Optimization of the Enterprise Risk Portfolio

By Eivind Helland and Kjell Garatun-Tjeldstø

Presented at the:
2013 Enterprise Risk Management Symposium
April 22-24, 2013

Optimization of the Enterprise Risk Portfolio

Eivind Helland and Kjell Garatun-Tjeldstø*

Abstract

We demonstrate an integrated enterprise risk management (ERM) solution to optimize the risk portfolio, identify natural hedges, create an optimal risk treatment plan, enhance risk culture, and facilitate risk reporting throughout the organization. A successful ERM program can be advantageous to all stakeholders by improving and protecting earnings by reducing earnings volatility, enhancing employees' and customers' health and safety, and preventing environmental damage. The case study focuses on risk in the offshore industry with estimations of the enterprise-wide risk exposure by the use of the Total Enterprise Risk Manager (TERM) software solution.

1. Introduction

Enterprise risk management (ERM) is a holistic risk management approach to risk associated with running a business. All uncertainties impacting a company's earnings either positively or negatively should be accounted for. According to the Casualty Actuarial Society (CAS), ERM is defined as "The process by which organizations in all industries assess, control, exploit, finance and monitor risks from all sources for the purpose of increasing the organization's short and long term value to its stakeholders" (ERM Committee 2003). Shareholders prefer stable earnings and predictability, which is a sign of good management and a healthy enterprise strategy.

Efficient ERM benefits companies with strategic competitive advantages by providing deeper insights into their businesses and thereby making better decisions for all stakeholders. In response to the emergence of new risks and marketplace needs and conditions, the credit rating agency Standard & Poor's has extended its rating process to embrace ERM as it applies to nonfinancial companies. The values of a positive ERM score directly impacts on the cost of capital and indirectly, but powerfully, on a firm's risk resilience reputation. New standards (ISO 31000, COSO ERM Framework, AS/NZS 4360),

* Eivind Helland and Kjell Garatun-Tjeldstø are respectively Managing and Technical Director at SWISSNOR GmbH, Allmendstrasse 45, 5400 Baden, Switzerland, eivind.helland@swissnor.com.

laws, and regulations have also led to a steep demand for ERM solutions and to a need for implementation of ERM systems within corporations. All private companies and public organizations need to have a forward-looking framework that encourages a culture of performance and enhanced risk awareness. Senior management and boards of directors must be engaged in the establishment of risk management policies and processes, which allow them to gain an overview of the Earnings at Risk (EaR) caused by different risk exposures, and define their risk appetite.

The organizations IRM, AIRMIC, and Alarm have published a guide (2010) that provides a structured approach to ERM and the requirements of the international risk management standard, ISO 31000. A thorough description and inspiration of a value-based ERM framework and methodology can be found in the work of Segal (2011). In this paper we demonstrate how to implement an integrated risk management solution in order to optimize the enterprise risk portfolio, identify natural hedges, create an optimal risk treatment plan, and facilitate risk reporting throughout the organization. It provides the necessary key risk measures and indicators to the C-suite [CEO, CFO, CRO, COO] and to different levels of management in the company.

2. Methodology

2.1. Enterprise Risk Management Process

Enterprise risk management can be defined as an approach to managing all key business risks and opportunities with the intent of maximizing shareholder value. The ERM universe can be considered as three-dimensional, defined by risk category, company scope, and risk assessment and treatment. The process owner should be the Chief Risk Officer (CRO) with risk methodology skills and broad experience in various business functions such as manufacturing, operations, sales, and finance, which enables the CRO to fully understand the business and the process flow within the company. An overview of the process is depicted in Figure 1.

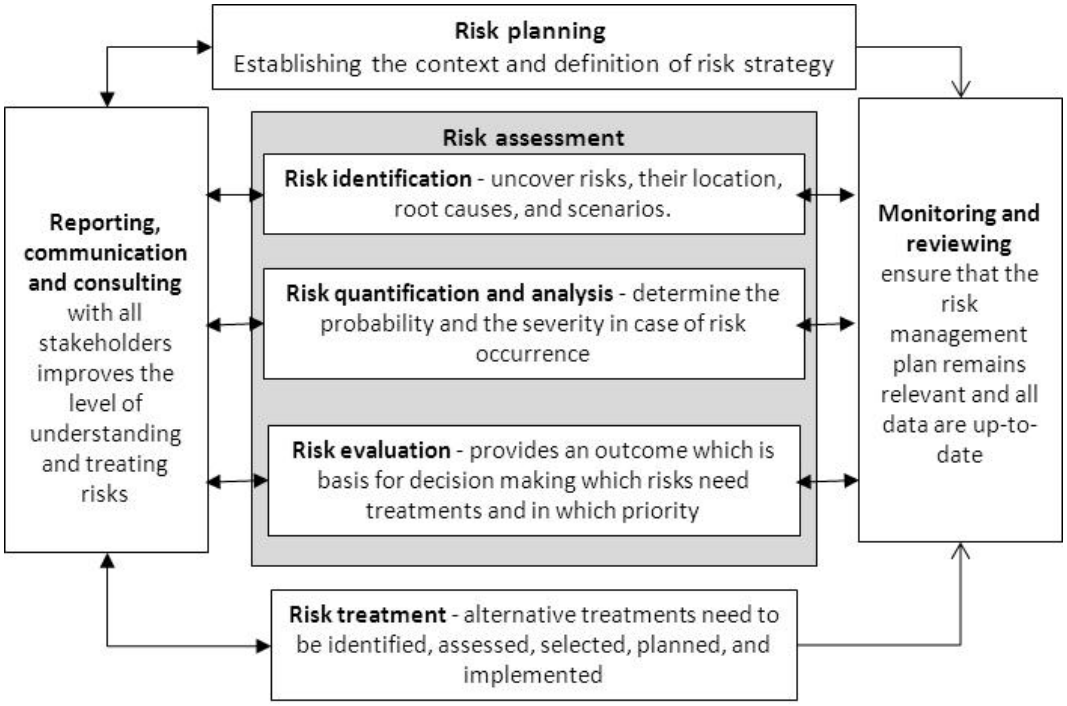

Figure 1: Enterprise Risk Management Process

2.2. Risk Planning

Risk management plans must include the details of the major process steps, including an implementation plan and the outline of the risk governance structure. The risk management plan defines the risk management tools, project team roles, and responsibilities and outlines the timing and frequency of facilitated risk management workshops and reporting requirements.

2.2.1. Risk Category

The ERM program should cover all risk categories and exposures that can influence the value of a company, including hazard, financial, operational, and strategic risks. Any given risk exposure can be either a speculative or a hazard risk. Speculative risk is a situation in which either profit, loss, or no loss is possible (e.g., stock investment). The decision to venture into a new market, purchase new equipment, diversify the existing product line, expand or contract areas of operations, commit more to advertising, borrow additional capital, etc., carries risks inherent to the business with a positive or negative outcome. Hazard risk occurs from an accidental loss and includes only the possibility of loss and no loss. ERM

considers all types of risk an organization faces. The following four main classes can be defined (ERM Committee 2003):

- *Hazard risk:* Business interruption exposure; Criminal exposure; Environmental liability exposure; General liability exposure; Health and safety exposure; Machinery and boiler exposure; Natural disaster exposure; Product liability exposure; Property exposure.
- *Financial risk*: Financial exposure; Credit exposure.
- *Operational risk:* Fleet operation and marine exposure; IT and Electronic exposure; Personnel and human capital exposure; Production, technological, and R&D exposure; Project risk exposure; Supply chain exposure.
- *Strategic risk*: Compliance, regulatory and legal exposure; Corporate governance and ethics exposure; Intellectual property exposure; Marketing and product management exposure; Reputational and brand exposure; Social, economic, and political exposure.

2.2.2. Company Level

The company level at which the risk is assessed, owned, and treated can be enterprise-wide, location based, country based, based on a predefined geographical zone, based on a business unit, or based on a project.

