NIILM University

Risk Managment

Content

Chapter 1

Introduction to risk management

Risk management is the identification, assessment, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives, whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Risks can come from uncertainty in financial markets, threats from project failures (at any phase in design, development, production, or sustainment life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attack from an adversary, or events of uncertain or unpredictable root-cause. Natural causes and disasters also refers to Act of God in a legal term which is for events outside human control, such as sudden floods or other natural disasters, for which no one can be held responsible. In the law of contracts, an act of God may be interpreted as an implied defence under the rule of impossibility or impracticability. If so, the promise is discharged because of unforeseen occurrences, which were unavoidable and would result in insurmountable delay, expense, or other material breach.

An example scenario could assume that an opera singer and a concert hall have a contract. The singer promises to appear and perform at a certain time on a certain date. The hall promises to have the stage and audio equipment ready for her. However, a tornado destroys the hall a month before the concert is to take place. Of course, the hall is not responsible for the tornado. It may be impossible for the hall to rebuild in time to keep its promise. On the other hand, it may be possible but extraordinarily expensive to reconstruct on such short notice. The hall would argue that the tornado was an act of God and excuses its nonperformance via impossibility or impracticability.

In other contracts, such as indemnification, an act of God may be no excuse, and in fact may be the central risk assumed by the promisor—e.g., flood insurance or crop insurance—the only variables being the timing and extent of the damage. In many cases, failure by way of ignoring obvious risks due to "natural phenomena" will not be sufficient to excuse performance of the obligation, even if the events are relatively rare: e.g., the year 2000 problem in computers. Under the Uniform Commercial Code, 2-615, failure to deliver goods sold may be excused by an "act of God" if the absence of such act was a "basic assumption" of the contract, but has made the delivery "commercially impracticable".

Recently, human activities have been claimed to be the root causes of some events until now considered natural disasters. In particular:

water pressure in dams releasing a geological fault

geothermal injections of water provoking earthquakes

drilling provoking mud volcano

Such events are possibly threatening the legal status of Acts of God and may establish liabilities where none existed until now.

Several risk management standards have been developed including the Project Management Institute, the National Institute of Standards and Technology, actuarial societies, and ISO standards. Methods, definitions and goals vary widely according to whether the risk management method is in the context of project management, security, engineering, industrial processes, financial portfolios, actuarial assessments, or public health and safety.

The strategies to manage threats (uncertainties with negative consequences) typically include transferring the threat to another party, avoiding the threat, reducing the negative effect or probability of the threat, or even accepting some or all of the potential or actual consequences of a particular threat, and the opposites for opportunities (uncertain future states with benefits).

Certain aspects of many of the risk management standards have come under criticism for having no measurable improvement on risk, whether the confidence in estimates and decisions seem to increase.

Introduction

A widely used vocabulary for risk management is defined by ISO Guide 73, "Risk management. Vocabulary.

In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss (or impact) and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled in descending order. In practice the process of assessing overall risk can be difficult, and balancing resources used to mitigate between risks with a high probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled.

Intangible risk management identifies a new type of a risk that has a 100% probability of occurring but is ignored by the organization due to a lack of identification ability. For example, when deficient knowledge is applied to a situation, a knowledge risk materializes. Relationship risk appears when ineffective collaboration occurs. Process-engagement risk may be an issue when ineffective operational procedures are applied. These risks directly reduce the productivity of knowledge workers, decrease cost-effectiveness, profitability, service, quality, reputation, brand value, and earnings quality. Intangible risk management allows risk management to create immediate value from the identification and reduction of risks that reduce productivity.

Risk management also faces difficulties in allocating resources. This is the idea of opportunity cost. Resources spent on risk management could have been spent on more profitable activities. Again, ideal risk management minimizes spending (or manpower or other resources) and also minimizes the negative effects of risks.

Method of risk management

For the most part, these methods consist of the following elements, performed, more or less, in the following order.

- identify, characterize threats
- assess the vulnerability of critical assets to specific threats
- determine the risk (i.e. the expected likelihood and consequences of specific types of attacks on specific assets)
- identify ways to reduce those risks
- prioritize risk reduction measures based on a strategy
- Principles of risk management

The International Organization for Standardization (ISO) identifies the following principles of risk management:

Risk management should:

- create value – resources expended to mitigate risk should be less than the consequence of inaction, or (as in value engineering), the gain should exceed the pain
- be an integral part of organizational processes
- be part of decision making process
- explicitly address uncertainty and assumptions
- be systematic and structured
- be based on the best available information
- be tailorable
- take human factors into account
- be transparent and inclusive
- be dynamic, iterative and responsive to change
- be capable of continual improvement and enhancement
- be continually or periodically re-assessed

To summarize:

The process of identification, analysis and either acceptance or mitigation of uncertainty in investment decision-making. Essentially, risk management occurs anytime an investor or fund manager analyzes and attempts to quantify the potential for losses in an investment and then takes the appropriate action (or inaction) given their investment objectives and risk tolerance. Inadequate risk management can result in severe consequences for companies as well as individuals. For example, the recession that began in 2008 was largely caused by the loose credit risk management of financial firms.

Simply put, risk management is a two-step process - determining what risks exist in an investment and then handling those risks in a way best-suited to your investment objectives. Risk management occurs everywhere in the financial world. It occurs when an investor buys low-risk government bonds over more risky corporate debt, when a fund manager hedges their currency exposure with currency derivatives and when a bank performs a credit check on an individual before issuing them a personal line of credit.

Chapter 2

Process of risk management

According to the standard ISO 31000 "Risk management – Principles and guidelines on implementation, the process of risk management consists of several steps as follows:

Establishing the context which involves:

- ✓ identification of risk in a selected domain of interest
- ✓ planning the remainder of the process
- ✓ mapping out the following:
- ✓ the social scope of risk management
- ✓ the identity and objectives of stakeholders
- ✓ the basis upon which risks will be evaluated, constraints.
- ✓ defining a framework for the activity and an agenda for identification
- ✓ developing an analysis of risks involved in the process
- ✓ mitigation or solution of risks using available technological, human and organizational resources.
- ✓ Identification

After establishing the context, the next step in the process of managing risk is to identify potential risks. Risks are about events that, when triggered, cause problems or benefits. Hence, risk identification can start with the source of our problems and those of our competitors (benefit), or with the problem itself.

Source analysis - Risk sources may be internal or external to the system that is the target of risk management (use mitigation instead of management since by its own definition risk deals with factors of decision-making that cannot be managed).

Examples of risk sources are: stakeholders of a project, employees of a company or the weather over an airport.

Problem analysis - Risks are related to identified threats. For example: the threat of losing money, the threat of abuse of confidential information or the threat of human errors, accidents and casualties. The threats may exist with various entities, most important with shareholders, customers and legislative bodies such as the government.

