RC25329 (WAT1211-046) November 14, 2012
Computer Science

IBM Research Report

Knowledge Driven Enterprise Risk Management

Nitin Nayak
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 208
Yorktown Heights, NY 10598
USA

Rama Akkiraju
IBM Research Division
Almaden Research Center
650 Harry Road
San Jose, CA 95120-6099
USA

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

Knowledge driven Enterprise Risk Management

Nitin Nayak
IBM Thomas J. Watson Research Center
Hawthorne, New York, USA
nnayak@us.ibm.com

Rama Akkiraju
IBM Almaden Research Center
San Jose, California, USA
Akkiraju@us.ibm.com

***Abstract*—In this paper we describe a knowledge management approach for addressing enterprise-level risks and present our experiences in piloting its implementation within a large, multi-organizational enterprise. Our approach facilitates cross organizational discussion and enables enterprise-level perspectives in risk identification, analysis and management thereby avoiding the dangerous pitfalls of silo-approach to risk management. Our tool consists of two parts: (1) a knowledge management tool that enables the collection, and visualization, of risk data and collaboration among risk managers of various organizations within an enterprise (2) an Enterprise Risk Management (ERM) risk assessment and analysis workbench that enables risk managers to (a) qualitatively analyze the interrelationships among various risk elements, and their impact on business objectives and (b) quantitatively assess the risk exposure, and the impact of risk mitigation projects. To the best of our knowledge this is the first of its kind of a tool that provides a knowledge management based approach to enterprise risk management.**

Keywords-component; Enterprise Risk Management, Knowledge management tools for risk

I. INTRODUCTION

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. Best practices for enterprise risk management have steadily matured over the years as is evident from the release of several industrial standards, including ERM Integrated Framework from COSO [1] and the most recent ISO-31000 standard for risk management from the International Standards Organization in 2009 [2]. These best practices focus on the available techniques and guidelines to perform various steps in the ERM process outlined in Figure 1.

Despite the progress made on the ERM methodology aspect, many organizations are still finding it challenging to implement these best practices. In our view this situation is primarily due to the lack of appropriate tools to support the implementation of ERM processes in large multi-organizational enterprises. For such organizations the ERM process is more than just monitoring and managing risks. For them the ability to identify fast evolving risks across one or more business units and geographies, ability to have a common risk language across the enterprise, ability to promote risk-related learning across business units and geographies about causes of various risks, various mitigation techniques for similar risks in different contexts, and getting an overall sense of the enterprise's risk profile is also important.

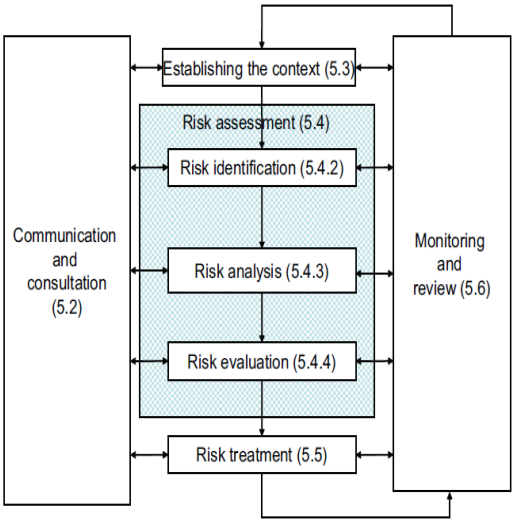


Figure 1. ISO 31000 risk management process

Most tools that are currently available focus on monitoring and managing risks without providing much help for identifying the right risks, analyzing their root causes, and aiding in making investment decisions in appropriate risk mitigation solutions on an ongoing basis. As a result, many enterprises that invest only in risk monitoring and management solutions for individual organizational units may have a false sense of being well-prepared. They may not realize that their traditional silo-approach to risk management is inadequate to address enterprise-level risks. In our view, tools that improve risk transparency and risk understanding across all parts of an enterprise are much better at both identifying the emergence of enterprise level risks and developing creative, cross-functional risk mitigation and management solutions for addressing these risks. Additionally, these

tools can also address other important issues such as loss of risk-related expertise as baby boomers retire.

In this paper we describe a knowledge management approach for addressing enterprise-level risks along with our experiences in piloting its implementation within a large, multi-organizational enterprise. Our ERM process pilot implemented a schedule-driven data collection process to integrate risk-related information from various parts of the global enterprise in order to understand their enterprise-level impact, allow an enterprise-wide status review of various risk mitigation projects, and also highlight opportunities for cross-organizational learning where multiple business units are facing similar risks. In implementing the ERM process we have identified the need for three kinds of role players – business managers, executive decision-makers, and ERM analysts, along with their role-based tool requirements. The knowledge management tool that we have developed provides features to improve the ease of expressing risk-related information for business managers, introduces a common risk-related taxonomy across the enterprise, improves cross-organizational learning related to risk mitigation and management activities, helps identify the emergence of enterprise-level risks that usually comes as a surprise to senior executives and the board of directors, and analyzes financial investments in expensive risk mitigation solutions based on their enterprise-wide risk reduction benefits and returns on investment.

The remainder of the paper is organized as follows. Section II provides an overview of some of the challenges in implementing ERM program in large multi-organizational enterprises. Section III describes the salient features of the knowledge-based ERM workbench tool designed and developed to address the above challenges. In Section IV, we share our experiences in implementing an ERM program that leveraged the ERM workbench in a pilot situation. Section V concludes the paper with some observations on ERM programs as well as areas where we think further improvement and investigation is required.