2.3. Risk Identification

Risk identification involves determining the risk scenarios that represent potential threats and opportunities to the company. Risk scenario analysis is an essential tool for ERM to identify, analyze, and prioritize the risks for the company (Segal 2011). Scenario analysis is a process of analyzing possible future events by considering alternative possible outcomes. This may take form as brain storming, and the judgment of field experts represents an extremely valuable contribution. The identification of risk scenarios can be carried out by using a variety of tools, such as the following:

- Risk assessment questionnaires for hazard and operational risks
- Historical incident data for hazards risks
- Financial statements and accounting records for the identification of financial risks

- Flow charts and organizational charts for operational risks
- Personal interviews with experts from different departments for all risk classes
- Risk workshops with upper management and board members for identification of strategic risks
- Techniques applied for identification of hazard risks (Bahr 1997):
    - Hazard review—a mainly intuitive, qualitative review of the installation to identify the hazards that are present
    - Hazard check list—a review of the installation against a list of hazards that have been identified in previous hazard assessments
    - Hazard and operability study (HAZOP)—a systematic review of the process plant design, to evaluate the effects of deviations from normal operating conditions
    - What-If Analysis—a flexible review technique, which can be applied to any installation, operation, or process, to identify hazards
    - SWIFT—the Structured What-If Checklist technique combines the relatively unstructured What-If technique with the more organized and thorough aspects of the HAZOP technique
    - HAZID—a systematic review of the possible causes and consequences of hazardous events
    - Failure modes, effects, and criticality analysis (FMECA)—a systematic review of a mechanical system, to evaluate the effects of failures of individual components
    - Emergency Systems Survivability Analysis—a systematic review of the ability of emergency systems to withstand accident conditions
    - Safety inspections and audits—visual examinations of an existing installation and its operating procedures to identify potential safety hazards.

2.4. Risk Quantification and Analysis

2.4.1. Risk Matrix and Risk Level Definitions

A risk matrix with definitions of probability (annual frequency) and severity must be defined to classify the identified risk scenarios (Fig. 2).

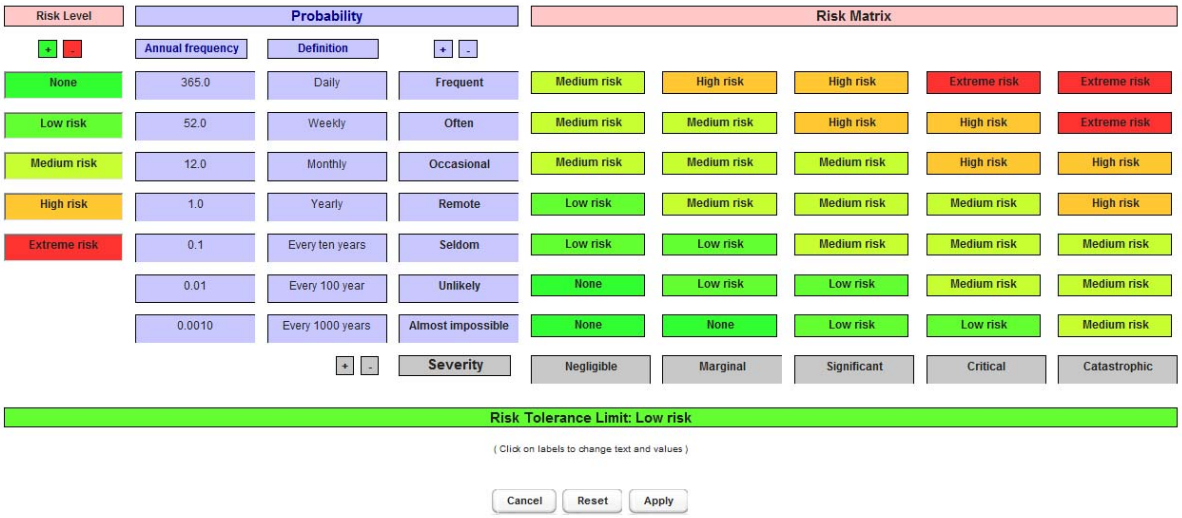

Figure 2: Definition of the Risk Matrix

The severity definitions of the main risk exposures should be set according to company standards (Fig. 3). This should be carried out to clarify the scale and improve the objectivity of the risk scenario analysis. A severity grading based on an annual percentage deviation of earnings, turnover, or impact on the employees' health and safety can be used as a risk measure for each risk category. This permits the use of the same risk measure and a unique matrix when assessing the risk at one specific location, one country, a project, one business unit, or consolidated to the entire company.

Severity definitions

Risk Exposure	Negligible	Marginal	Significant	Critical	Catastrophic
Business interruption and net income exposure	Business interruption less than a day	Business interruption less than a week	Business interruption less than a month	Business interruption less than six months	Total business interruption for 1-2 years
Compliance, regulatory and legal exposure	Minor compliance deficiencies	Some compliance and regulatory deficiencies	Some compliance and regulatory deficiencies.Legal deficiencies.	Major compliance and regulatory deficiencies.Legal deficiencies leading to trials.	Major compliance and regulatory deficiencies.Legal deficiencies leading to trials with a high impact.
Corporate governance and ethics exposure	Smaller corporate governance and ethics risk exposure. Minor financial impact of < 2% total turnover.	Marginal corporate governance and ethics risk exposure. Minor financial impact of < 5% total turnover.	Significant corporate governance and ethics risk exposure. Financial impact of < 25% total turnover.	Critical corporate governance and ethics risk exposure. Major financial impact of 60-80% total turnover.	Catastrophic corporate governance and ethics risk exposure. Financial impact of >80% total turnover.
Credit exposure	Smaller credit loss exposure. Minor financial impact of < 2% total turnover.	Marginal credit loss exposure. Minor financial impact of < 5% total turnover.	Significant credit loss exposure. Financial impact of < 25% total turnover.	Critical credit loss exposure. Major financial impact of 60-80% total turnover.	Catastrophic credit loss exposure. Financial impact of >80% total turnover.

Figure 3: Severity Definitions per Risk Category

Incident and deviation investigations can also be used to develop risk scenarios. Incidents are unexpected events related to maintaining plant operations, safety, security, compliance, or financial incidents. Deviations are measured differences between an observed value and an expected or normal value for a process or product condition or are an anomaly from a documented standard or process. Incident and deviation management includes investigations to determine root causes, immediate corrective actions, and the creation and documentation of the treatment actions necessary to prevent future similar events. An incident or deviation report should be developed to a risk scenario to investigate different potential outcomes (Figs. 4 and 5).

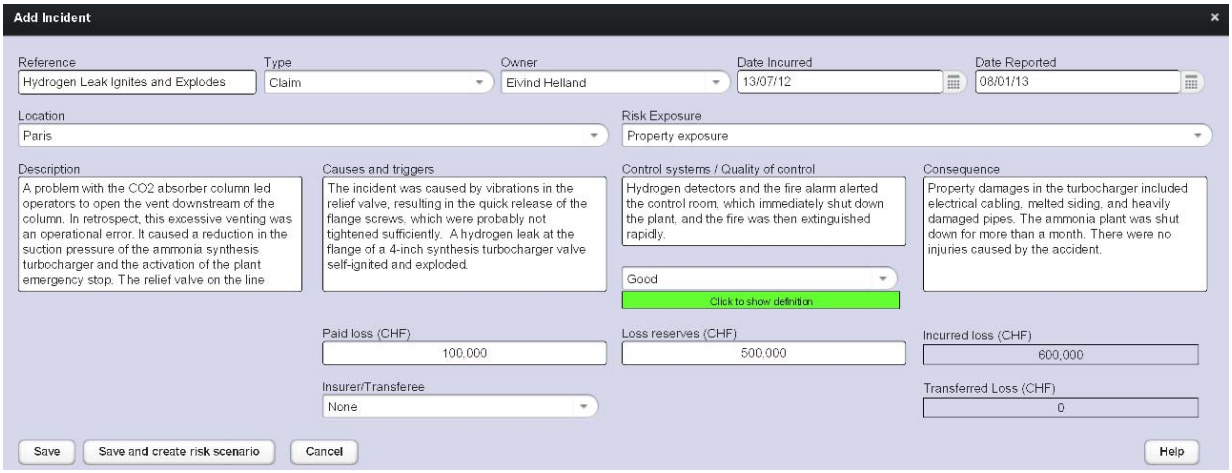

Figure 4: Incident and Deviation Analysis

The expected loss and/or gain can be estimated in several ways. It can be represented by the probability-weighted average of loss and/or gain under all possible scenarios (stochastic) or by the loss and/or gain under the most likely scenario (deterministic). A deterministic approach can be used to choose realistically the most serious scenario (severity and associated frequency) from this family. The risk scenario analysis comprises a thought-provoking process in which experts are asked to find key risks defined by their source (production, human resources, financial department, supply chain, logistics,

trading department, etc.). Since it involves the participation of experts at local business units, the ERM program will also gain a higher level of ownership and acceptance within the organization.