When either source or problem is known, the events that a source may trigger or the events that can lead to a problem can be investigated. For example: stakeholders withdrawing during a project may endanger funding of the project; confidential information may be stolen by employees even within a closed network; lightning striking an aircraft during takeoff may make all people on board immediate casualties.

The chosen method of identifying risks may depend on culture, industry practice and compliance. The identification methods are formed by templates or the development of templates for identifying source, problem or event. Common risk identification methods are:

Objectives-based risk identification- Organizations and project teams have objectives. Any event that may endanger achieving an objective partly or completely is identified as risk.

Scenario-based risk identification - In scenario analysis different scenarios are created. The scenarios may be the alternative ways to achieve an objective, or an analysis of the interaction of forces in, for example, a market or battle. Any event that triggers an undesired scenario alternative is identified as risk – see Futures Studies for methodology used by Futurists.

Taxonomy-based risk identification - The taxonomy in taxonomy-based risk identification is a breakdown of possible risk sources. Based on the taxonomy and knowledge of best practices, a questionnaire is compiled. The answers to the questions reveal risks.

Common-risk checking - In several industries, lists with known risks are available. Each risk in the list can be checked for application to a particular situation

Risk charting - This method combines the above approaches by listing resources at risk, threats to those resources, modifying factors which may increase or decrease the risk and consequences it is wished to avoid. Creating a matrix under these headings enables a variety of approaches. One can begin with resources and consider the threats they are exposed to and the consequences of each. Alternatively one can start with the threats and examine which resources they would affect, or one can begin with the consequences and determine which combination of threats and resources would be involved to bring them about.

Assessment

Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard). Quantitative risk assessment requires calculations of two components of risk (R):, the magnitude of the potential loss (L), and the probability (p) that the loss will occur. Acceptable risk is a risk that is understood and tolerated usually because the cost or difficulty of implementing an effective countermeasure for the associated vulnerability exceeds the expectation of loss.

In all types of engineering of complex systems sophisticated risk assessments are often made within Safety engineering and Reliability engineering when it concerns threats to life, environment or machine functioning. The nuclear, aerospace, oil, rail and military industries have a long history of dealing with risk assessment. Also, medical, hospital, social service and food industries control risks and perform risk assessments on a continual basis. Methods for assessment of risk may differ between industries and whether it pertains to general financial decisions or environmental, ecological, or public health risk assessment.

Risk assessment consists of an objective evaluation of risk in which assumptions and uncertainties are clearly considered and presented. Part of the difficulty in risk management is that measurement of both of the quantities in which risk assessment is concerned - potential loss and probability of occurrence - can be very difficult to measure. The chance of error in measuring these two concepts is large. Risk with a large potential loss and a low probability of occurring is often treated differently from one with a low potential loss and a high likelihood of occurring. In theory, both are of nearly equal priority, but in practice it can be very difficult to manage when faced with the scarcity of resources, especially time, in which to conduct the risk management process.

Financial decisions, such as insurance, express loss in terms of dollar amounts. When risk assessment is used for public health or environmental decisions, loss can be quantified in a common metric such as a country's currency or some numerical measure of a location's quality of life. For public health and environmental decisions, loss is simply a verbal description of the outcome, such as increased cancer incidence or incidence of birth defects.

If the risk estimate takes into account information on the number of individuals exposed, it is termed a "population risk" and is in units of expected increased cases per a time period. If the risk estimate does not take into account the number of individuals exposed, it is termed an "individual risk" and is in units of incidence rate per a time period. Population risks are of more use for cost/benefit analysis; individual risks are of more use for evaluating whether risks to individuals are "acceptable".

Once risks have been identified, they must then be assessed as to their potential severity of impact (generally a negative impact, such as damage or loss) and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of the probability of an unlikely event occurring. Therefore, in the assessment process it is critical to make the best educated decisions in order to properly prioritize the implementation of the risk management plan.

Even a short-term positive improvement can have long-term negative impacts. Take the "turnpike" example. A highway is widened to allow more traffic. More traffic capacity leads to greater development in the areas surrounding the improved traffic capacity. Over time, traffic thereby increases to fill available capacity. Turnpikes thereby need to be expanded in a seemingly endless cycles. There are many other engineering examples where expanded capacity (to do any function) is soon filled by increased demand. Since expansion comes at a cost, the resulting growth could become unsustainable without forecasting and management.

The fundamental difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kinds of past incidents. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for intangible assets. Asset valuation is another question that needs to be addressed. Thus, best educated opinions and available statistics are the primary sources of information. Nevertheless, risk assessment should produce such information for the management of the organization that the primary risks are easy to understand and that the risk management decisions may be prioritized. Thus, there have been several theories and attempts to quantify risks. Numerous different risk formulae exist, but perhaps the most widely accepted formula for risk quantification is:

Rate (or probability) of occurrence multiplied by the impact of the event equals risk magnitude.

Risk assessment in public health

In the context of public health, risk assessment is the process of quantifying the probability of a harmful effect to individuals or populations from certain human activities. In most countries the use of specific chemicals or the operations of specific facilities (e.g. power plants, manufacturing plants) is not allowed unless it can be shown that they do not increase the risk of death or illness above a specific threshold. For example, the American Food and Drug Administration (FDA) regulates food safety through risk assessment. The FDA required in 1973 that cancer-causing compounds must not be present in meat at concentrations that would cause a cancer risk greater than 1 in a million lifetimes. The US Environmental Protection Agency provides basic information about environmental risk assessments for the public via its risk assessment portal. The Stockholm Convention on persistent organic pollutants (POPs) supports a qualitative risk framework for public health protection from chemicals that display environmental and biological persistence, bioaccumulation, toxicity (PBT) and long range transport; most global chemicals that meet this criteria have been previously assessed quantitatively by national and international health agencies.

How the risk is determined?

In the estimation of risks, three or more steps are involved that require the inputs of different disciplines:

Hazard Identification, aims to determine the qualitative nature of the potential adverse consequences of the contaminant (chemical, radiation, noise, etc.) and the strength of the evidence it can have that effect. This is done, for chemical hazards, by drawing from the results of the sciences of toxicology and epidemiology. For other kinds of hazard, engineering or other disciplines are involved.

Dose-Response Analysis, is determining the relationship between dose and the probability or the incidence of effect (dose-response assessment). The complexity of this step in many contexts derives mainly from the need to extrapolate results from experimental animals (e.g. mouse, rat) to humans, and/or from high to lower doses. In addition, the differences between individuals due to genetics or other factors mean that the hazard may be higher for particular groups, called susceptible populations. An alternative to dose-response estimation is to determine a concentration unlikely to yield observable effects, that is, a no effect concentration. In developing such a dose, to account for the largely unknown effects of animal to human extrapolations, increased variability in humans, or missing data, a prudent approach is often adopted by including safety factors in the estimate of the "safe" dose, typically a factor of 10 for each unknown step.