II. CHALLENGES IN IMPLEMENTING AN ERM PROGRAM IN LARGE, MULTI-ORGANIZATIONAL ENTERPRISES

There are several challenges in implementing ERM programs, especially within large, multi-organizational enterprises – both organizational challenges as well as tool-related. This section provides an overview of these challenges that we either encountered in our pilot or were provided as business requirements by experts from the enterprise's financial function as well as mentioned by several Chief Financial Officers (CFOs) and Chief Risk Officers (CROs) of major US firms with whom we had the opportunity to interact. Along with the description of the challenges, we have also outlined the shortcomings of current ERM tools to address these challenges and business requirements.

A. Organizational Challenges

Organization's openness to implementing an ERM program: Although it sounds incredulous, one of the biggest challenges is overcoming senior executive and board's concerns about implementing ERM programs. Besides the cost-benefit argument, one of the interesting concerns we came across was the concomitant increase in enterprise's liability with increased awareness of its risks. The issue here is that if the ERM program identified certain imminent risks but there weren't adequate enterprise resources to fund their monitoring, mitigation, and management then the enterprise would be open to lawsuits for negligence in case the risks did materialize. Knowing about risks but not implementing corrective actions is tantamount to shirking management responsibility in their minds. However, this kind of thinking should have no place in any forward-looking enterprise. ERM was designed to help enterprise's identify and prioritize risks so the management can decide what to do about them; in some cases nothing by design and accepting the consequences. Not knowing the risks is not the equivalent of not having those risks [3].

Turnover of experienced risk professionals: Assessing risks involves a certain amount of domain and historical knowledge to properly gage the likelihood and impact of these risks. Most organizations will have a specific budget that in most cases will not cover mitigation of all the identified risks. Experienced employees weigh in on the risk assessment to decide which risks are most likely and/or most devastating to create a shortlist of risks that can be analyzed, mitigated, and managed. With large numbers of baby boomers retiring across the globe, one can expect a shortage of experienced risk management staff. This situation can be addressed to a large extent by centralizing the risk-related knowledge based on a common taxonomy and covering all aspects of the ERM model (see bullet further down on the ERM model details)

Employees' hesitation to voice opinion: In a multi-organizational enterprise with operations in several parts of the globe, one commonly encounters certain cultural practices that prevent junior employees from freely voicing their opinions in the presence of senior management. These situations may prevent the enterprise from correctly identifying and assessing evolving risks as well as prevent from improving the capabilities of existing risk mitigation programs. Such situations can be corrected to some degree by supporting anonymous input by all participants using tools with anonymized voting feature.

Too much dependence on siloed thinking versus enterprise-level thinking: Traditionally, risks have been managed within functional silos such as production-related risks, supply-related risks, financial risks, etc. However, silo-based risk management 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 [4]. 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.

Knowledge management and data review process: Although this is usually addressed within the ERM tool, the issue of having submission and review process is a critical one in order to maintain adequate data quality in the ERM knowledge-base as well as to prevent duplication of risk-related information. Allowing free submission of risk-related data into the ERM knowledge-base is important but controlling the final quality of the submission requires a pre-established data review process and dedicated team.

B. Tool-related concerns and requirements

Risk assessment (likelihood and impact) approaches: There are three approaches to modeling risk assessment based on the data type – quantitative, semi-quantitative, and qualitative. Although at first glance, quantitative modeling seems more detailed and more amenable to mathematical manipulation, the challenge is that risk likelihood and risk impact are both highly probabilistic. Having a numeric value gives the impression of precision to variables that are widely varying estimates [1]. On the other hand, only qualitative approach such as Low, Medium, High values are easy to provide but the meaning associated with these values can change from person to person, across business units and across geographies. Additionally, these values do not lend themselves to any form of mathematical aggregation. Our preferred approach is to go with semi-quantitative approach which tries to capture the ease of qualitative values and associates these values with numeric ranges to support high-level computation.

Assessing effects of correlated risks across different parts of the enterprise: Many risks that are small from the perspective of individual business units are usually ignored when it comes to risk mitigation. However, if these risks are common to several business units and are also correlated then their impact can be quite significant at the enterprise-level. Examples of such risks include currency exchange rate fluctuations as well as natural disasters that could impact several country operations simultaneously. The ability to identify and model these correlated risks at the enterprise level becomes important.

Support for knowledge sharing and organizational learning: From the senior executive's perspective, this is an important issue to enable an ERM program. The ability to quickly learn about specific risks, their related root causes, associated risk mitigation actions and their effectiveness, key risk indicators to track, etc. within and across business units is one of the key advantages of implementing an ERM program. Additionally, the users should have the ability to provide feedback and ratings on the data quality as well as ability to reuse data from the common data source to reduce duplication.

Common risk-related language (taxonomy): This is complementary to the requirement above. Having multiple definitions of the same risk element within a multi-organizational enterprise reduces data quality, increases search time, and reduces reusability to say the least. Having tools to help an enterprise-wide review committee to update and manage the ERM repository content is crucial [5].

Comprehensive ERM-related data model with both risk elements and relationships: The scope of the ERM related data model is usually decided by the scope of features a tool provides. Given the preponderance of risk monitoring and risk management tools, the most common risk-elements include risks, risk management techniques, risk owners, and key risk indicators. Many other important elements such as risk causal factors, risk mitigation solutions, and performance indicators of risk mitigation solutions may or may not be included. Figure 2 below shows a comprehensive ERM entity model and associated relationships.

