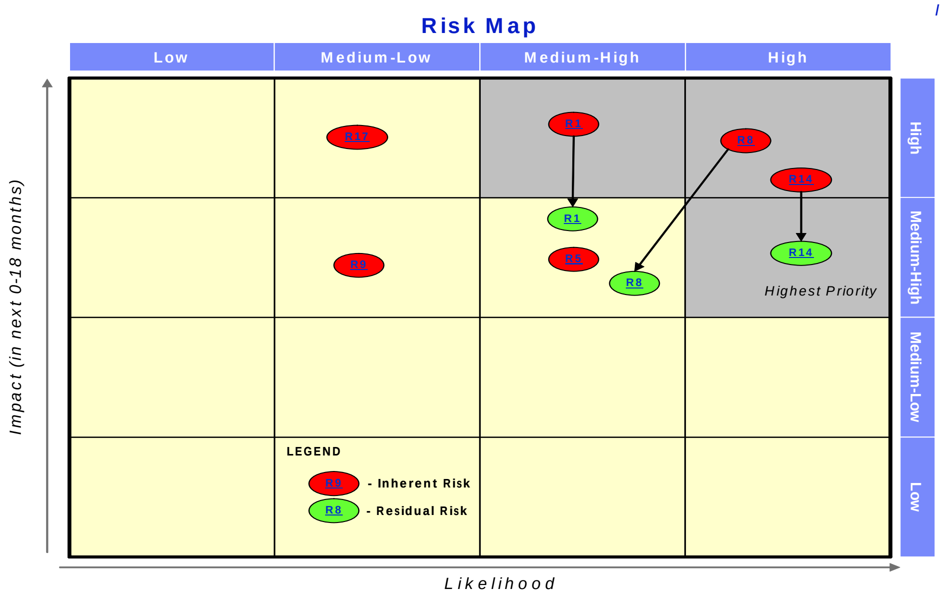
ERM REPOSITORY

The ERM repository is essential to integrating various steps within the ERM methodology shown in Figure 1. It allows the users to store, organize, and retrieve ERM content created by various components of the ERM tool suite while controlling user access and authorization to ensure that sensitive data is disseminated only on a need to know basis. The ERM elements can be organized using multiple risk taxonomies simultaneously such as industry, business function, geography, risk type, etc. The ERM content thus organized can be rapidly searched using both filters and keywords as shown in Figure 2. This allows the user to formulate interesting queries to retrieve say for example, all risks that apply to enterprises in a specific industry, located within a specific geography and trying to achieve a specific business objective. We have also introduced additional capabilities within the software to replicate parts of the ERM model across multiple projects thereby improving user productivity.

ERM RISK ASSESSMENT WORKBENCH

This module supports step 3 in the ERM methodology shown in Figure 1. The ERM Risk Assessment Workbench is designed to help the user capture risk assessment information regarding various risks in terms of likelihood of a risk event and the impact should such an event occur. Optionally, users can also include the risk velocity, i.e. an estimate of the time frame within which such a risk event might occur, as part of the risk assessment information. The ERM Assessment Workbench is integrated with the ERM Repository thereby allowing the user to review any ERM content while making risk prioritization decisions. The risk assessment values are used to automatically generate the ERM Risk Map as shown in Figure 4, which allows the user to position various risks relative to each other based on their inherent risk likelihood and impact. The inherent risk assessment provides an estimate of the risk likelihood and impact when no risk mitigation action is put in place. For many business risks, such information is usually very subjective but the relative comparison amongst risks helps in prioritizing risks for further analysis. These prioritized risks are shown in the top right quadrants in the ERM Risk Map. Based on the risk assessment and the potential to reduce the risk likelihood, impact, or both, the business consultant can recommend various risk response actions such as:

- Risks that are considered high priority (in the top right corner) but have limited risk reduction potential can be either completely accepted or completely avoided (for example by changing the business model).
- Risks considered high priority in the top right corner that have high potential for reduction can be either shared (for example by purchasing insurance or by establishing joint ventures with other parties) or mitigated (for example by reducing the likelihood, impact, or both through redesign of process / product / contract etc.). Such risks are then subjected to further detailed investigation for developing a detailed risk mitigation solution using tools discussed below.