Exposure Quantification, aims to determine the amount of a contaminant (dose) that individuals and populations will receive. This is done by examining the results of the discipline of exposure assessment. As different location, lifestyles and other factors likely influence the amount of contaminant that is received, a range or distribution of possible values is generated in this step. Particular care is taken to determine the exposure of the susceptible population(s).

Finally, the results of the three steps above are then combined to produce an estimate of risk. Because of the different susceptibilities and exposures, this risk will vary within a population.

Composite Risk Index

The above formula can also be re-written in terms of a Composite Risk Index, as follows:

Composite Risk Index = Impact of Risk event x Probability of Occurrence

The impact of the risk event is commonly assessed on a scale of 1 to 5, where 1 and 5 represent the minimum and maximum possible impact of an occurrence of a risk (usually in terms of financial losses). However, the 1 to 5 scale can be arbitrary and need not be on a linear scale.

The probability of occurrence is likewise commonly assessed on a scale from 1 to 5, where 1 represents a very low probability of the risk event actually occurring while 5 represents a very high probability of occurrence. This axis may be expressed in either mathematical terms (event occurs once a year, once in ten years, once in 100 years etc.) or may be expressed in "plain english" (event has occurred here very often; event has been known to occur here; event has been known to occur in the industry etc.). Again, the 1 to 5 scale can be arbitrary or non-linear depending on decisions by subject-matter experts.

The Composite Index thus can take values ranging (typically) from 1 through 25, and this range is usually arbitrarily divided into three sub-ranges. The overall risk assessment is then Low, Medium or High, depending on the sub-range containing the calculated value of the Composite Index. For instance, the three sub-ranges could be defined as 1 to 8, 9 to 16 and 17 to 25.

Note that the probability of risk occurrence is difficult to estimate, since the past data on frequencies are not readily available, as mentioned above. After all, probability does not imply certainty.

Likewise, the impact of the risk is not easy to estimate since it is often difficult to estimate the potential loss in the event of risk occurrence.

Further, both the above factors can change in magnitude depending on the adequacy of risk avoidance and prevention measures taken and due to changes in the external business environment. Hence it is absolutely necessary to periodically re-assess risks and intensify/relax mitigation measures, or as necessary. Changes in procedures, technology, schedules, budgets, market conditions, political environment, or other factors typically require re-assessment of risks.

Chapter 3

Risk Options

Risk mitigation measures are usually formulated according to one or more of the following major risk options, which are:

Design a new business process with adequate built-in risk control and containment measures from the start.

Periodically re-assess risks that are accepted in ongoing processes as a normal feature of business operations and modify mitigation measures.

Transfer risks to an external agency (e.g. an insurance company)

Avoid risks altogether (e.g. by closing down a particular high-risk business area)

Later research has shown that the financial benefits of risk management are less dependent on the formula used but are more dependent on the frequency and how risk assessment is performed.

In business it is imperative to be able to present the findings of risk assessments in financial, market, or schedule terms. Robert Courtney Jr. (IBM, 1970) proposed a formula for presenting risks in financial terms. The Courtney formula was accepted as the official risk analysis method for the US governmental agencies. The formula proposes calculation of ALE (annualised loss expectancy) and compares the expected loss value to the security control implementation costs (cost-benefit analysis).

Cost–benefit analysis (CBA), sometimes called benefit–cost analysis (BCA), is a systematic process for calculating and comparing benefits and costs of a project, decision or government policy (hereafter, "project"). CBA has two purposes:

To determine if it is a sound investment/decision (justification/feasibility), To provide a basis for comparing projects. It involves comparing the total expected cost of each option against the total expected benefits, to see whether the benefits outweigh the costs, and by how much.

CBA is related to, but distinct from cost-effectiveness analysis. In CBA, benefits and costs are expressed in monetary terms, and are adjusted for the time value of money, so that all flows of benefits and flows of project costs over time (which tend to occur at different points in time) are expressed on a common basis in terms of their "net present value."

Closely related, but slightly different, formal techniques include cost-effectiveness analysis, cost–utility analysis, economic impact analysis, fiscal impact analysis, and Social return on investment (SROI) analysis.

Cost–benefit analysis is often used by governments and other organizations, such as private sector businesses, to evaluate the desirability of a given policy. It is an analysis of the expected balance of benefits and costs, including an account of foregone alternatives and the status quo. CBA helps predict whether the benefits of a policy outweigh its costs, and by how much relative to other alternatives (i.e. one can rank alternate policies in terms of the cost–benefit ratio). Generally, accurate cost–benefit analysis identifies choices that increase welfare from a utilitarian perspective. Assuming an accurate CBA, changing the status quo by implementing the alternative with the lowest cost–benefit ratio can improve Pareto efficiency. An analyst using CBA should recognize that perfect evaluation of all present and future costs and benefits is difficult, and while CBA can offer a well-educated estimate of the best alternative, perfection in terms of economic efficiency and social welfare are not guaranteed.

The following is a list of steps that comprise a generic cost–benefit analysis.

- ✓ List alternative projects/programs.
- ✓ List stakeholders.
- ✓ Select measurement(s) and measure all cost/benefit elements.
- ✓ Predict outcome of cost and benefits over relevant time period.
- ✓ Convert all costs and benefits into a common currency.
- ✓ Apply discount rate.
- ✓ Calculate net present value of project options.

- ✓ Perform sensitivity analysis.
- ✓ Adopt recommended choice.

Potential risk treatments

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories:

Avoidance (eliminate, withdraw from or not become involved)

Reduction (optimize – mitigate)

Sharing (transfer – outsource or insure)

Retention (accept and budget)

Ideal use of these strategies may not be possible. Some of them may involve trade-offs that are not acceptable to the organization or person making the risk management decisions. Another source, from the US Department of Defense (see link), Defense Acquisition University, calls these categories ACAT, for Avoid, Control, Accept, or Transfer. This use of the ACAT acronym is reminiscent of another ACAT (for Acquisition Category) used in US Defense industry procurements, in which Risk Management figures prominently in decision making and planning.

Risk avoidance

This includes not performing an activity that could carry risk. An example would be not buying a property or business in order to not take on the legal liability that comes with it. Another would be not flying in order not to take the risk that the airplane were to be hijacked. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits. Increasing risk regulation in hospitals has led to avoidance of treating higher risk conditions, in favour of patients presenting with lower risk.

Hazard prevention

Hazard prevention refers to the prevention of risks in an emergency. The first and most effective stage of hazard prevention is the elimination of hazards. If this takes too long, is too costly, or is otherwise impractical, the second stage is mitigation.

Risk reduction

Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. For example, sprinklers are designed to put out a fire to reduce the risk of loss by fire. This method may cause a greater loss by water damage and therefore may not be suitable. Halon fire suppression systems may mitigate that risk, but the cost may be prohibitive as a strategy.

Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and effort applied. By an offshore drilling contractor effectively applying HSE Management in its organization, it can optimize risk to achieve levels of residual risk that are tolerable.