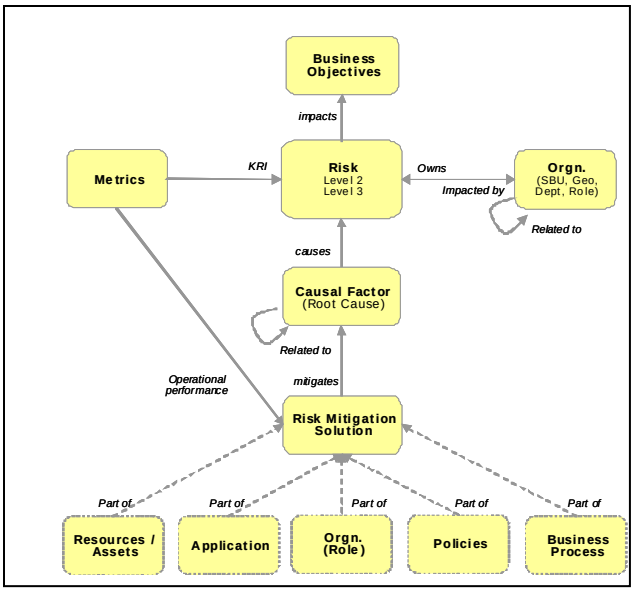


Figure 2. Our enterprise risk element model

Ability to analyze cross-effects of changes to various risk elements: An important view into the enterprise's ERM environment is the view of various relationships amongst models of risk elements. Knowing which root causes are common to multiple risks and which risk mitigation solutions can address these root causes along with links to associated risk owners is critical to quickly traversing and understanding the complex many-to-many relationship structure.

Support for making optimal risk-related investment decisions: As mentioned earlier, the budget for mitigating and managing risks is usually limited and so has to be

stretched to address several risks. Knowing which risk mitigation solutions provide the most reduction in the enterprise's risk exposure is a good way to optimize investment decisions.

C. *Data-related concerns and requirements*

Data analytics techniques such as statistical analysis, data mining, and predictive learning have had a major impact on how businesses learn, organize and manage themselves. These techniques rely on historical data collected over several years and so the choice of data elements now to be collected over a long period will decide what kind of analysis is possible in future. The selection of data elements should be guided by a clear articulation of what the business wants to learn about itself. This will further drive the choice of appropriate model designs and consequently appropriate data to collect. For risk assessment, the required data can be qualitative, semi-quantitative, and quantitative in nature depending on the solution technique used. Additionally, data related to analyzing risk mitigation projects is equally important. This data allows one to model and understand solution implementation progress, solution effectiveness, effect of solution variations, etc. Below are some examples of business learning objectives related to risk and their data implications.

Ability to identify emergence of new risks across the enterprise: This really boils down to having an ability to collect the current risk sentiment from multiple organizations in a common format and based on a common schedule. This will require the availability of online tools for gathering risk data and also having the appropriate role players such as ERM analysts to analyze the risks at the enterprise level.

Support for capturing risk assessment data from various starting points: In some situations of assessing risks, it may be useful to start with a clean slate and get inputs from independent parties on the likelihood and impact of specific risks. This makes sense in the case of new risks that may have not been identified before because one shouldn't bias the assessment value. On the other hand, there are situations where the likelihood and impact values may be pre-selected either based on their values in the previous period or based on the knowledge of risk experts.

Support for enterprise risk modeling for different sizes of constituent organizations: The risk appetite of an organization also depends on its size. For a large organization, what represents Low impact risk could in fact be Medium or High impact risk for a small organization. For ERM purposes however, the different scales should be normalized based on the risk appetite at the enterprise-level.

III. DESIGN OF THE ENTERPRISE RISK MANAGEMENT WORKBENCH TOOL

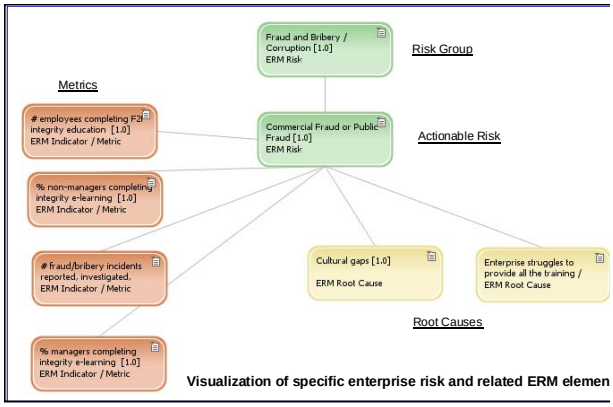
The design of the ERM Workbench is based on two complementary principles: provide support for the traditional tools for risk identification, assessment, analysis, mitigation and management and then enhance these further with a common, collaborative environment to promote knowledge sharing and reuse, organizational transparency, and collaborative risk mitigation solution design. The section below provides an overview of the various modules:

A. *ERM Modeler*

The ERM modeler feature helps model the client's ERM environment for purposes of risk assessment, analysis, mitigation solution design, and management. It supports a structured model consisting of the following risk elements and their relationships:

- Business objective – these drive the identification of risks. A risk is only a risk if it will prevent achievement of the business objectives.
- Risk – these are modeled at various levels of granularity (usually 3) to describe further specialization of the risk. For example, Financial Risk (level 1) may have several level 2 risks such as fraud by employees, currency risk, etc. The fraud itself may have further specialization such as embezzlement, insider trading, malfeasance, etc. at level 3.
- Causal Factor – There could be several drivers of risk and the main causal factors are termed as root causes. Each risk may have several root causes and on the other hand, each root cause could affect several risks.
- Risk Mitigation Solution – These preventive measures are associated with addressing level 3 risks (also termed actionable risks). These solutions can have several components including processes, policies, organizational roles, applications, and other resources/assets for preventive risk events. Each risk mitigation solution can be used to address multiple root causes and on the other hand, each root cause may have several risk mitigation solutions associated with controlling it.
- Metric – These are both key risk indicators (KRI) for tracking risks and key performance indicators (KPI) for tracking performance of risk mitigation actions.
- Organization – Modeled at several levels of hierarchy, these are associated with ownership of managing specific risks. Each organization may be responsible for managing multiple risks but in many enterprises, each risk may be owned by only one organization to prevent confusion of ownership.