The bottom-up approach can be used to identify risk at the site or project level, which can be pieced together and consolidated to the business unit or company level. It creates a robust risk culture where all parties are involved and feel ownership. The head of risk management (CRO) can consolidate risk scenarios from one location or other subgroups into a larger set of locations and even enterprise-wide if relevant.

The top-down approach starts with the big picture, and a risk scenario is defined at the company level to get insights about the main key risks relevant for the company's performance. This facilitates the risk dialogue of the enterprise-wide risks among the board members. If relevant, the allocation of the cost of risk to the subsystem levels can be defined, until the entire specification is reduced to base elements such as locations or cost centers. Both the bottom-up and top-down approaches should be used simultaneously to connect the risk at different levels and permit critical risk information to be detected in a timely manner. The outcome of the analysis can be presented in a risk map showing the risk level of all individual risks within the company (Fig. 6).

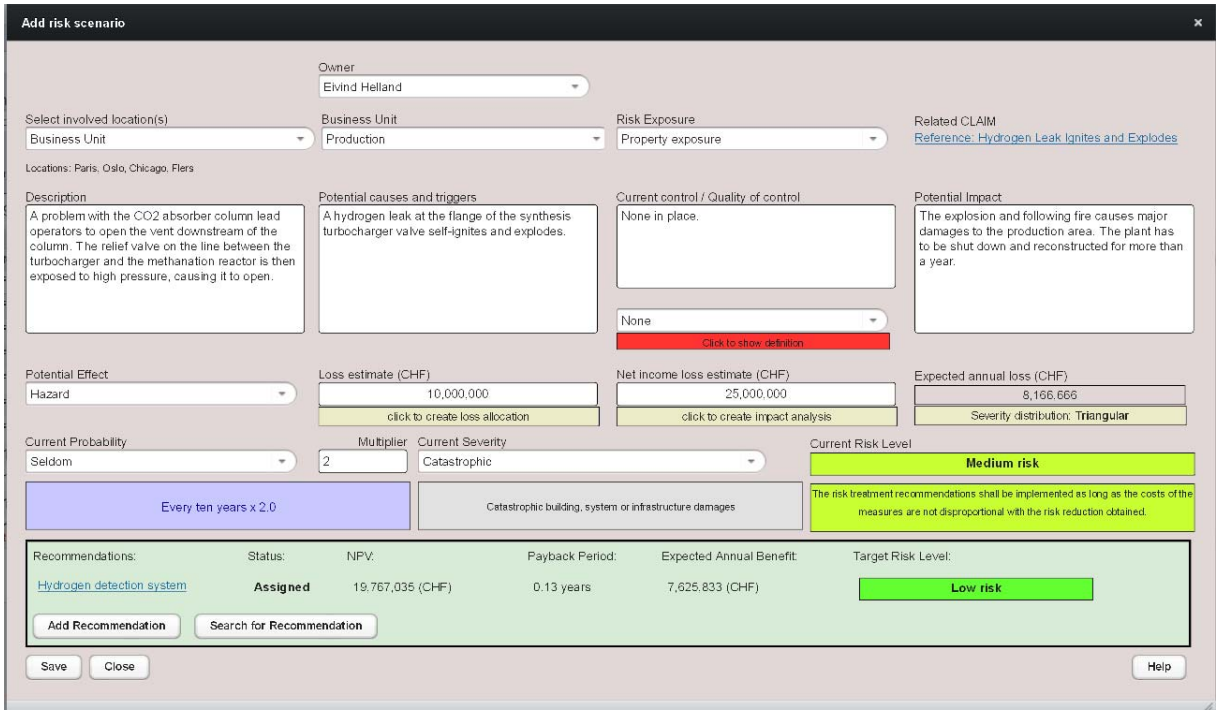

Figure 5: Risk Scenario Analysis

As part of the risk scenario analysis one should undertake a Business Impact Analysis to identify secondary losses, which will certainly occur. Every company needs to identify what the impact to the business would be in the event of a disruption and determine basic recovery requirements. Critical activities may be defined as primary business functions that must continue to support the business. The following should be identified:

- Critical business activities
- The impact on the business in the event of a disruption
- How long could the business could survive without performing this activity.

As part of a Business Impact Analysis one should assign Recovery Time Objectives (RTOs) to each function. The RTO is the time from which you declare a crisis or disaster to the time that the critical business function must be fully operational to avoid serious financial loss.

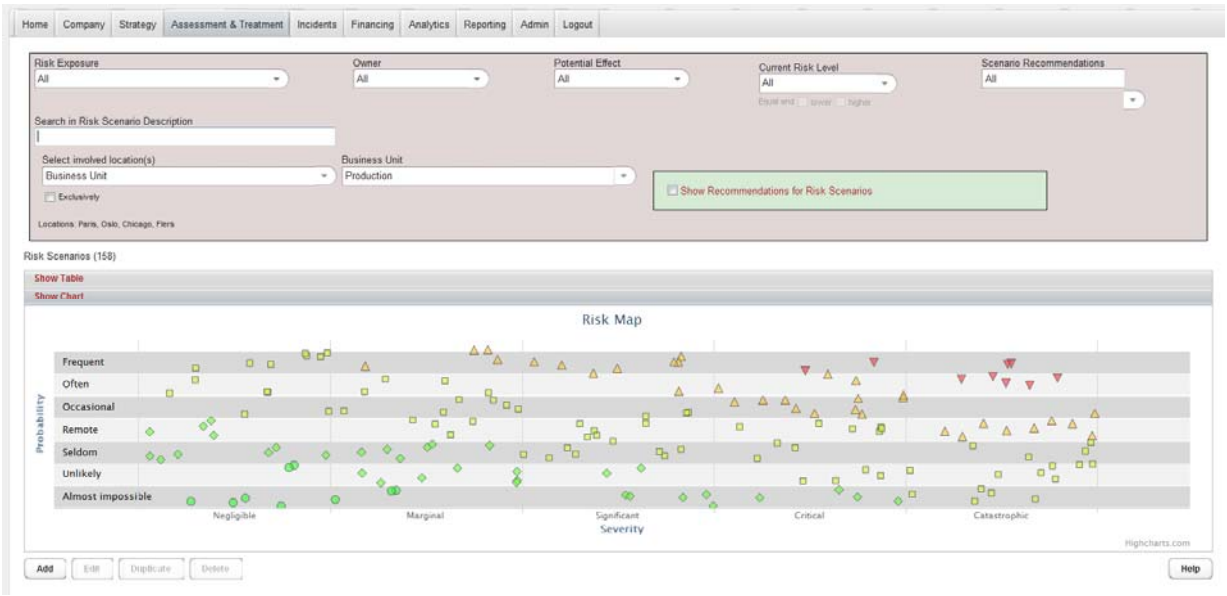

Figure 6: Risk Map

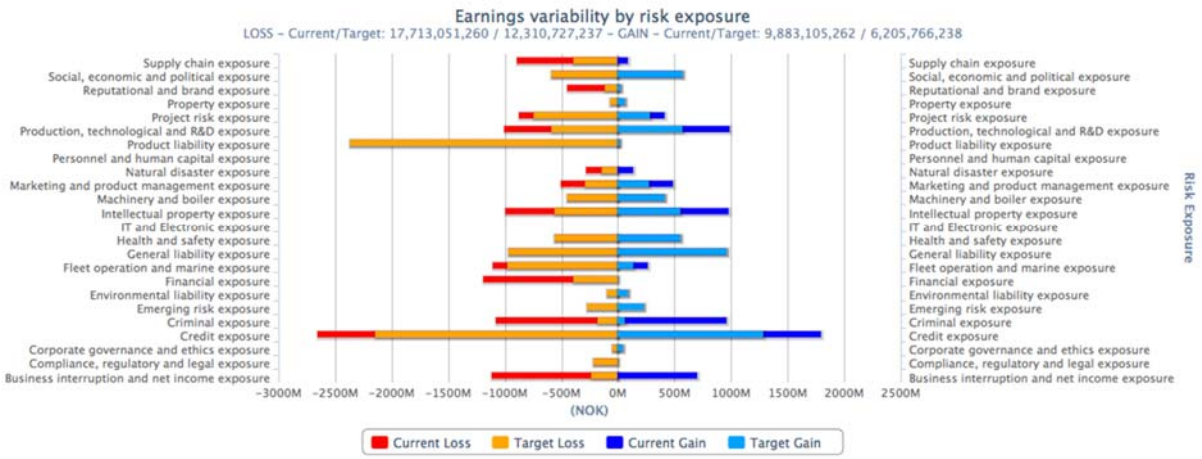

Figure 7: Expected Earnings Variability

The expected annual loss or gain aggregated over each risk exposure, either enterprise-wide, per location, business unit, or project based, is calculated based on the output of all risk scenarios (Fig. 7) in a tornado chart. Tornado charts attempt to capture how much of an impact a risk has on a particular metric such as revenue, net income, or earnings per share. Tornado charts are valuable because executives can see, in one place, the biggest risks in terms of a single performance metric. However, this provides only the expected loss and/or gain and no distributions (Segal 2011; Friggo and Læssøe 2012).