Modern software development methodologies reduce risk by developing and delivering software incrementally. Early methodologies suffered from the fact that they only delivered software in the final phase of development; any problems encountered in earlier phases meant costly rework and often jeopardized the whole project. By developing in iterations, software projects can limit effort wasted to a single iteration.

Outsourcing could be an example of risk reduction if the outsourcer can demonstrate higher capability at managing or reducing risks. For example, a company may outsource only its software development, the manufacturing of hard goods, or customer support needs to another company, while handling the business management itself. This way, the company can concentrate more on business development without having to worry as much about the manufacturing process, managing the development team, or finding a physical location for a call center.

Risk sharing

Briefly defined as "sharing with another party the burden of loss or the benefit of gain, from a risk, and the measures to reduce a risk."

The term of 'risk transfer' is often used in place of risk sharing in the mistaken belief that you can transfer a risk to a third party through insurance or outsourcing. In practice if the insurance company or contractor go bankrupt or end up in court, the original risk is likely to still revert to the first party. As such in the terminology of practitioners and scholars alike, the purchase of an insurance contract is often described as a "transfer of risk." However, technically speaking, the buyer of the contract generally retains legal responsibility for the losses "transferred", meaning that insurance may be described more accurately as a post-event compensatory mechanism. For example, a personal injuries insurance policy does not transfer the risk of a car accident to the insurance company. The risk still lies with the policy holder namely the person who has been in the accident. The insurance policy simply provides that if an accident (the event) occurs involving the policy holder then some compensation may be payable to the policy holder that is commensurate to the suffering/damage.

Some ways of managing risk fall into multiple categories. Risk retention pools are technically retaining the risk for the group, but spreading it over the whole group involves transfer among individual members of the group. This is different from traditional insurance, in that no premium is exchanged between members of the group up front, but instead losses are assessed to all members of the group.

Risk retention

Involves accepting the loss, or benefit of gain, from a risk when it occurs. True self insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

Chapter 4

Create a Risk Management Plan

A Risk Management Plan is a document that a project manager prepares to foresee risks, estimate impacts, and define responses to issues. It also contains a risk assessment matrix.

A risk is "an uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objectives." Risk is inherent with any project, and project managers should assess risks continually and develop plans to address them. The risk management plan contains an analysis of likely risks with both high and low impact, as well as mitigation strategies to help the project avoid being derailed should common problems arise. Risk management plans should be periodically reviewed by the project team to avoid having the analysis become stale and not reflective of actual potential project risks.

Most critically, risk management plans include a risk strategy. Broadly, there are four potential strategies, with numerous variations. Projects may choose to:

Avoid risk — Change plans to circumvent the problem;

Control/Mitigate risk; — Reduces impact or likelihood (or both) through intermediate steps;

Accept risk — Take the chance of negative impact (or auto-insurance), eventually budget the cost (e.g. via a contingency budget line);

Transfer risk — Outsource risk (or a portion of the risk - Share risk) to third party/ies that can manage the outcome. This is done e.g. financially through insurance contracts or hedging transactions, or operationally through outsourcing an activity.

(Mnemonic: SARA for Share Avoid Reduce Accept, or A-CAT for "Avoid, Control, Accept, or Transfer")

Risk management plans often include matrices.

The United States Department of Defense, as part of acquisition, uses risk management planning that may have a Risk Management Plan document for the specific project. The general intent of the RMP in this context is to define the scope of risks to be tracked and means of documenting reports. It is also desired that there would be an integrated relationship to other processes. An example of this would be explaining which developmental tests verify risks of the design type were minimized are stated as part of the Test and Evaluation Master Plan. A further example would be instructions from 5000.2D that for programs that are part of a System of systems the risk management strategy shall specifically address integration and interoperability as a risk area. The RMP specific process and templates shift over time (e.g. the disappearance of 2002 documents Defense Finance and Accounting Service / System Risk Management Plan, and the SPAWAR Risk Management Process).

Select appropriate controls or countermeasures to measure each risk. Risk mitigation needs to be approved by the appropriate level of management. For instance, a risk concerning the image of the organization should have top management decision behind it whereas IT management would have the authority to decide on computer virus risks.

The risk management plan should propose applicable and effective security controls for managing the risks. For example, an observed high risk of computer viruses could be mitigated by acquiring and implementing antivirus software. A good risk management plan should contain a schedule for control implementation and responsible persons for those actions.

According to ISO/IEC 27001, the stage immediately after completion of the risk assessment phase consists of preparing a Risk Treatment Plan, which should document the decisions about how each of the identified risks should be handled. Mitigation of risks often means selection of security controls, which should be documented in a Statement of Applicability, which identifies which particular control objectives and controls from the standard have been selected, and why.

Implementation

Implementation follows all of the planned methods for mitigating the effect of the risks. Purchase insurance policies for the risks that have been decided to be transferred to an insurer, avoid all risks that can be avoided without sacrificing the entity's goals, reduce others, and retain the rest.

Review and evaluation of the plan

Initial risk management plans will never be perfect. Practice, experience, and actual loss results will necessitate changes in the plan and contribute information to allow possible different decisions to be made in dealing with the risks being faced.

Chapter 5

Areas of risk management

As applied to corporate finance, risk management is the technique for measuring, monitoring and controlling the financial or operational risk on a firm's balance sheet. See value at risk.

The Basel II framework breaks risks into market risk (price risk), credit risk and operational risk and also specifies methods for calculating capital requirements for each of these components.

Market risk (price risk)

Market risk is the risk of losses in positions arising from movements in market prices.

Types of market risk

Some market risks include:

Equity risk, the risk that stock or stock indices (e.g. Euro Stoxx 50, etc.) prices and/or their implied volatility will change.

Interest rate risk, the risk that interest rates (e.g. Libor, Euribor, etc.) and/or their implied volatility will change.

Currency risk, the risk that foreign exchange rates (e.g. EUR/USD, EUR/GBP, etc.) and/or their implied volatility will change.

Commodity risk, the risk that commodity prices (e.g. corn, copper, crude oil, etc.) and/or their implied volatility will change.

Risk management

All businesses take risks based on two factors: the probability an adverse circumstance will come about and the cost of such adverse circumstance. Risk management is the study of how to control risks and balance the possibility of gains.

Measuring the potential loss amount due to market risk

As with other forms of risk, the potential loss amount due to market risk may be measured in a number of ways or conventions. Traditionally, one convention is to use Value at Risk. The conventions of using Value at risk is well established and accepted in the short-term risk management practice.

However, it contains a number of limiting assumptions that constrain its accuracy. The first assumption is that the composition of the portfolio measured remains unchanged over the specified period. Over short time horizons, this limiting assumption is often regarded as reasonable. However, over longer time horizons, many of the positions in the portfolio may have been changed. The Value at Risk of the unchanged portfolio is no longer relevant.

The Variance Covariance and Historical Simulation approach to calculating Value at Risk also assumes that historical correlations are stable and will not change in the future or breakdown under times of market stress.