Identified Risks

R1	Sociopolitical Risk
R5	Service Delivery
R8	Sales / Business Model
R9	Rising Cost of Doing Business in a Rapid Growth Country
R14	Regulatory compliance / Government regulations
R17	Market shifts / Market Opportunity Capture

ERM Risk Analysis Workbench

This module supports step 4 in the ERM methodology shown in Figure 1. The ERM Risk Analysis Workbench is designed to investigate in greater detail the client's ERM environment as well as specific risks. For this purpose, we provide both qualitative as well as quantitative analysis capabilities. Examples of qualitative analyses include:

1. Root Cause Analysis. For this we provide ability to graphically model risks and causal factors to assist consultants to brainstorm and identify root causes using 5-whys approach.
2. ERM Environment Analysis. This provides the user with an overview of inter-related ERM entities such as risks, related root causes, existing risk controls, existing organizational ownership, current business objectives impacted, and current key risk indicators. The ERM environment analysis allows one to answer a variety of questions that can be useful in understanding and improving the client's ERM environment. Some sample queries that can be answered include: Which risks impact my business objectives? What are the root causes associated with these risks? Which organizations are impacted by any specific risk? Where does the organizational risk ownership reside for a specific risk? Which root causes and associated risks will be impacted by new risk mitigation projects? Which risk metrics and key risk indicators (KRIs) are meaningful for specific risks?
3. ERM Coverage Rationalization including,
    - *Risk Control Rationalization* to understand how well identified risks are covered by existing risk controls. Some risks may have too many controls and could be candidates for reduction and associated costs. On the other hand, some risks may have no risk controls and require investment.
    - *Organizational Ownership Rationalization* to understand which risks impact several organizations and which organization should own it. Traditionally, each organization tends to mitigate its risks without taking

into account how similarly affected organizations are mitigating the same risks. This silo-oriented approach to risk management can lead to problems at the enterprise level as noted in the automotive company example [2] in the Introduction section.

- *Root Cause Rationalization* helps to understand whether one or more root causes have been identified for each prioritize risk. Issues such as do any risks have too many root causes requiring further rationalization and are there risks where no root causes have been identified are addressed.

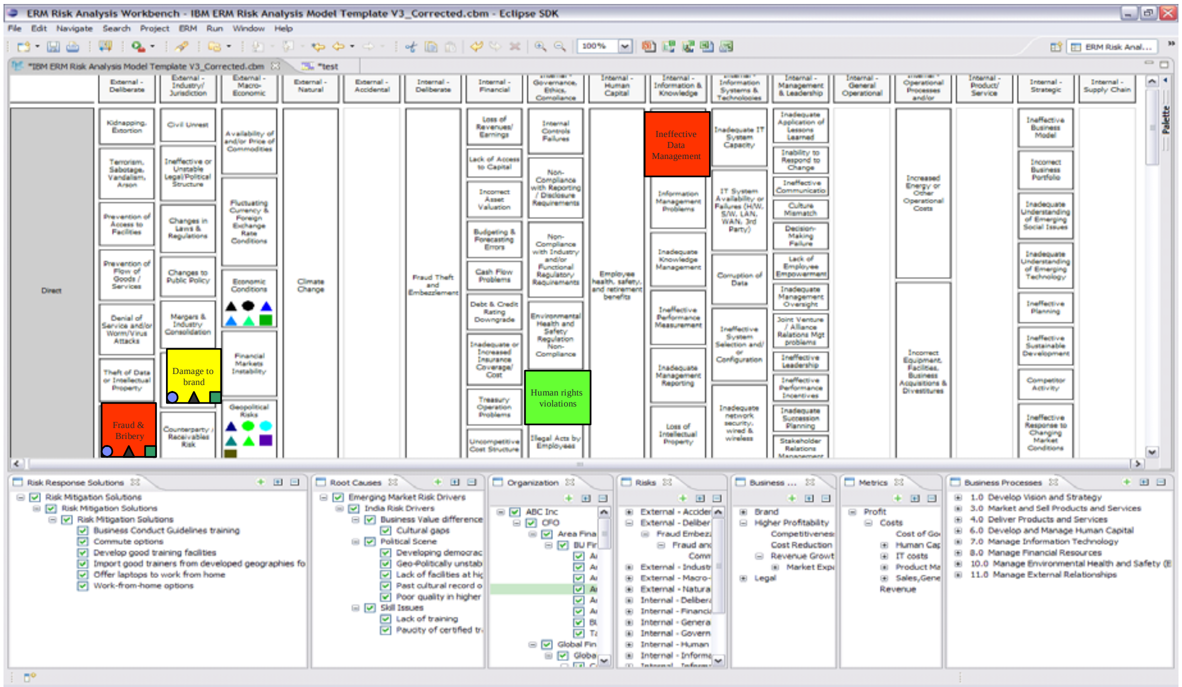
4. ERM Heat-map Analysis. Using a color-coded map as shown in Figure 5, this analysis highlights risks that are within acceptable range and those that are outside the acceptable range. Such a risk heat map can be useful in both the pre-mitigation stage (comparing inherent risk vs. acceptable risk) and in the post-mitigation stage (comparing residual risk vs. acceptable risk). Detailed ERM heat-map highlighting the gaps between measured and acceptable values of specific risk metrics is also available.