The ERM modeler is web-based and provides a set of pre-designed templates of the above ERM elements and their associations so the users can configure them with



Visualization of specific enterprise risk and related ERM elemen

client-specific details. It also provides the ability to visualize details of the client's ERM environment as shown in Figure 3.

Figure 3. Enterprise risk model for a specific risk: 'Fraud and Bribery'

B. *ERM Repository and knowledge-base*

The ERM content in the form of customized ERM models and their associations are organized using multiple risk taxonomies (industry, domain, etc.). Usually, a set of pre-configured ERM model elements is available to all users for reuse in the form of ERM reference models. Users can copy these into their own project space and edit them as appropriate for further customization. At any stage, the ERM model can be graphically visualized to understand the big picture and relationship details as shown in Figure 3. In addition to the structured ERM model, there is also web-based, rich collaborative platform that allows users to have context-specific discussion threads, comments, attachments, and ratings for various ERM elements. Fast ERM content searching using both filters and keywords is also available. Access to the ERM Repository is controlled and users given either read or write permissions to ERM models based on their access privileges.

C. *ERM Risk Assessment Workbench*

The risk assessment technique used in the ERM tool suite uses semi-quantitative data for reasons discussed in section II. Additionally, for enterprises with business units of different sizes the choice of semi-quantitative data helps to transform risk impact values for one business unit to be compared with another business unit with different risk tolerance. The values of risk likelihood and impact are input from mostly expert judgement since for emerging risks there may be limited data availability. The workbench is integrated with ERM Repository and is used for collecting enterprise-wide risk assessment data for risks identified by each business unit or country and generating related risk maps as shown in Figure 4. These risk maps are drawn to organization-specific risk scale based on organization's risk appetite and describe the impact in both qualitative terms (e.g. Low, Medium, and High) as well as associated financial range. Individual organization-level risks can also be transformed using the enterprise-level risk scale to identify risks that may be large enough to be addressed by the enterprise. Similarly, correlated risks across organizations can be combined and placed on the enterprise risk map to identify risks that could be worrisome at the organization level.

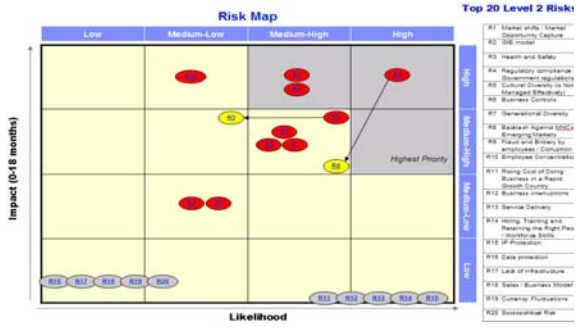


Figure 4. ERM Risk Assessment Workbench: Risk Map showing the tradeoffs between likelihood of risk and impact of risk on a qualitative scale.

D. *ERM Risk Analysis Workbench*

ERM Risk Analysis Workbench provides support for both qualitative and financial investment analyses. Qualitative analyses include root cause analysis, risk mitigation portfolio rationalization, and risk ownership rationalization, which are provided via various views of the ERM environment and the many-to-many relationships amongst the various risk elements. On the other hand, financial analyses include cost-benefit analysis for various risk mitigation solutions and risk mitigation portfolio optimization taking the many-to-many associations between risks and root causes and root causes and risk mitigation solutions. This risk analysis workbench is explained in detail in the next section.

E. *ERM Risk Mitigation Workbench*

ERM Risk Mitigation Workbench captures the final decision about the risk mitigation solutions, risk ownership, KRIs, KPIs, etc. that can then be used to configure downstream risk monitoring and management applications using vendor tools such as IBM OpenPages [7], SAP Risk Management [8] , Oracle Risk Management [9] etc.

This section gave the readers an overview of the various components of our enterprise risk management tool. In the next section we provide details on one specific workbench i.e. ERM Risk Analysis Workbench.

IV. ERM Risk Analysis Workbench: Qualitative Risk Analyses

Often multiple business units in an enterprise are responsible for achieving specific business objectives. We envision our Risk Analysis Workbench as a tool that unifies the perspectives for multiple business units by linking the risk analysis with the larger enterprise context. Below we describe the qualitative and quantitative analytical capabilities of our ERM Risk Analysis Workbench.

The qualitative analysis perspective of ERM Risk Analysis Workbench aims to answer the following questions.

- What are the risks to a given set of business objectives?
- Which key performance indicators (KPIs) will get impacted as a result of a given set of risks?
- Which organization owns the given set of risks?
- Which business processes face what risks?
- Which business processes a given set of risks impact?
- Which risk mitigation solutions are most applicable (based on best-practices) for a given set of risks?
- Which KRIs measure a given set of risks?