In addition, care has to be taken regarding the intervening cash flow, embedded options, changes in floating rate interest rates of the financial positions in the portfolio. They cannot be ignored if their impact can be large.

Credit risk

Credit risk refers to the risk that a borrower will default on any type of debt by failing to make required payments. The risk is primarily that of the lender and includes lost principal and interest, disruption to cash flows, and increased collection costs. The loss may be complete or partial and can arise in a number of circumstances. For example:

A consumer may fail to make a payment due on a mortgage loan, credit card, line of credit, or other loan

A company is unable to repay asset-secured fixed or floating charge debt

A business or consumer does not pay a trade invoice when due

A business does not pay an employee's earned wages when due

A business or government bond issuer does not make a payment on a coupon or principal payment when due

An insolvent insurance company does not pay a policy obligation

An insolvent bank won't return funds to a depositor

A government grants bankruptcy protection to an insolvent consumer or business

To reduce the lender's credit risk, the lender may perform a credit check on the prospective borrower, may require the borrower to take out appropriate insurance, such as mortgage insurance or seek security or guarantees of third parties. In general, the higher the risk, the higher will be the interest rate that the debtor will be asked to pay on the debt.

Types of credit risk

Credit risk can be classified as follows:

Credit default risk — The risk of loss arising from a debtor being unlikely to pay its loan obligations in full or the debtor is more than 90 days past due on any material credit obligation; default risk may impact all credit-sensitive transactions, including loans, securities and derivatives.

Concentration risk — The risk associated with any single exposure or group of exposures with the potential to produce large enough losses to threaten a bank's core operations. It may arise in the form of single name concentration or industry concentration.

Country risk — The risk of loss arising from a sovereign state freezing foreign currency payments (transfer/conversion risk) or when it defaults on its obligations (sovereign risk); this type of risk is prominently associated with the country's macroeconomic performance and its political stability.

Assessing credit risk

Significant resources and sophisticated programs are used to analyze and manage risk. Some companies run a credit risk department whose job is to assess the financial health of their customers, and extend credit (or not) accordingly. They may use in house programs to advise on avoiding, reducing and transferring risk. They also use third party provided intelligence. Companies like Standard & Poor's, Moody's, Fitch Ratings, Dun and Bradstreet, and Rapid Ratings provide such information for a fee.

Most lenders employ their own models (credit scorecards) to rank potential and existing customers according to risk, and then apply appropriate strategies. With products such as unsecured personal loans or mortgages, lenders charge a higher price for higher risk customers and vice versa. With revolving products such as credit cards and overdrafts, risk is controlled through the setting of credit limits. Some products also require collateral, most commonly in the form of property.

Credit scoring models also form part of the framework used by banks or lending institutions to grant credit to clients. For corporate and commercial borrowers, these models generally have qualitative and quantitative sections outlining various aspects of the risk including, but not limited to, operating experience, management expertise, asset quality, and leverage and liquidity ratios, respectively. Once this information has been fully reviewed by credit officers and credit committees, the lender provides the funds subject to the terms and conditions presented within the contract (as outlined above).

Sovereign risk

Sovereign risk is the risk of a government being unwilling or unable to meet its loan obligations, or reneging on loans it guarantees. Many countries have faced sovereign risk in the late-2000s global recession. The existence of such risk means that creditors should take a two-stage decision process when deciding to lend to a firm based in a foreign country. Firstly one should consider the sovereign risk quality of the country and then consider the firm's credit quality.

Five macroeconomic variables that affect the probability of sovereign debt rescheduling are:

Debt service ratio

Import ratio

Investment ratio

Variance of export revenue

Domestic money supply growth

The probability of rescheduling is an increasing function of debt service ratio, import ratio, variance of export revenue and domestic money supply growth. The likelihood of rescheduling is a decreasing function of investment ratio due to future economic productivity gains. Debt rescheduling likelihood can increase if the investment ratio rises as the foreign country could become less dependent on its external creditors and so be less concerned about receiving credit from these countries/investors.

Counterparty risk

A counterparty risk, also known as a default risk, is a risk that a counterparty will not pay as obligated on a bond, credit derivative, trade credit insurance or payment protection insurance contract, or other trade or transaction. Financial institutions may hedge or take out credit insurance. Offsetting counterparty risk is not always possible, e.g. because of temporary liquidity issues or longer term systemic reasons.

Counterparty risk increases due to positively correlated risk factors. Accounting for correlation between portfolio risk factors and counterparty default in risk management methodology is not trivial.

Mitigating credit risk

Lenders mitigate credit risk using several methods:

Risk-based pricing: Lenders generally charge a higher interest rate to borrowers who are more likely to default, a practice called risk-based pricing. Lenders consider factors relating to the loan such as loan purpose, credit rating, and loan-to-value ratio and estimates the effect on yield (credit spread).

Covenants: Lenders may write stipulations on the borrower, called covenants, into loan agreements:

Periodically report its financial condition

Refrain from paying dividends, repurchasing shares, borrowing further, or other specific, voluntary actions that negatively affect the company's financial position

Repay the loan in full, at the lender's request, in certain events such as changes in the borrower's debt-to-equity ratio or interest coverage ratio

Credit insurance and credit derivatives: Lenders and bond holders may hedge their credit risk by purchasing credit insurance or credit derivatives. These contracts transfer the risk from the lender to the seller (insurer) in exchange for payment. The most common credit derivative is the credit default swap.

Tightening: Lenders can reduce credit risk by reducing the amount of credit extended, either in total or to certain borrowers. For example, a distributor selling its products to a troubled retailer may attempt to lessen credit risk by reducing payment terms from net 30 to net 15.

Diversification: Lenders to a small number of borrowers (or kinds of borrower) face a high degree of unsystematic credit risk, called concentration risk. Lenders reduce this risk by diversifying the borrower pool.

Deposit insurance: Many governments establish deposit insurance to guarantee bank deposits in the event of insolvency and encourage consumers to hold their savings in the banking system instead of in cash.

Operational risk

An operational risk is defined as a risk incurred by an organisation's internal activities.

Operational risk is the broad discipline focusing on the risks arising from the people, systems and processes through which a company operates. It can also include other classes of risk, such as fraud, legal risks, physical or environmental risks.

A widely used definition of operational risk is the one contained in the Basel II regulations. This definition states that operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

Operational risk management differs from other types of risk, because it is not used to generate profit (e.g. credit risk is exploited by lending institutions to create profit, market risk is exploited by traders and fund managers, and insurance risk is exploited by insurers). They all however manage operational risk to keep losses within their risk appetite - the amount of risk they are prepared to accept in pursuit of their objectives. What this means in practical terms is that organisations accept that their people, processes and systems are imperfect, and that losses will arise from errors and ineffective operations. The size of the loss they are prepared to accept, because the cost of correcting the errors or improving the systems is disproportionate to the benefit they will receive, determines their appetite for operational risk.