Our quantitative risk analysis is primarily to support making ERM investment decisions by understanding the financial implications of risks and risk mitigation projects. Examples of quantitative analysis include

1. *Cost-benefit analysis* that compares the cost of reusing existing risk control or implementing new risk control with its estimated risk reduction can be very useful in making ERM investment decisions.

2. *Risk control portfolio optimization*. The ability to recommend an optimal portfolio of risk controls that achieves the largest risk reduction while respecting budgetary constraints is a very useful decision support feature [7]. Additionally, there are opportunities to present various risk control portfolios in terms of an efficiency frontier thereby allowing the user to choose an operating point in line with their budgetary and risk reduction preference. This module supports step 5 in the ERM methodology shown in Figure 1. The risk analysis performed in step 4 allows the user to make several operating decisions such as: Which risks to mitigate and select appropriate risk mitigation solution? Which key risk indicators to track for a given risk? Which organization should own a particular risk? Which organization role should be responsible for owning the risk response solution, for tracking associated key risk indicators, etc? These decisions are aggregated to provide a structure for various risk mitigation solutions in the ERM Risk Mitigation Workbench.

3. *ERM Risk Mitigation Workbench*: This solution structure provides the input required for configuring various downstream vendor applications for risk monitoring, audit and compliance, project management, reporting, etc. (i.e., step 6 in the ERM methodology shown in Figure 1). The output of the ERM Risk Mitigation Workbench is in the form of an XML documents and csv file formats and is designed to automatically


ERM Risk Analysis Workbench - IBM ERM Risk Analysis Model Template V3_Corrected.cbm - Eclipse SDK
File Edit Navigate Search Project ERM Run Window Help
100%
ERM Risk Anal...
*IBM ERM Risk Analysis Model Template V3_Corrected.cbm
*test
Palette

Direct

External - Deliberate: Kidnapping, Extortion; Terrorism, Sabotage, Vandalism, Arson; Prevention of Access to Facilities; Prevention of Flow of Goods / Services; Denial of Service and/or Worm/Virus Attacks; Theft of Data or Intellectual Property; Fraud & Bribery

External - Industry/ Jurisdiction: Civil Unrest; Ineffective or Unstable Legal/Political Structure; Changes in Laws & Regulations; Changes to Public Policy; Mergers & Industry Consolidation; Damage to brand; Counterparty / Receivables Risk

External - Macro-Economic: Availability of and/or Price of Commodities; Fluctuating Currency & Foreign Exchange Rate Conditions; Economic Conditions; Financial Markets Instability; Geopolitical Risks