To facilitate answering these questions, the tool offers 'views' of the following models of an enterprise: (1) A business process view based on a business process model of an enterprise, (2) an organizational view that represents the organizational structure that strives to achieve specific business objectives, (3) A hierarchy of risks (4) A hierarchy of root causal factors (5) A hierarchy of risk metrics (6) A hierarchy of risk mitigation solutions. When all these views are put together, their inter-relationships can be viewed visually and qualitatively in the tool. Keeping track of so much information at once could be overwhelming to decision makers and so we provide multiple perspectives, such as Risk Analysis, Organizational Analysis, Root Cause Analysis and Risk Mitigation Analysis etc. Each of these perspectives enables decision makers to ask specific questions and get insights to those questions. Below we describe each of these perspectives in detail. Throughout the discussion in the remainder of this section, we will illustrate the analyses using our Risk Analysis Workbench tool. To orient the user to the tool layout we first describe the tool briefly. Due to space limitations, we will not be able to show the visuals of the tool for all perspectives. We will illustrate the key concepts here and explain the mechanism for each of the analyses below.

Figure 6 shows the layout of our ERM Risk Analysis Workbench. It has two main parts: (1) A map area on the top that orients a decision maker and gives a big-picture context of which risks the decision maker is analyzing and (2) a view area on the bottom which consists of various views that pertain to the specific kind of analysis that the user is performing.. This map area organizes risks that an organization faces into columns based on a taxonomy while the rows represent the scope of applicability of a given a risk i.e. whether the risk is applicable at enterprise level, or at individual business unit level, or applicable across a specific business area. This organizational context drives the rest of the analyses. In the bottom view area, sample views include: business objectives, organizations, risks, root causes, key risk indicators, existing risk controls, potential risk mitigation projects, etc. Each view is presented in a subsection with associated data presented in a hierarchical tree structure. The tree views can be expanded and collapsed as needed. Relationships among various view elements are represented as a 'daisy chain' i.e. a semantic network that shows relationships like 'a' is related to 'b' and 'b' is related to 'c', therefore you can derive the relationship between 'a' and 'c' etc. These qualitative relationships are often useful to quickly assess the breadth of impact of a decision. For example, if an organization would like to mitigate a specific risk, the daisy-chain analysis enables a decision maker to reason about which risk mitigation solutions might apply, which business objectives they might in turn help achieve, which root causes do they address etc. by traversing the semantic network. Of course, the initial relationships are fed into the tool but the tool brings together multiple pair-wise relationships together into a larger context by linking them in an n-ary relationship perspective.

A. Risk Analysis Perspective

Some risks affect multiple organizations, and multiple business objectives while the impact of other risks is local and isolated. The purpose of risk analysis perspective in the Risk Analysis Workbench is to aid decision makers in identifying the scope of each risk via visual qualitative analysis. As shown in the figure below, the purple-colored highlighting shows the impacted elements. The risk analysis perspective, can help decision makers reason about the following relationships in order to understand the scope of risk impact:.

- Which business objectives does a risk impact?
- How to measure a risk? i.e., which risk metrics apply?
- What causal factors drive this risk?
- Which organization is responsible for this risk?
- What is the risk exposure from this risk, both financial and non-financial.

B. Root Cause Analysis Perspective

Using the Root Cause Analysis perspective, decision makers can get qualitative answers to questions such as: Which risks does this root cause impact? Which controls/risk response programs are in place to address the root cause? What is their effectiveness of these solutions on a qualitative scale? This is done by visualizing the explicitly stated as well as the inferred relationships among various 'views'.

C. Risk Mitigation Analysis Perspective

For example, in the risk mitigation perspective, decision makers can query the root causes that the selected risk mitigation action can address. If any qualitative information is available about the effectiveness of the chosen risk mitigation program in addressing the specific root causes in the past, that information can be visualized as well. Decision makers would appreciate knowing this information as they may not want to support implementation of risk mitigation programs that were proven to be ineffective in addressing specific root causes. The tool enables saving and visualizing such organizational knowledge. If the tool is connected to real-time monitoring tools, then this information can be kept updated.

D. Organization Perspective

In the organization perspective, decision makers can probe into the following:

- What are the risks this organization is exposed to?
- Which business processes are the responsibility of the organization and which risks are related to these business processes?
- What controls/risk response programs is this organization currently implementing?
- What is the effectiveness of the existing controls/risk response programs?

Once the quantitative analysis is done, decision makers would like to know the amount of risk exposure from each risk to an organization and the potential risk reduction that might occur as a result of implementing specific risk mitigation programs. We offer the quantitative analyses perspective in the ERM Risk Analysis Workbench to enable users to conduct what-if scenarios to obtain answers to such questions. Next section introduces quantitative analyses that are supported in the tool.

V. QUANTITATIVE RISK ANALYSIS

Before we begin, we define the following terms that we use in our quantitative risk analysis approach.

- **Inherent Risk**: The amount of risk (impact and likelihood of occurrence) before any risk mitigation action is taken. This can be estimated prior to any discussion on risk response actions
  - Expected Gross Risk = Pre-mitigation probability of occurrence of risk event X impact of risk event
- **Acceptable Risk**: The impact and likelihood of Occurrence of risk that is acceptable to the organization based on its risk appetite. This can be estimated prior to any discussion on risk response actions. It can also be updated later while designing the risk response.
  - Expected Acceptable Risk = Acceptable probability of occurrence of risk event X Acceptable impact of risk event
- **Initial Estimated Residual Risk:** The amount of risk (impact and likelihood of occurrence) estimated to be remaining after one or risk response solutions are put in place. This is estimated before the risk response solutions are actually implemented.
  - Expected Initial Estimated Residual Risk = Estimated Residual probability of occurrence of the risk event X Estimated Residual impact of the risk event
- **Current Residual Risk**: The amount of risk (impact and likelihood of occurrence) remaining after a set of specific risk mitigation actions are put in place to address specific root causes of risk. This is point-in-time data.
  - Expected Current Residual Risk = Residual probability of occurrence of risk event X Residual impact of risk event