2.4.2. Monte Carlo Simulation of Earnings Variability

A Monte Carlo simulation can be used to model the distribution of the earnings variability over a time period by running multiple simulations. Stochastic processes are used for the occurrence, the size of loss or gain, and the potential outcome (loss, no loss, or gain) of the risk scenarios defined by the domain experts. The number of occurrences of a risk scenario could be modeled with a constant or a Poisson distribution over a time interval. The severity of a risk scenario can readily be described by the normal, lognormal, uniform, triangular, generalized hyperbolic, or discrete customized probability distribution functions. The calibration of the parameters can be done by using own loss history data, external sources, or the results of an event tree analysis. The triangular process is advantageous to use for business

decision and project management modeling where data are scarce since it requires only the minimal, maximal, and likeliest value (Fig. 8).

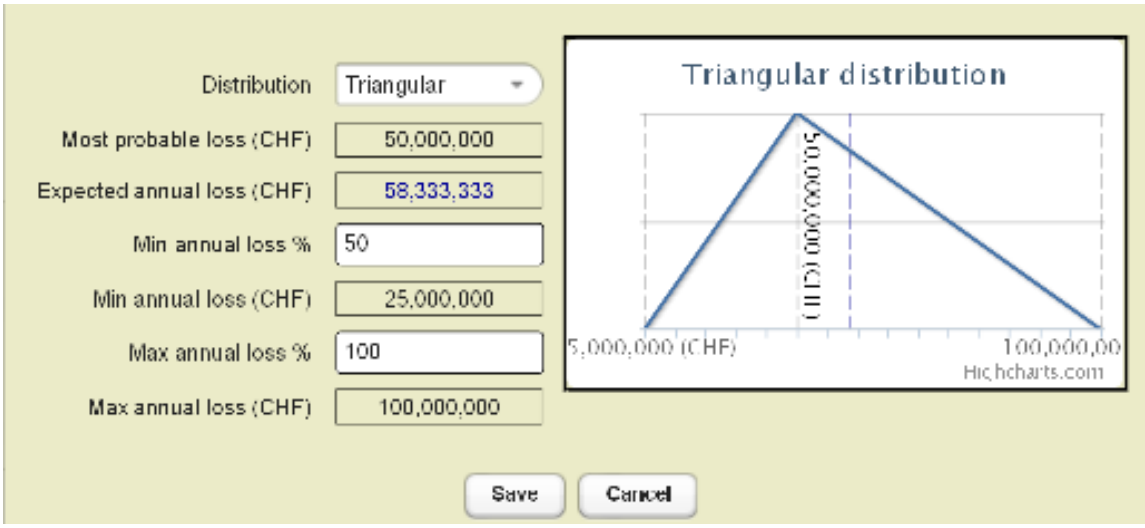

Figure 8: Severity Distribution Functions for the Risk Scenario Analysis

2.4.3. Modeling of Risk Interdependencies

It is crucial to identify catalyst risks, which can have major cross-functional impacts and initiate other risk exposures. Several methods can be used to investigate the risk interdependencies:

- Cross-impact analysis based on Vester's paper computer method to determine active/passive risks and cross-linked/isolated risks (Montagne et al. 2012)
- Interpretive Structural Modeling to construct a structural hierarchy of the risks (Gorvett and Liu 2007)
- Quantitative Monte Carlo simulations with asymmetric correlation coefficients.

The interconnectedness of the different risk scenarios can be evaluated by carrying out the cross-impact analysis based on Vester's paper computer method to determine active/passive risks and cross-linked/isolated risks. We define the interdependencies between risks to be none (0), low (1), medium (2), and high (3). The interdependency matrix shows to which degree each risk element is connected to the others (Table 1). The horizontal line shows how a risk interrelates to the other risks, for example,

that Risk 1 has a high influence on Risk 2. The "Active sum" quantifies the effect of each risk on the others. The vertical column indicates how the individual risk is being influenced by the others, and the "Passive sum" quantifies to which degree it is being influenced.

Table 1

Interdependency Matrix

	Risk 1	Risk 2	Risk 3	Risk 4	Active sum	Q	P
Risk 1		3	2	0	5	2.5	0.46
Risk 2	1		2	3	6	1.0	1.66
Risk 3	1	1		1	3	0.4	0.97
Risk 4	0	2	3		5	1.3	0.92
Passive sum	**2**	**6**	**7**	**4**			

The ratio Q = Active sum/Passive sum indicates the relationship between influencing others and being influenced. If $Q > 1$, it is defined as an active risk, and if less than 1, a passive risk. The product P = Active sum × Passive sum (normalized by the average product) quantifies how the risk is interconnected to other risks. A high P value (> 1) indicates that it is involved in above-average many cause-effect relationships.

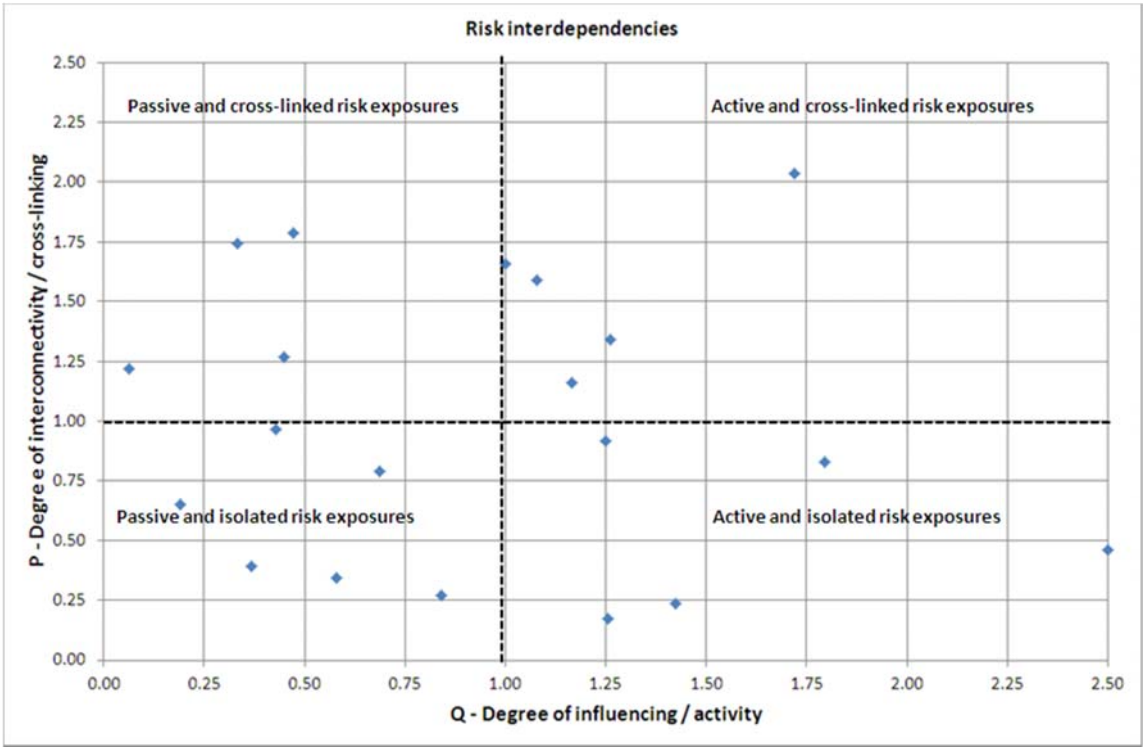

Figure 9: Risk Interconnectivity Map

Each risk can be positioned according to their *P* and *Q* value in a risk interdependency chart. For a first setup, it could help in determining which risks to be investigated in more detail with respect to conditional probability and correlations. Based on the results shown in Figure 9 we can detect the risks with the highest cross-functional impacts. Mitigations on active and cross-linked risks are crucial since there may be feedback loops intensifying the impact. Mitigations on active and isolated risks have a huge impact on a few other risk exposures; thus it is important to investigate them in a targeted way.