External - Natural: Climate Change

External - Accidental

Internal - Deliberate: Fraud Theft and Embezzlement

Internal - Financial: Loss of Revenues/ Earnings; Lack of Access to Capital; Incorrect Asset Valuation; Budgeting & Forecasting Errors; Cash Flow Problems; Debt & Credit Rating Downgrade; Inadequate or Increased Insurance Coverage/ Cost; Treasury Operation Problems; Uncompetitive Cost Structure

Internal - Governance, Ethics, Compliance: Internal Controls Failures; Non-Compliance with Reporting / Disclosure Requirements; Non-Compliance with Industry and/or Functional Regulatory Requirements; Environmental Health and Safety Regulation Non-Compliance; Human rights violations; Illegal Acts by Employees

Internal - Human Capital: Employee health, safety, and retirement benefits

Internal - Information & Knowledge: Ineffective Data Management; Information Management Problems; Inadequate Knowledge Management; Ineffective Performance Measurement; Inadequate Management Reporting; Loss of Intellectual Property

Internal - Information Systems & Technologies: Inadequate IT System Capacity; IT System Availability or Failures (H/W, S/W, LAN, WAN, 3rd Party); Corruption of Data; Ineffective System Selection and/ or Configuration; Inadequate network security, wired & wireless

Internal - Management & Leadership: Inadequate Application of Lessons Learned; Inability to Respond to Change; Ineffective Communicatio; Culture Mismatch; Decision-Making Failure; Lack of Employee Empowerment; Inadequate Management Oversight; Joint Venture / Alliance Relations Mgt problems; Ineffective Leadership; Ineffective Performance Incentives; Inadequate Succession Planning; Stakeholder Relations Management

Internal - General Operational

Internal - Operational Processes and/or: Increased Energy or Other Operational Costs; Incorrect Equipment, Facilities, Business Acquisitions & Divestitures

Internal - Product/ Service

Internal - Strategic: Ineffective Business Model; Incorrect Business Portfolio; Inadequate Understanding of Emerging Social Issues; Inadequate Understanding of Emerging Technology; Ineffective Planning; Ineffective Sustainable Development; Competitor Activity; Ineffective Response to Changing Market Conditions

Internal - Supply Chain

Risk Response Solutions
- ☑ Risk Mitigation Solutions
  - ☑ Risk Mitigation Solutions
    - ☑ Risk Mitigation Solutions
      - ☑ Business Conduct Guidelines training
      - ☑ Commute options
      - ☑ Develop good training facilities
      - ☑ Import good trainers from developed geographies fo
      - ☑ Offer laptops to work from home
      - ☑ Work-from-home options

Root Causes
- ☑ Emerging Market Risk Drivers
  - ☑ India Risk Drivers
    - ☑ Business Value difference
      - ☑ Cultural gaps
    - ☑ Political Scene
      - ☑ Developing democrac
      - ☑ Geo-Politically unstab
      - ☑ Lack of facilities at hig
      - ☑ Past cultural record o
      - ☑ Poor quality in higher
    - ☑ Skill Issues
      - ☑ Lack of training
      - ☑ Paucity of certified tr

Organization
- ☑ ABC Inc
  - ☑ CFO
    - ☑ Area Fina
      - ☑ BU Fir
        - ☑ A
        - ☑ A
        - ☑ A
        - ☑ A
        - ☑ A
        - ☑ A
        - ☑ B
        - ☑ T
    - ☑ Global Fin
      - ☑ Globa

Risks
- External - Accider
- External - Deliber
  - Fraud Embez
    - Fraud anc
      - Comm
- External - Industr
- External - Macro-
- External - Natura
- Internal - Delibera
- Internal - Financia
- Internal - Genera
- Internal - Govern
- Internal - Human
- Internal - Informa

Business ...
- Brand
- Higher Profitability
  - Competitivenes
  - Cost Reduction
  - Revenue Growt
    - Market Expa
- Legal

Metrics
- Profit
  - Costs
    - Cost of Go
    - Human Cap
    - IT costs
    - Product Ma
    - Sales,Gene
  - Revenue

Business Processes
- 1.0 Develop Vision and Strategy
- 3.0 Market and Sell Products and Services
- 4.0 Deliver Products and Services
- 6.0 Develop and Manage Human Capital
- 7.0 Manage Information Technology
- 8.0 Manage Financial Resources
- 10.0 Manage Environmental Health and Safety (E
- 11.0 Manage External Relationships

configure many parameters within the downstream vendor applications. This linking to risk monitoring, audit and compliance enables us to support a lifecycle approach to risk management. Risk management is not a one-time effort. Risks need to be constantly monitored and managed. Our tool supports linking the upstream design to downstream runtime tools making this process more seamless.