The quantitative analysis tool offers the following analyses

A. Risk Metric Heatmap Analysis

The main insight offered by this analysis is which risks (as measured by risk metrics) are worse than tolerable range? To do this a company's 'as-is' values of risk metrics are compared to the desired value ranges and the results are shown as a 'heatmap' on the RiskTypeMap described in figure 6. Risk components in the Risk Map will be colored as follows:

- Red: if the as-is value (AS_IS_VALUE) of at least one of the risk metrics associated with the chosen risk is above its corresponding minimum desired target-value (MIN TO_BE_VALUE).
- Yellow: If the as-is value (AS_IS_VALUE) of at least one of the risk metrics associated with the chosen risk is between its corresponding minimum (MIN TO_BE_VALUE) and target desired-value (TO_BE_VALUE).
- Green: If **ALL** the as-is values (AS_IS_VALUE) for all the risk metrics associated with the chosen risk are equal to or below their corresponding target desired values (TO_BE_VALUE).

This heatmap analysis is conducted once before risk mitigation programs are implemented and is repeated as often as needed after the implementation of the chosen risk mitigation programs. As noted at the beginning of this subsection, the purpose of these heatmaps is to enable decision makers to asses which risks are in tolerable ranges and how things have changed after implementing the risk mitigation programs.

B. Risk Exposure Estimation

The purpose of risk exposure estimation is to compute the overall inherent risk exposure for a given set of risks. Say 'Fraud & Bribery', 'Business disruptions due to natural hazards', 'Employee turnover' are the 3 risks identified for an area: what is the overall risk exposure of these three risks together. We assume that *independence* holds in estimating the risk. We understand that in real-world risks can potentially influence one another significantly. Decision-makers are made aware of this '*independence*' assumption We formulate the problem as follows:

Given:

- 'n' number of risks.
- For each risk:
  - Likelihood of occurrence (on a scale of 0-1)
  - Impact (in given currency and valid for a time period)

Compute:

- The '***overall risk exposure***' for a given set of risks.

We use the following algorithm to compute the individual risk exposure as follows:

Expected Inherent Risk = probability of occurrence of the risk event X impact of the risk event

To compute the overall inherent risk exposure for a chosen set of risks, we simply sum up the individual 'expected inherent risk' values.

$$\sum_{r=i}^{r=n} IR$$

Where IR represents 'Inherent Risk'. The formula indicates that IR needs to be computed by summing the individual 'IR's of risks 1..n.

C. *Residual Risk Estimation*

In residual risk estimation, our goal is to compute the amount of residual risk after implementing specific risk mitigation programs. We formulate the problem as follows.

Given:

- 'n' risks, 'm' rootcauses, 'k' risk response solutions
- A network of many-to-many relationships between risks, rootcauses and the associated risk response solutions (e.g. each risk can have multiple rootcauses, each rootcause can be the driver for multiple risks, each rootcause could have multiple risk response solutions and each risk response solution can address multiple root causes)
- For each risk:
  - Likelihood of occurrence (on a scale of 0-1)
  - Impact of risk event occurence (in given currency)
- Risk Reduction that can be attributed to each risk response solution based on risk/ root-cause/risk mitigation relationship
  - Eg: Likelihood of occurrence of risk (0-1), Impact of risk (in USD $) in a given time period (start time and end time) after this risk response plan is put in place
  - Effectiveness of risk response program (in % terms) (assumption: applies equally across all risks affected by risk response program.)

Compute

- For each of the 'k' risk response solutions, show the total amount of risk reduction contribued by this risk response solution across all selected 'n' risks that it influences.
- For each of the 'n' risks, show the maximal (upper bound) and minimal (lower bound) amount of risk reduction expected as a result of all of the 'k' chosen risk response solutions. Assumption: 'k' risk response solutions are working independently of one another.

We use the following simple algorithm to compute the residual risk:

The risk reduction due to a specific risk control is computed as the difference between the inherent risk impact value and the residual risk impact value that have been derived as discussed above. Upper bound of risk reduction is obtained by summing up these differences. Literature exists on using regression based approaches to discover the correlations among risks [10] and to use that to estimate the positive or negative influences risk controls might have in reducing the risk [6].

D. *Return on investment (ROI) of Risk Mitigation Projects*

In Return on Investment analysis, various risk mitigation projects are ranked based on the amount of risk reduction they offer per unit of investment made. The total risk reduction is a function of:

- risk reduction estimated for a given risk when the risk control is deployed
- number of risks impacted by the risk control

It is calculated as follows.

Rdi,j = Risk reduction amount for Risk i from Risk Control j

Rdi,j = Expected Value of Inherent Risk i – Expected Value of Residual Risk i due to Risk control j for all combinations of i and j.

TRdj = Total risk reduction associated with Risk control j

TRdj = Sum of Rdi,j over all risks $i = 1 \ldots N$

ROIj (percent) = (Sum (TRdj) – Cost j) * 100 / Cost j %

E. *Identifying the Optimal Risk Control Portfolio given a Budget constraint*

This analysis helps identify an optimal set of risk controls that produces the maximum overall risk reduction given the additional constraint of managing it within a given budget. In our heuristic approach we compare the cumulative cost of investing in Risk Control projects against the budget and show how much budget balance remains after each Risk Control project. It is computed as follows.