Once the most interrelated risk scenarios are defined, the asymmetrical correlations between pairs of individual risk scenarios can be set to model their interdependencies. Many risk scenarios are independent; that is, the correlation coefficient equals zero. However, some risk exposures are dependent and correlated to different degrees. Some exposures leading to an event can trigger other events (positive correlation), leading to a super-additivity condition of the total risk exposure. On the other hand, some exposures leading to an event can exclude other events or decrease its risk level (negative correlation), which would lead to a sub-additivity condition of the total risk exposure and be a natural hedge for the

company. Additionally, some risk exposure dependencies are asymmetrical; earthquakes might lead to fire (when gas lines are ruptured, releasing gas, or power lines brought down, causing arcing and sparks), but not vice versa.

2.5. Risk Evaluation and Decision Making

Risk quantification and analysis provides an outcome that is a basis for deciding which risks need treatments and in which priority. This information is put into the risk matrix, which is a decision-making tool that indicates the level of the company's individual risks. To decide which risk is accepted, tolerated, or must be dealt with, one needs to define a clear risk strategy. This involves the definition and agreement of risk acceptance criteria based on a company's risk capacity, appetite, and tolerance level. The COSO ERM standard defines risk appetite for the organization's overall acceptable level of risk, the degree of risk, on a broad-based level, that a company or other entity is willing to accept in pursuit of its goals, and risk tolerance to describe risk at a lower, more granular level. Ernst & Young defines it as follows (Ernst & Young Global Limited 2010):

- Risk capacity: the amount and type of risk an organization is able to support in pursuit of its business objectives. A company's risk exposure must be lower than its risk capacity.
- Risk appetite: the amount and type of risk an organization is willing to accept in pursuit of its business objectives. This is the limit of the target risk exposure.
- Risk tolerance for specific categories of risk, including strategic, operational, financial, and compliance risks. More operational than risk appetite, risk tolerance expresses the specific maximum risk that an organization is willing to take regarding each relevant risk (sub-) category, often in quantitative terms.
- A risk target is the optimal level of risk that an organization wants to take in pursuit of a specific business goal. Setting the risk target should be based on the desired return, on the risks implicit in trying to achieve those returns, and on a company's capability of managing those risks.

Figure 10: Earnings at Risk

The definition of risk appetite should be done after the enterprise risk exposure is estimated. Commonly used risk measures for risk appetite are company value, capital ratio, net income growth rate, or earnings per share (EPS) growth rate (Segal 2011). The EaR at the corporate level is a result of the Monte Carlo simulations and can be presented as a cumulative distribution of the annual losses or gains (Fig. 10). The unexpected deviation of the expected EaR of NOK (Norwegian kroner) 3.8 billion is less than NOK 3.7 billion (NOK 7.5−3.8 billion) with a probability of 95 percent. The risk appetite could be defined as a NOK 3 billion unexpected decrease of annual earnings or as a 5 percent percentage unexpected drop of the expected earnings of NOK 60 billion. Ideally, a company should expand its exposure to upside risk while reducing the potential for downside risk. While investors appreciate growth in earnings, they also appreciate some level of stability and predictability and are often willing to pay a premium for these attributes.

A risk tolerance limit at a lower level of the organization can be easier to manage for the risk-return balance of the business below the enterprise level (Segal 2011). Risk tolerance limits express a standpoint with regard to risk connected to loss of human lives and to personal injury as well as damage to the environment and to assets and financial interests. Breaching a risk tolerance limit should serve as a red alert for management—the risk position must be reduced. Risk appetite, tolerance, and targets are not static and must be updated with changes in a company's environment (economy, markets,

regulations, technology, etc.), strategy, and performance. The risk strategy should reflect the treatment actions required for different levels of individual risk exposures (Fig. 11).

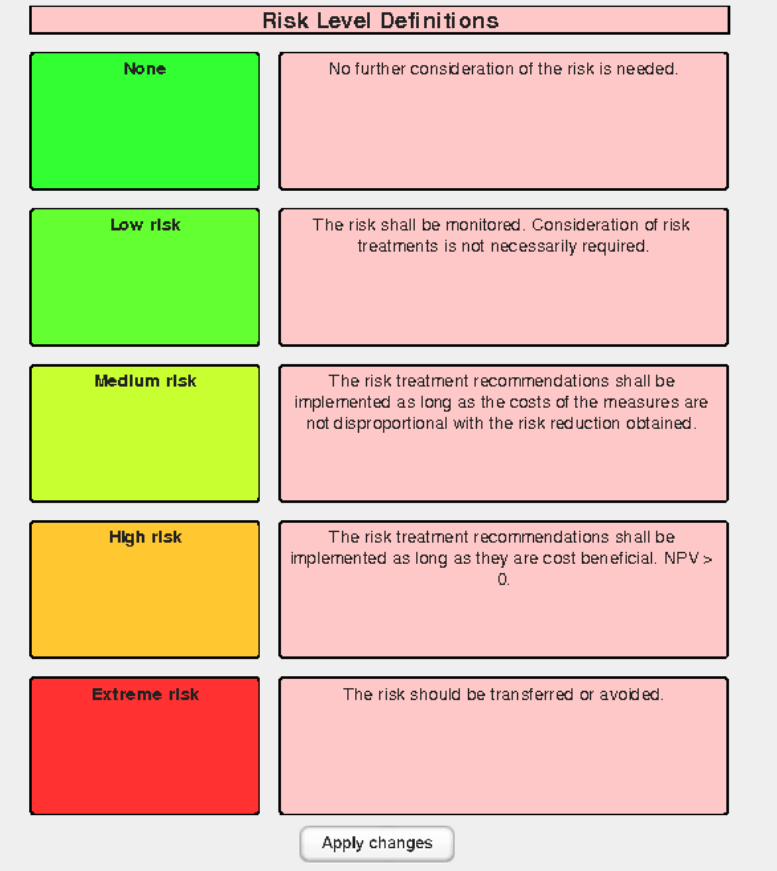

Figure 11: Risk-Level Definition

All risks classified above the company's risk tolerance limit should be treated (Fig. 12). Broadly, there are four potential treatment strategies, with numerous variations:

- Accept risk—Take the chance of negative impact, and eventually budget the cost; for example, self-retention
- Avoid risk— Change plans to circumvent the problem and do not engage in activities presenting the risk
- Control/mitigate risk—Reduce impact or likelihood (or both)

- Transfer risk—Outsource risk to third parties that can manage the outcome. This is done, for example, financially through insurance contracts or hedging transactions, or operationally through outsourcing an activity.