CONCLUDING REMARKS

Traditionally, risk management has been addressed in a piecemeal manner and tools have been developed to address specific areas within the larger enterprise risk management methodology. This paper presents an end-to-end approach to enterprise risk management starting with establishing and understanding the enterprise's business objectives and using a structured methodology supported by tools to (1) identify, assess, and prioritize risks, (2) analyze the prioritized risks along several dimensions to identify various risk control solution parameters, (3) create a high-level risk control solution structure, and (4) integrate with downstream risk monitoring, audit, and other applications available for implementing risk management within an enterprise. The use of an integrated ERM decision support tool suite to support the end-to-end enterprise risk management methodology provides several advantages including (1) information collected and decisions made within one stage of the methodology are captured and moved to the next stage without loss, (2) the collaborative, web-based tools improve the transparency of risk management process within the enterprise thereby reducing a silo-oriented risk management mentality and associated problems that are commonly found in many larger organizations, and (3) it improves the enterprise's ERM capability by fostering a common vocabulary across multiple business units within the enterprise and helps to make risk management an integral part of business operations. Additionally, a balanced approach to risk analysis where business insight is offered via both qualitative and quantitative methods allows more participation by business executives leading to richer modeling of the client's ERM environment. In designing the ERM tool suite, we have taken into account several inputs from both business consultants and clients. Some key concerns include the security of the risk-related information and ability to control access to this information on a need to know basis. Our tool supports this requirement for information protection.

The tool suite can be improved further along several dimensions. Some areas for further exploration include development of methodology and tooling to support integrated risk analytics that seamlessly tie qualitative risk analysis with quantitative risk analytics. Additionally, feedback mechanisms that support assessment of the effectiveness of the ERM solution based on risk monitoring and risk event data can help in further fine-tuning and improving the ERM capabilities of the enterprise.

In undertaking ERM engagements, we have encountered some interesting situations such as some client's reluctance to proceed unless they have set aside adequate budget and made proper arrangements to implement the ERM-related recommendations. This is because knowing the risks and not implementing relevant risk controls could make them susceptible to potential shareholder lawsuits and government regulators. In their view, not knowing the risks appears to be a safer bet. In other cases, clients were reluctant to document all their risks in a tool as that would leave them susceptible to legal complications when those risks are not properly mitigated. In future, we hope that success stories from adopting the ERM framework will mitigate such apprehensions by companies.

REFERENCES

[1] *IBM Global CFO Study 2008 http://www-935.ibm.com/services/uk/gbs/html/2008cfostudy.html*

[2] *How Enterprise Risk Management Increases Value for Your Organization" By Lawrence Burke, CPA – Florida CPA today May/June 2008 (htttp://www.ficpa.org)*

[3] *Enterprise Risk Management – Integrated Framework (Executive Summary and Framework) by the Committee of Sponsoring Organizations of the Treadway Commission, September 2004.*

[4] *Risky Business II: Enterprise Risk Management as a Core Management Process (Executive Summary), APQC Consortium Benchmarking Study 2008.*

[5] *IBM Solution Brief: Cognos Business Intelligence and Financial Performance Management – Enterprise Risk Management*

[6] *SAP Solution Brief: SAP Businessobjects Risk-Adjusted Management of enterprise performance – Enabling enterprise risk management*

[7] *D. Subramanian and F. Cheng, "Operational risk quantification & counter-measure portfolio optimization", Proceedings of the 2008 Winter Simulation Conference, Editors, S. J. Mason, R. Hill, L. Moench, and O. Rose.*