Since the mid-1990s, the topics of market risk and credit risk have been the subject of much debate and research, with the result that financial institutions have made significant progress in the identification, measurement and management of both these forms of risk. However, it is worth mentioning that the near collapse of the U.S. financial system in September 2008 is a clear indication that our ability to measure market and credit risk is far from perfect.

Globalization and deregulation in financial markets, combined with increased sophistication in financial technology, have introduced more complexities into the activities of banks and therefore their risk profiles. These reasons underscore banks' and supervisors' growing focus upon the identification and measurement of operational risk.

Events such as the September 11 terrorist attacks, rogue trading losses at Société Générale, Barings, AIB, UBS and National Australia Bank serve to highlight the fact that the scope of risk management extends beyond merely market and credit risk.

The list of risks (and, more importantly, the scale of these risks) faced by banks today includes fraud, system failures, terrorism and employee compensation claims. These types of risk are generally classified under the term 'operational risk'.

The identification and measurement of operational risk is a real and live issue for modern-day banks, particularly since the decision by the Basel Committee on Banking Supervision (BCBS) to introduce a capital charge for this risk as part of the new capital adequacy framework (Basel II).

Definition

The Basel II Committee defines operational risk as:

"The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."

However, the Basel Committee recognizes that operational risk is a term that has a variety of meanings and therefore, for internal purposes, banks are permitted to adopt their own definitions of operational risk, provided that the minimum elements in the Committee's definition are included.

Scope exclusions

The Basel II definition of operational risk excludes, for example, strategic risk - the risk of a loss arising from a poor strategic business decision.

Other risk terms are seen as potential consequences of operational risk events. For example, reputational risk (damage to an organization through loss of its reputation or standing) can arise as a consequence (or impact) of operational failures - as well as from other events.

Basel II event type categories

The following lists the official Basel II defined event types with some examples for each category:

Internal Fraud - misappropriation of assets, tax evasion, intentional mismarking of positions, bribery

External Fraud- theft of information, hacking damage, third-party theft and forgery

Employment Practices and Workplace Safety - discrimination, workers compensation, employee health and safety

Clients, Products, & Business Practice- market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning

Damage to Physical Assets - natural disasters, terrorism, vandalism

Business Disruption & Systems Failures - utility disruptions, software failures, hardware failures

Execution, Delivery, & Process Management - data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets

Difficulties

It is relatively straightforward for an organization to set and observe specific, measurable levels of market risk and credit risk because models exist which attempt to predict the potential impact of market movements, or changes in the cost of credit. It should be noted however that these models are only as good as the underlying assumptions, and a large part of the recent financial crisis arose because the valuations generated by these models for particular types of investments were based on incorrect assumptions.

By contrast it is relatively difficult to identify or assess levels of operational risk and its many sources. Historically organizations have accepted operational risk as an unavoidable cost of doing business. Many now though collect data on operational losses - for example through system failure or fraud - and are using this data to model operational risk and to calculate a capital reserve against future operational losses. In addition to the Basel II requirement for banks, this is now a requirement for European insurance firms who are in the process of implementing Solvency II, the equivalent of Basel II for the banking sector.

Methods of operational risk management

Basel II and various Supervisory bodies of the countries have prescribed various soundness standards for Operational Risk Management for Banks and similar Financial Institutions. To complement these standards, Basel II has given guidance to 3 broad methods of Capital calculation for Operational Risk

Basic Indicator Approach - based on annual revenue of the Financial Institution

Standardized Approach - based on annual revenue of each of the broad business lines of the Financial Institution

Advanced Measurement Approaches - based on the internally developed risk measurement framework of the bank adhering to the standards prescribed (methods include IMA, LDA, Scenario-based, Scorecard etc.)

The Operational Risk Management framework should include identification, measurement, monitoring, reporting, control and mitigation frameworks for Operational Risk.

Chapter 6

Enterprise risk management

Enterprise risk management (ERM) in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall. (ERM)

ERM can also be described as a risk-based approach to managing an enterprise, integrating concepts of internal control, the Sarbanes–Oxley Act, and strategic planning. ERM is evolving to address the needs of various stakeholders, who want to understand the broad spectrum of risks facing complex organizations to ensure they are appropriately managed. Regulators and debt rating agencies have increased their scrutiny on the risk management processes of companies.

ERM frameworks defined

There are various important ERM frameworks, each of which describes an approach for identifying, analyzing, responding to, and monitoring risks and opportunities, within the internal and external environment facing the enterprise. Management selects a risk response strategy for specific risks identified and analyzed, which may include:

Avoidance: exiting the activities giving rise to risk

Reduction: taking action to reduce the likelihood or impact related to the risk

Alternative Actions: deciding and considering other feasible steps to minimize risks.

Share or Insure: transferring or sharing a portion of the risk, to finance it

Accept: no action is taken, due to a cost/benefit decision

Monitoring is typically performed by management as part of its internal control activities, such as review of analytical reports or management committee meetings with relevant experts, to understand how the risk response strategy is working and whether the objectives are being achieved.

Casualty Actuarial Society framework

In 2003, the Casualty Actuarial Society (CAS) defined ERM as the discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organization's short- and long-term value to its stakeholders." The CAS conceptualized ERM as proceeding across the two dimensions of risk type and risk management processes.The risk types and examples include:

Hazard risk

Liability torts, Property damage, Natural catastrophe

Financial risk

Pricing risk, Asset risk, Currency risk, Liquidity risk

Operational risk

Customer satisfaction, Product failure, Integrity, Reputational risk

Strategic risks

Competition, Social trend, Capital availability

The risk management process involves:

Establishing Context: This includes an understanding of the current conditions in which the organization operates on an internal, external and risk management context.

Identifying Risks: This includes the documentation of the material threats to the organization's achievement of its objectives and the representation of areas that the organization may exploit for competitive advantage.

Analyzing/Quantifying Risks: This includes the calibration and, if possible, creation of probability distributions of outcomes for each material risk.

Integrating Risks: This includes the aggregation of all risk distributions, reflecting correlations and portfolio effects, and the formulation of the results in terms of impact on the organization's key performance metrics.

Assessing/Prioritizing Risks: This includes the determination of the contribution of each risk to the aggregate risk profile, and appropriate prioritization.

Treating/Exploiting Risks: This includes the development of strategies for controlling and exploiting the various risks.

Monitoring and Reviewing: This includes the continual measurement and monitoring of the risk environment and the performance of the risk management strategies.