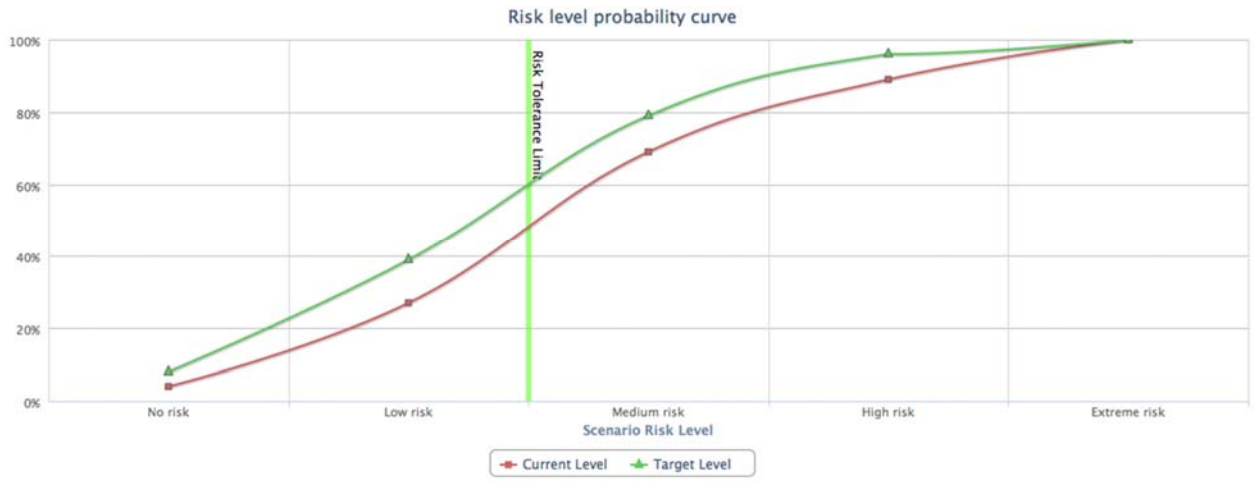

Figure 12: Risk-Level Distribution Curve

Key Risk Indicators (KRIs) for early warning of risk exposures should be defined and monitored. A KRI can be identified by a root-cause analysis to find the leading indicator triggering or initiating a risk event. A company can monitor and manage its most important risk targets and tolerance limits through a set of KRIs, which can be expressed in a variety of units, according to the specific risk under discussion. Examples of KRIs can be the number of calls to customer service related to product liability exposures, lawsuits filed against a company related to general liability exposures, commodity price, exchange rate related to financial exposures, change of number of competitors, or company stock performance in relation to competitors related to marketing exposures (Segal 2011; Beasley et al. 2010). KRIs can initiate action to mitigate developing risks by serving as triggering mechanisms for organizational units charged with monitoring particular KRIs.

2.6. Risk Treatment

Risk treatment actions need to be defined and prioritized and can be grouped into risk controlling (e.g., prevent, reduce, transfer, exploit, avoid, duplicate, separate, or diversify) and risk financing (e.g.,

transfer, retention, or insure). Risk treatment is the term used in ISO 31000 for taking action to modify risk. The recommendations of risk treatment aim to reduce the effect of uncertainty on the company's objectives, which means tackling anything that might lead to detrimental consequences together with whatever is beneficial in such a way that the result is a net benefit. The goal is both a decrease of the expected earnings at loss and a decrease of the distribution or tail risk such as the EaR or conditional earnings at risk (CEaR). To cover all key risk exposures, a company should establish a common risk treatment library that can be used by all business units to optimize the knowledge and human capital within the company.

2.6.1. Risk Financing

Risk financing is concerned with generating funds to pay for losses or offset earning variability experienced by a company. Risk-financing techniques can be categorized into risk transfer (guaranteed cost insurance, insurance derivatives), or funded retention by way of reserves (self-insurance), or hedging designed to minimize known, quantified risk. Hybrid plans are a group of risk-financing techniques involving elements of both retention and transfer (large deductible insurance, retrospective rating, captive insurance, pooling, finite-risk insurance). Alternative risk finance is the use of products and solutions that have grown out of the convergence of the banking and insurance industry. They include captive insurance companies and catastrophic bonds and finite risk products such as loss portfolio transfers and adverse development covers. Risk-financing objectives should be to include paying for losses, maintaining an appropriate level of liquidity, managing the cost of risk, and complying with legal requirements. These objectives should help risk management in selecting the appropriate risk-financing techniques.

2.6.2. Risk Controlling

ISO 31000 gives a list of alternative risk treatment options to be considered and indicates that there is a preferred order in which that consideration should take place, for example, first loss, prevention (decrease of probability), then loss reduction (decrease of severity):

- Avoidance: A risk management technique whereby risk of loss is prevented in its entirety by not engaging in activities presenting the risk.
- Contractual transfer: The use of contractual obligations such as indemnity and exculpatory agreements, waivers of recovery rights, and insurance requirements to pass along to others what would otherwise be one's own risks of loss.
- Duplication: A risk treatment technique that entails the utilization of backups or spares. For example, backup business data should be stored at a location separate from the main place of business.
- Loss prevention: A risk treatment technique seeking to reduce the possibility that a loss will occur.
- Loss reduction: A loss control activity focusing on reducing the severity of losses. Examples include building firewalls to reduce the spread of fire and installing automatic fire sprinklers.
- Separation: A risk treatment technique involving the separation of loss exposure units so that a loss in one unit is unlikely to occur at the same time as a loss in another unit.
- Diversification: A risk control technique that spreads loss exposures over several projects, products, areas, or markets.
- Operational: Application of the risk management process to operational risk (human, process, system, or technological uncertainties).
- Strategic: Methods to treat uncertainty arising from long-term policy decisions.

All risk treatment decisions should be evaluated in the context of ERM risk/return tradeoff analysis (Fig. 13). It should be evaluated if the recommendation increases the risk exposure in another area when implemented.

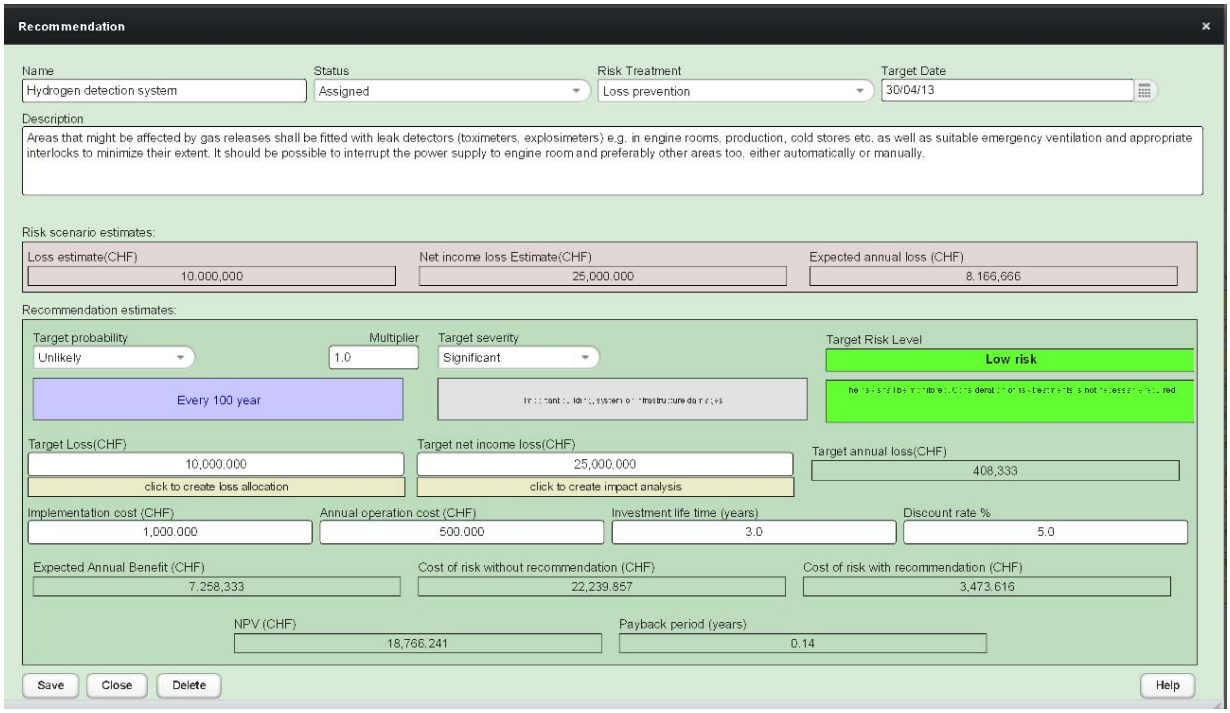

Figure 13: Cost-Benefit Analysis of Risk Treatment Actions

A cost-benefit analysis of each treatment action can be carried out and documented in a Risk Level–Net Present Value chart to prioritize the actions (Fig. 14). The business unit or site level can thus optimize its cost of risk. The chart is typically made up of the expected annual loss and direct and indirect losses arising from risk control and risk-financing activities.