Given

- TB: Total Investment Budget for risk mitigation projects

Algorithm:

- BBj = Budget Balance after implementing Risk Control project j in the sorted list.
- BB0 = TB i.e. the Budget Balance before implementing the first risk control equals the Total Budget.
- BBj = BB(j-1) - Cost$j$
- Stop when BBj < 0. The preceding (j-1) projects can provide the largest risk reduction within the budget constraints.

F. *Calculating Inherent Risk and Residual Risk given a Range of Values*

In many instances, it is difficult for the decision makers to estimate the actual amount of risk in monetary terms. Therefore, we facilitate data collection using a semi-quantitative scale consisting of low, medium, high values and and associated numeric risk likelihood and impact value ranges obtained by interviewing multiple experts and executives. If, on the other hand, the user provides only a single value as the most likely monetary value then we will use this value in our computations.

This sums up the high-level description of the qualitative and quantitative analyses supported by our ERM Risk Analysis Workbench.

VI. DISCUSSION

We ran a pilot of our ERM knowledge management tool and the Risk Analysis Workbench in a large multi national company that specializes in semiconductors and information technology (IT) domain. The results of our

pilot are encouraging. Multiple business units working with the enterprise-level ERM coordinator started out by identifying the roles and responsibilities of the various groups. The business units provided the business managers who were responsible for assessing the risks in their business environment that could prevent achieving the business objectives for their respective business units. Using the ERM Risk Assessment Workbench, they modeled their business units ERM environment including identified risks, the risk assessment, root causes, KRIs, and risk mitigation solutions in place if any. During this exercise, the different business units compared notes with each another to identify risks that were common across several business units and brought the common risks to a common community area. They collaborated with each other in identifying the root causes, risk measurement metrics, and risk controls that apply to the identified risk. If certain root causes were specific to a particular business unit, they were moved to the business unit specific community areas by still linking them with the risks in the common community area. The process enabled a constructive discussion and notes sharing on the topics of which risk mitigation programs were successful in each business unit and why and the lessons learned. They were captured as annotations on risk mitigation elements in the knowledge management tool.

Once the data was captured in the knowledge management tool, the ERM Risk Analysis Workbench was used to qualitatively analyze the relationships along with quantitative assessment of the risk exposure and the effectiveness of the risk mitigation programs within each business unit. Even during this process, different business unit's shared notes through the collaborative platform.

As shown in Figure 5, the business-unit specific ERM models were provided on a quarterly schedule to the enterprise-level coordinator / ERM analyst. Using the ERM Workbench, the ERM analyst could then automatically collate all the information provided by individual business units to generate three types of charts: (1) charts providing information on the implementation status of the current risk mitigation programs deployed by various business units, (2) business-unit specific risk maps drawn to the enterprise-level risk scale to identify any risks large enough to be of concern to the enterprise, and (3) risk specific charts to show which risks were common to multiple business units, the associated risk mitigation solutions employed by these business units along with their effectiveness. These third set of charts allowed the ERM analyst to identify early any risks that might be emerging across several parts of the enterprise and also help identify opportunities for those business units struggling with mitigating these common risks to learn from other successful implementors.

At the end of this exercise each business unit found our risk knowledge management tool to be very useful in defining, and managing risks and in collaborating with global organizations for coordination and sharing lessons learned. Overall, the tool and the process enabled a global, enterprise-level risk management perspective rather than a silo-based business unit level risk management.

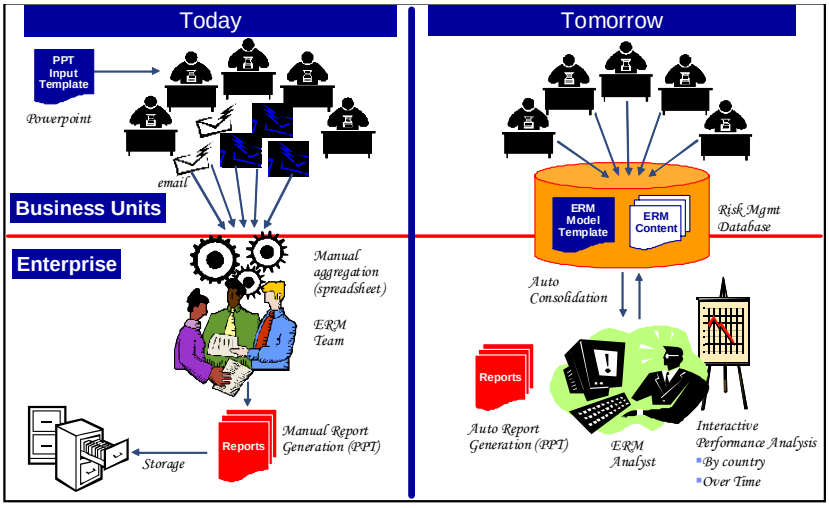


Figure 5. Enterprise Risk Management: Today and Tomorrow

REFERENCES

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

[2] International Standard ISO 31000, "Risk Management – Principle and Guidelines", www.iso.org, November 15, 2009.

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

[4] Gregory L. White, "A Mismanaged Palladium Stockpile Was Catalyst for Ford's Write-Off", The Wall Street Journal, February 6, 2002.

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

[6] 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.