COSO ERM framework

The COSO "Enterprise Risk Management-Integrated Framework" published in 2004 defines ERM as a "…process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

The COSO ERM Framework has eight Components and four objectives categories. It is an expansion of the COSO Internal Control-Integrated Framework published in 1992 and amended in 1994. The eight components - additional components highlighted - are:

Internal Environment

Objective Setting

Event Identification

Risk Assessment

Risk Response

Control Activities

Information and Communication

Monitoring

The four objectives categories - additional components highlighted - are:

Strategy - high-level goals, aligned with and supporting the organization's mission

Operations - effective and efficient use of resources

Financial Reporting - reliability of operational and financial reporting

Compliance - compliance with applicable laws and regulations

RIMS Risk Maturity Model

The RIMS Risk Maturity Model (RMM) for Enterprise Risk Management, published in 2008, is an umbrella framework of content and methodology that detail the requirements for sustainable and effective enterprise risk management. The RMM model consists of twenty-five competency drivers for seven attributes that create ERM’s value and utility in an organization. The 7 attributes are:

ERM-based approach

ERM process management

Risk appetite management

Root cause discipline

Uncovering risks

Performance management

Business resiliency and sustainability

The model was published by the Risk and Insurance Management society and developed with the support of co-developer Steven Minsky, CEO of LogicManager. The Risk Maturity Model is based on the Capability Maturity Model, a methodology founded by the Carnegie Mellon University Software Engineering Institute (SEI) in the 1980's.

Implementing an ERM program

Goals of an ERM program

Organizations by nature manage risks and have a variety of existing departments or functions ("risk functions") that identify and manage particular risks. However, each risk function varies in capability and how it coordinates with other risk functions. A central goal and challenge of ERM is improving this capability and coordination, while integrating the output to provide a unified picture of risk for stakeholders and improving the organization's ability to manage the risks effectively.

Typical risk functions

The primary risk functions in large corporations that may participate in an ERM program typically include:

Strategic planning - identifies external threats and competitive opportunities, along with strategic initiatives to address them

Marketing - understands the target customer to ensure product/service alignment with customer requirements

Compliance & Ethics - monitors compliance with code of conduct and directs fraud investigations

Accounting / Financial compliance - directs the Sarbanes-Oxley Section 302 and 404 assessment, which identifies financial reporting risks

Law Department - manages litigation and analyzes emerging legal trends that may impact the organization

Insurance - ensures the proper insurance coverage for the organization

Treasury - ensures cash is sufficient to meet business needs, while managing risk related to commodity pricing or foreign exchange

Operational Quality Assurance - verifies operational output is within tolerances

Operations management - ensures the business runs day-to-day and that related barriers are surfaced for resolution

Credit - ensures any credit provided to customers is appropriate to their ability to pay

Customer service - ensures customer complaints are handled promptly and root causes are reported to operations for resolution

Internal audit - evaluates the effectiveness of each of the above risk functions and recommends improvements

Common challenges in ERM implementation

Various consulting firms offer suggestions for how to implement an ERM program.Common topics and challenges include:

Identifying executive sponsors for ERM.

Establishing a common risk language or glossary.

Describing the entity's risk appetite (i.e., risks it will and will not take)

Identifying and describing the risks in a "risk inventory".

Implementing a risk-ranking methodology to prioritize risks within and across functions.

Establishing a risk committee and or Chief Risk Officer (CRO) to coordinate certain activities of the risk functions.

Establishing ownership for particular risks and responses.

Demonstrating the cost-benefit of the risk management effort.

Developing action plans to ensure the risks are appropriately managed.

Developing consolidated reporting for various stakeholders.

Monitoring the results of actions taken to mitigate risk.

Ensuring efficient risk coverage by internal auditors, consulting teams, and other evaluating entities.

Developing a technical ERM framework that enables secure participation by 3rd parties and remote employees.

Internal audit role

In addition to information technology audit, internal auditors play an important role in evaluating the risk management processes of an organization and advocating their continued improvement. However, to preserve its organizational independence and objective judgment, Internal Audit professional standards indicate the function should not take any direct responsibility for making risk management decisions for the enterprise or managing the risk management function.

Internal auditors typically perform an annual risk assessment of the enterprise, to develop a plan of audit engagements for the upcoming year. This plan is updated at various frequencies in practice. This typically involves review of the various risk assessments performed by the enterprise (e.g., strategic plans, competitive benchmarking, and SOX top-down risk assessment), consideration of prior audits, and interviews with a variety of senior management. It is designed for identifying audit projects, not to identify, prioritize, and manage risks directly for the enterprise.

Current issues in ERM

The risk management processes of U.S. corporations are under increasing regulatory and private scrutiny. Risk is an essential part of any business. Properly managed, it drives growth and opportunity. Executives struggle with business pressures that may be partly or completely beyond their immediate control, such as distressed financial markets; mergers, acquisitions and restructurings; disruptive technology change; geopolitical instabilities; and the rising price of energy.

Sarbanes-Oxley Act requirements

Section 404 of the Sarbanes-Oxley Act of 2002 required U.S. publicly traded corporations to utilize a control framework in their internal control assessments. Many opted for the COSO Internal Control Framework, which includes a risk assessment element. In addition, new guidance issued by the Securities and Exchange Commission (SEC) and PCAOB in 2007 placed increasing scrutiny on top-down risk assessment and included a specific requirement to perform a fraud risk assessment. Fraud risk assessments typically involve identifying scenarios of potential (or experienced) fraud, related exposure to the organization, related controls, and any action taken as a result.

NYSE corporate governance rules

The New York Stock Exchange requires the Audit Committees of its listed companies to "discuss policies with respect to risk assessment and risk management." The related commentary continues: "While it is the job of the CEO and senior management to assess and manage the company's exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the company's major financial risk exposures and the steps management has taken to monitor and control such exposures. The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken. Many companies, particularly financial companies, manage and assess their risk through mechanisms other than the audit committee. The processes these companies have in place should be reviewed in a general manner by the audit committee, but they need not be replaced by the audit committee."

ERM and corporate debt ratings

Standard & Poor's (S&P), the debt rating agency, plans to include a series of questions about risk management in its company evaluation process. This will rollout to financial companies in 2007. The results of this inquiry is one of the many factors considered in debt rating, which has a corresponding impact on the interest rates lenders charge companies for loans or bonds. On May

7, 2008, S&P also announced that it would begin including an ERM assessment in its ratings for non-financial companies starting in 2009, with initial comments in its reports during Q4 2008.

ISO 31000 : the new International Risk Management Standard

ISO 31000 is an International Standard for Risk Management which was published on 13 November 2009. An accompanying standard, ISO 31010 - Risk Assessment Techniques, soon followed publication (December 1, 2009) together with the updated Risk Management vocabulary ISO Guide 73.

Actuarial response

Casualty Actuarial Society

In 2003, the Enterprise Risk Management Committee of the Casualty Actuarial Society (CAS) issued its overview of ERM. This paper laid out the evolution, rationale, definitions, and frameworks for ERM from the casualty actuarial perspective, and also included a vocabulary, conceptual and technical foundations, actual practice and applications, and case studies.