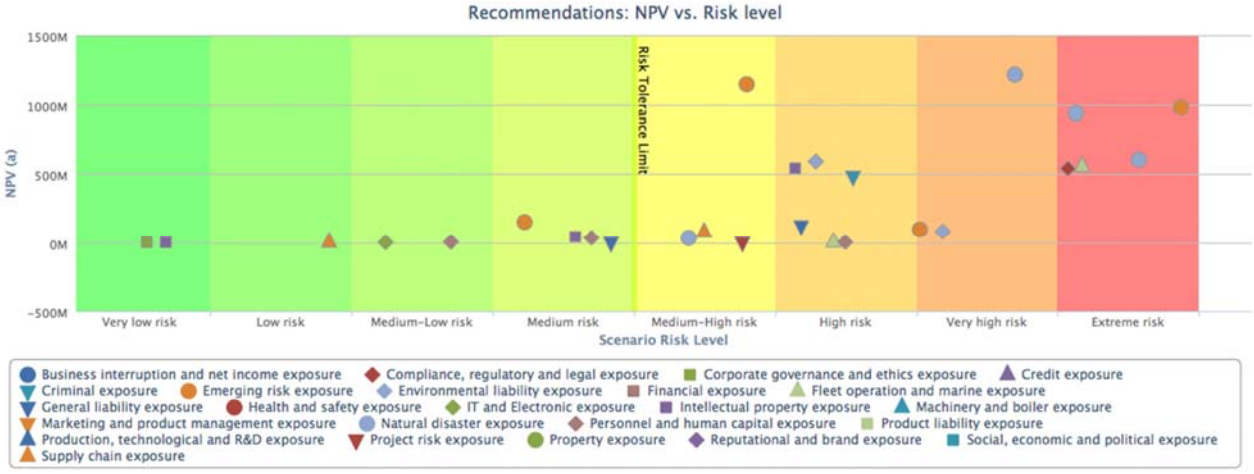

Figure 14: Risk Treatment Actions by Risk Level and Net Present Value

The modeling of interdependency between risk scenarios allows us to map the risk interconnectivity to detect risk exposures, which can act as catalysts or natural hedges. Once identified, risk treatment actions can be defined to decrease the dependencies between correlated key risk exposures, such as use of flexible hoses to reduce the risk of gas explosion due to gas leakage in the case of an earthquake. Further on, risk opportunities can be readily spotted and the risk portfolio optimized by identifying natural hedges. If the commodity price of raw materials increases, the company's margin and direct profit will decrease (negative impact), but it will also hinder new market entrants, which might lead to an increased market share (positive impact).

2.7. Risk Monitoring, Reporting, and Communication

Risk communication is an interactive process of exchange of information and opinion on risk among the executive board, risk assessors, risk managers, and other parties. Risk communication is an integral and ongoing part of the risk analysis exercise, and ideally all stakeholder groups should be involved from the start. The identification of particular interest groups and their representatives should make up a part of an overall risk communication strategy. This strategy should also cover who should communicate information to the public, and the manner in which it will be done.

2.7.1. Periodic Risk Management Report

A risk management report should contribute to sound risk management and decision making by their relevant recipients, including, in particular, the board and senior management. Risk management reports should cover all material risk areas within the organization and monitor changes and improvements such as the following:

- ERM policy statement
- Risk Management Department structure
- Risk assessment procedure

- Definition of risk appetite
- Presentation of prioritized risks for the company locations (country, business unit, project based, per location, etc.)
- EaR per risk class
- Risk treatment activities
- Insurance and risk transfer financing
- Losses and forecasts
- Allocation of cost of risk
- Risk management training topics and priorities
- Communication of risk
- Risk activities and risk priorities for the coming period

2.7.2. Business Continuity Plan

Business continuity and resiliency planning (BCP or BCRP) "identif[y] an organization's exposure to internal and external threats and synthesize hard and soft assets to provide effective prevention and recovery for the organization, while maintaining competitive advantage and value system integrity" (Elliott et al. 1999). A business continuity plan is a roadmap for continuing operations under adverse conditions and a document containing all of the information required to ensure that the business is able to resume critical business activities should a crisis or disaster occur.

The objectives of the plan are to:

- Undertake risk management assessment
- Define and prioritize critical business functions
- Detail an immediate response to a critical incident
- Detail strategies and actions to be taken to enable staying in business
- Review and update the plan on a regular basis.

3. Case Study: ERM in the Offshore Industry

A risk assessment based on the main risk exposures in the offshore industry was carried out. The total enterprise-wide risk exposure can be presented by its EaR by risk category or to give a clear overview of the importance of the different key risk exposures (Fig. 15).

Government regulation is an evolving strategic risk for the industry. Since the Deepwater Horizon oil spill in 2010, the U.S. government has asserted the right to issue drilling moratoriums for its offshore areas. Such moratoriums essentially end all activity in the covered area and supersede prior contracts. Governments around the world have varying levels of regulatory oversight and rules. In some areas, the requirements are minimal, but there is always the risk of more regulation and more expensive operating requirements. An important risk in the offshore drilling industry stems from the fact that it is both a service industry and dependent upon its customers and their budgets, and highly sensitive to commodity prices. If major oil and gas producers foresee lower energy prices, they shorten their drilling budgets. Therefore, some drilling companies pursue multiyear contracts for their services, giving them a guaranteed book of business, but at the cost of locking in a rate that may not be competitive years later.

Most accident sequences and technical failures involve human errors rooted in management decisions. Manmade disasters can cover a lot more ground—anything from minor fires onboard the rig to major accidents that result in the loss of the rig. The main causes of offshore operating losses are fire (including lightening and explosion) and blow-out. The most common consequences are linked to damages to property (e.g., a platform or a mobile rig and pipelines), damages to the environment (e.g., pollution), financial losses due to operation disruption, and loss of human lives or bodily injury. The following risk exposures should be included (Brandsæter 2002):

- Blow-out—uncontrolled release of crude oil and/or natural gas from an oil well or gas well after pressure control systems have failed
- Process fire and gas explosion
- Nonprocess fire
- Falling objects
- Ship and helicopter collisions (injuries/fatalities to passengers and crew, impact to installation)
- Earthquakes
- Extreme weather conditions

- Commodity prices
- Regulations.

Other risk exposures are loss of key personnel, IT risks, and health and safety of personnel in a confined area. Musculoskeletal disorders (MSDs) are widely reported by offshore workers; cramped work areas, heavy physical work, frequent stair climbing, poor ergonomic design of workplaces, and psychosocial work stress generally are all potential causes of MSD (University of Oxford 2010). Since the industry is risk taking by nature, any company operating in this sector should carefully consider its insurance program and accurately define the size of the policy deductibles. The only few exceptions are companies that have reached such a size that they can decide to assume all their own risk. The main types of insurance coverage commonly used in the offshore energy insurance include the following:

- Business interruption
- Excess liability insurance
- Offshore physical damage coverage for physical damage or loss to offshore fixed platforms, pipelines, and production and accommodation facilities
- Operator's extra expense
- Workers' compensation.

The risk scenario development can be estimated by use of the event tree technique, based on identified hazards and parameters that are expected to influence the outcome and hence the total risk (Fig. 16). Based on the results we can set up a customized probability distribution function to model the severity of this risk scenario for the Monte Carlo simulation of the company's total risk exposure (Fig. 17).