[7] IBM OpenPages Governance, Risk and Compliance http://www-01.ibm.com/software/analytics/openpages/

[8] SAP Businessobjects Governance, Risk, and Compliance Solutions http://www.sap.com/solutions/sapbusinessobjects/large/governance-risk-compliance/index.epx

[9] Oracle Fusion Governance Risk and Compliance http://www.oracle.com/us/solutions/corporate-governance/index.html

[10] N. Abe, R. Akkiraju, S. Buckley, M. Ettl, P. Huang, D. Subramanian, F. Tipu, "On optimizing the selection of business transformation projects" IBM Systems Journal, Vol 46, No 4, July 2007.

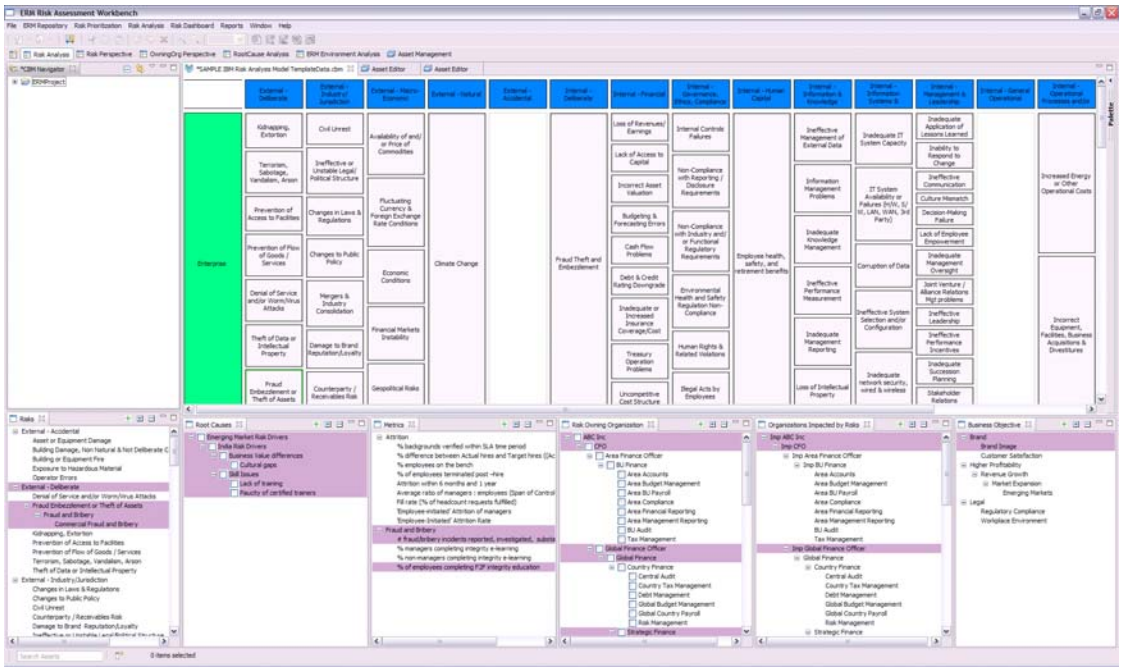


Figure 5. Risk Analysis Workbench: Qualitative Perspective showing daisy-chain analysis

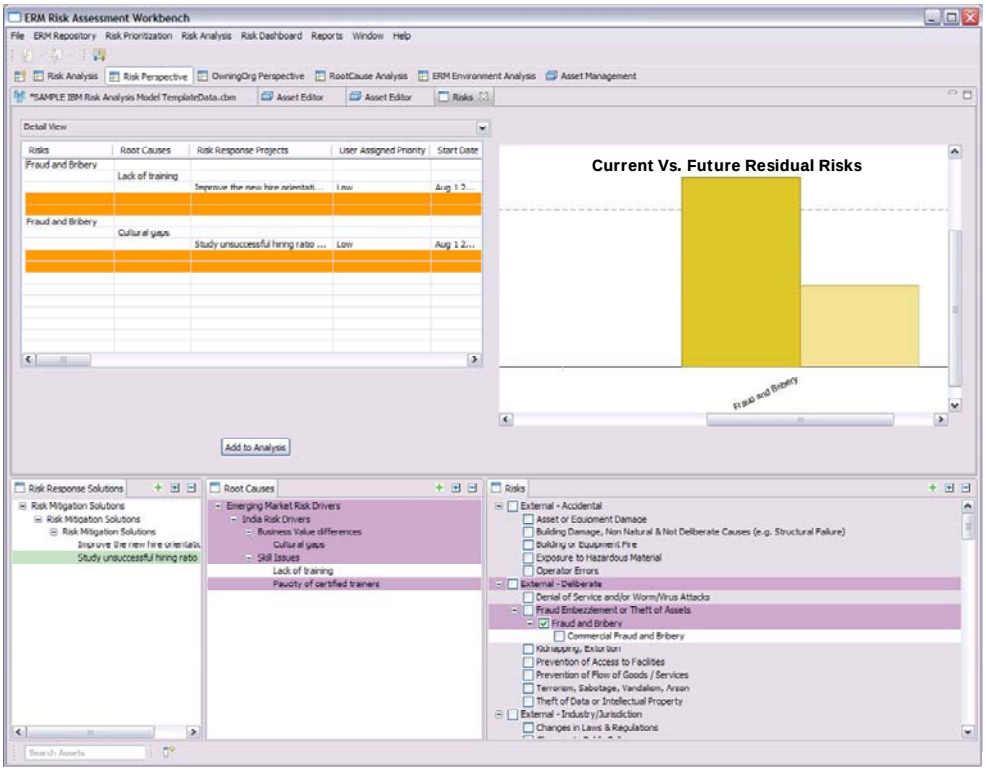


Figure 6. Risk Analysis Workbench: Quantitative Analysis: Residual risk calculation