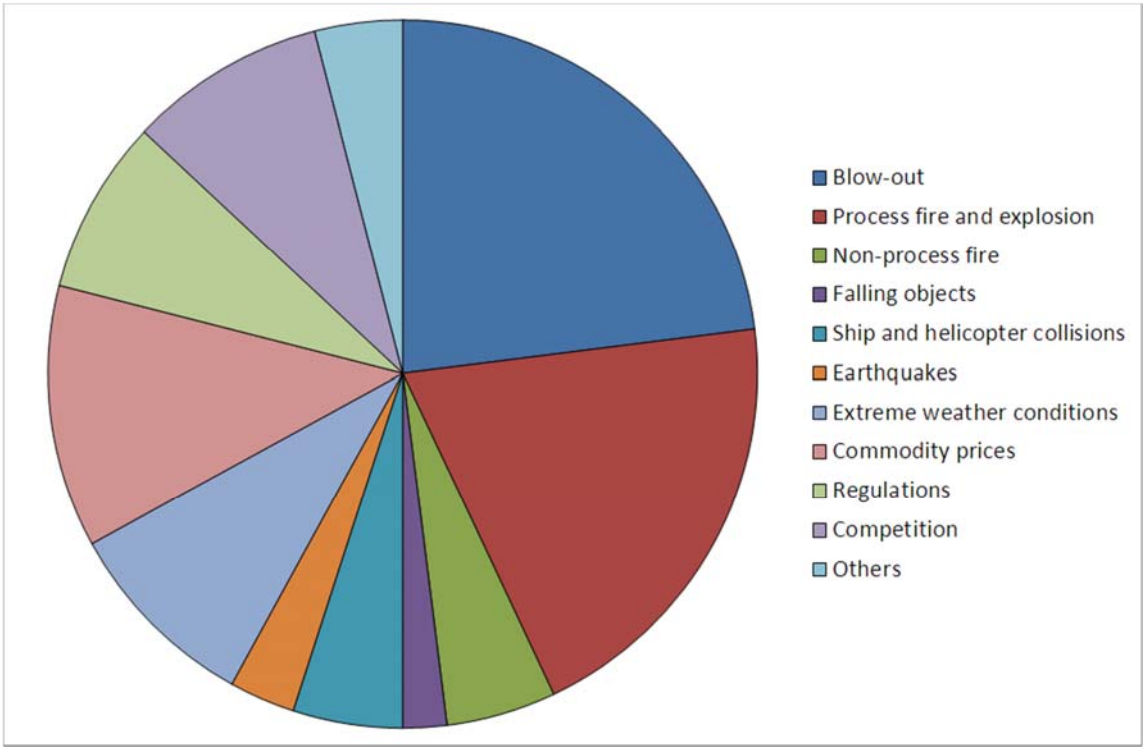

Figure 15: Earnings at Risk per Key Risk Exposure

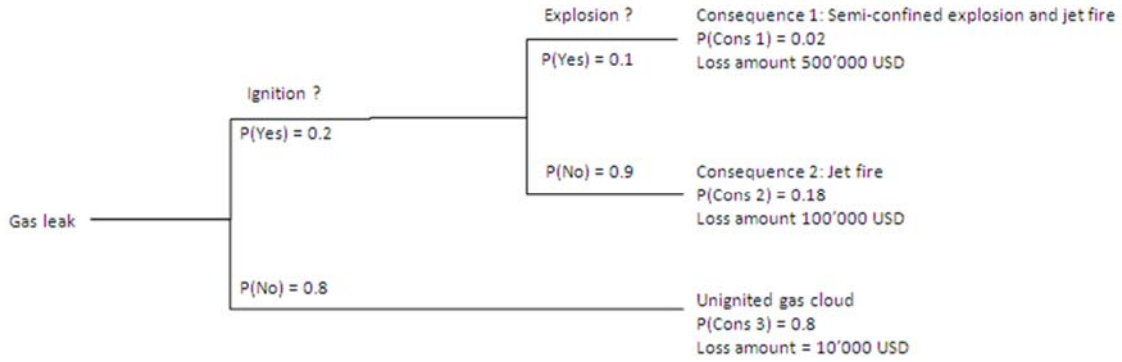

Figure 16: Event Tree Analysis

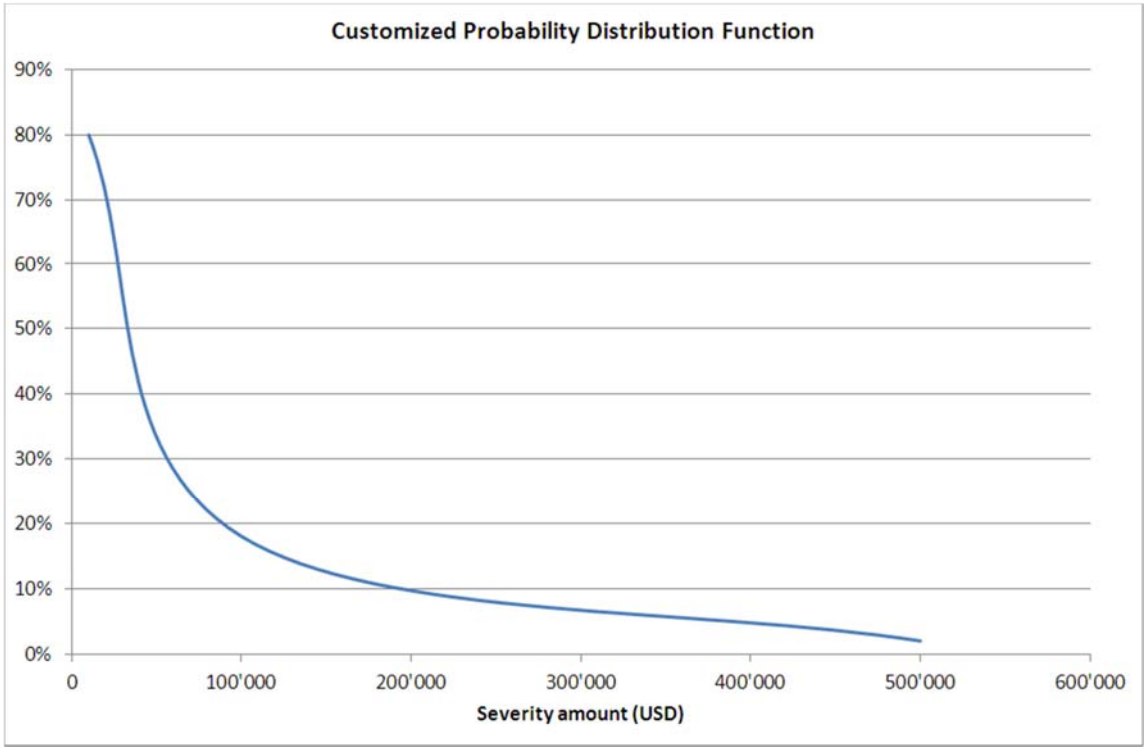

Figure 17: Probability Distribution Function Based on the Event Tree Analysis

4. Conclusion

Many risk management systems are not sufficiently developed for the various departments and/or project managers (production, logistics, research, H&R, etc.) to assess their familiar risks (a bottom-up risk approach by the local subject matter experts) and integrate them in a consolidated system so that the CRO can readily combine the all relevant business information to depict the company's EaR for the executive board members. An integrated tool used by all departments and business units ensures consistency in how the input and results are used, reduces sources of error, and decreases time spent in manual operations. An integrated risk management solution should be implemented to facilitate risk information throughout the organization, optimize the enterprise risk portfolio, identify natural hedges, create an optimal risk treatment plan, and track KRIs for early warning of key risk exposures.

References

Bahr, N. 1997. *System Safety Engineering and Risk Assessment: A Practical Approach.* Philadelphia: Taylor & Francis.

Beasley, M. S., B. C. Branson, and B. V. Hancock. 2010. Developing Key Risk Indicators to Strengthen Enterprise Risk Management. ERM Initiative at North Carolina State University.

Brandsæter, A. 2002. Risk Assessment in the Offshore Industry. *Safety Science* 231–269.

Elliot, D., E. Swartz, and B. Herbane. 1999. Just Waiting for the Next Big Bang: Business Continuity Planning in the UK Finance Sector. *Journal of Applied Management Studies* 8: 43–60.

Enterprise Risk Management Committee. 2003. Overview of Enterprise Risk Management. Casualty Actuarial Society. May.

Ernst & Young Global Limited. 2010. Risk Appetite: The Strategic Balancing Act. http://www.ey.com/GL/en/Services/Advisory/Risk-appetite--the-strategic-balancing-act.

Frigo, M. L., and H. Læssøe. 2012. Strategic Risk Management at the Lego Group. *Strategic Finance,* February.

Gorvett, R., and N. Liu. 2007. Measuring Operational Risk Interdependencies Using Interpretive Structural Modeling. ERM Symposium, Chicago.

IRM, AIRMIC, and Alarm. 2010. A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000.

Montagne, E., E. Norell, and D. Vaterlaus. 2012. Risikoexposition messbar machen, io management. Axel Springer Switzerland.

Segal, S. 2011. *Corporate Value of Enterprise Risk Management.* New York: Wiley.

University of Oxford. 2010. Offshore Working Time in Relation to Performance, Health and Safety: A Review of Current Practice and Evidence. Prepared by the University of Oxford for the Health and Safety Executive.