The CAS has specific stated ERM goals, including being "a leading supplier internationally of educational materials relating to Enterprise Risk Management (ERM) in the property casualty insurance arena," and has sponsored research, development, and training of casualty actuaries in that regard. The CAS has refrained from issuing its own credential; instead, in 2007, the CAS Board decided that the CAS should participate in the initiative to develop a global ERM designation, and make a final decision at some later date.

Society of Actuaries

In 2007, the Society of Actuaries developed the Chartered Enterprise Risk Analyst (CERA) credential in response to the growing field of enterprise risk management. This is the first new professional credential to be introduced by the SOA since 1949. A CERA studies to focus on how various risks, including operational, investment, strategic, and reputational combine to affect organizations. CERAs work in environments beyond insurance, reinsurance and the consulting markets, including broader financial services, energy, transportation, media, technology, manufacturing and healthcare.

It takes approximately three to four years to complete the CERA curriculum which combines basic actuarial science, ERM principles and a course on professionalism. To earn the CERA credential, candidates must take five exams, fulfill an educational experience requirement, complete one online course, and attend one in-person course on professionalism. CERAs are members of the Society of Actuaries.

Institute and Faculty of Actuaries

The Institute and Faculty of Actuaries (the merged body formed in 2010 from the Institute of Actuaries and the Faculty of Actuaries) is the professional body representing actuaries in the United Kingdom. In March 2008, Enterprise Risk Management was adopted as one of the six actuarial practice areas, reflecting the increased involvement of actuaries in the ERM field.

A regular newsletter communicates the ongoing work that the profession performs in respect of ERM.

Some of the key areas that the profession works on are summarised below (together with some of the recent outcomes in each area):

Education, CPD, Career Support and Development

From April 2010 actuaries were able to study ERM as one of the Specialist Technical Stage exams (ST9 course information), which (with other exam passes) gives candidates the Chartered Enterprise Risk Actuary (CERA) qualification. In July 2010 the first nine actuaries to obtain the CERA qualification were announced. The CERA qualification is offered by 13 participating actuarial associations, with further information available at a global or UK level.

Various events (e.g. networking evenings and webinars) are available to actuaries and other interested parties. The main event is the Risk and Investment Conference, which is often held during the summer months (e.g. 2011 Risk & Investment Conference). There is also some regularly reviewed material available from the profession which may be of use in developing knowledge of ERM.

Research & Thought Leadership

A committee has been established to consider research and thought leadership in the ERM field (including what the “elevator speech” on ERM issues might be, definition of the scope of ERM and demonstration of the value of ERM).

Some areas in which work has been completed include:

- ERM - A guide to Implementation

- A survey on actuaries in risk management

- A suggested common risk classification system for the actuarial profession

Research topics will be categorised and subject to a number of tests before proceeding with the research.

- enterprise-wide test (not just topic-specific / silo-based)

- risk management test (management = taking actions, not just modelling)

- director test (important enough for the Board, not just line managers)

Communications & Marketing

Actuaries continue to look to demonstrate and promote the value of actuaries and the CERA qualification in the field of ERM - including through publication of articles in the Actuary

The Actuarial Profession also liases with other professions where appropriate- e.g. the Institution of Civil Engineers on considering ERM in the context of Risk Analysis and Management for Projects (RAMP).

Companies Increasingly Focusing on ERM

It is clear that companies recognize ERM as a critical management issue. This is demonstrated through the prominence assigned to ERM within organizations and the resources devoted to building ERM capabilities. In a 2008 survey by Towers Perrin, at most life insurance companies, responsibility for ERM resides within the C-suite. Most often, the chief risk officer (CRO) or the chief financial officer (CFO) is in charge of ERM, and these individuals typically report directly to the chief executive officer. From their vantage point, the CRO and CFO are able to look across the organization and develop a perspective on the risk profile of the firm and how that profile matches its risk appetite. They act as drivers to improve skills, tools and processes for evaluating risks and to weigh various actions to manage those exposures. Companies are also actively enhancing their ERM tools and capabilities. Three quarters of responding companies said they have tools for specifically monitoring and managing enterprise-wide risk. These tools are used primarily for identifying and measuring risk and for management decision making. Respondents also reported that they have made good progress in building their ERM capabilities in certain areas.

In this study, more than 80% of respondents reported that they currently have adequate or better controls in place for most major risks. In addition, about 60% currently have a coordinated process for risk governance and include risk management in decision making to optimize risk adjusted returns.

In another survey conducted in May and June 2008, against the backdrop of the developing financial crisis, six major findings came to light regarding risk and capital management among insurers worldwide:

Embedding ERM is proving to be a significant challenge

Company size matters

European insurers are better positioned

ERM is influencing important strategic decisions

Economic capital standards are gaining ground

Operational risk remains a weak spot

In enterprise risk management, a risk is defined as a possible event or circumstance that can have negative influences on the enterprise in question. Its impact can be on the very existence, the resources (human and capital), the products and services, or the customers of the enterprise, as well as external impacts on society, markets, or the environment. In a financial institution, enterprise risk management is normally thought of as the combination of credit risk, interest rate risk or asset liability management, liquidity risk, market risk, and operational risk.

In the more general case, every probable risk can have a pre-formulated plan to deal with its possible consequences (to ensure contingency if the risk becomes a liability).

From the information above and the average cost per employee over time, or cost accrual ratio, a project manager can estimate:

the cost associated with the risk if it arises, estimated by multiplying employee costs per unit time by the estimated time lost (cost impact, C where C = cost accrual ratio * S).

the probable increase in time associated with a risk (schedule variance due to risk, Rs where Rs = P * S):

Sorting on this value puts the highest risks to the schedule first. This is intended to cause the greatest risks to the project to be attempted first so that risk is minimized as quickly as possible.

This is slightly misleading as schedule variances with a large P and small S and vice versa are not equivalent. (The risk of the RMS Titanic sinking vs. the passengers' meals being served at slightly the wrong time).

the probable increase in cost associated with a risk (cost variance due to risk, Rc where Rc = P*C = P*CAR*S = P*S*CAR)

sorting on this value puts the highest risks to the budget first.

see concerns about schedule variance as this is a function of it, as illustrated in the equation above.

Risk in a project or process can be due either to Special Cause Variation or Common Cause Variation and requires appropriate treatment. That is to re-iterate the concern about extremal cases not being equivalent in the list immediately above.

Risk management activities as applied to project management

In project management, risk management includes the following activities:

Planning how risk will be managed in the particular project. Plans should include risk management tasks, responsibilities, activities and budget.

Assigning a risk officer – a team member other than a project manager who is responsible for foreseeing potential project problems. Typical characteristic of risk officer is a healthy skepticism.

Maintaining live project risk database. Each risk should have the following attributes: opening date, title, short description, probability and importance. Optionally a risk may have an assigned person responsible for its resolution and a date by which the risk must be resolved.

Creating anonymous risk reporting channel. Each team member should have the possibility to report risks that he/she foresees in the project.

Preparing mitigation plans for risks that are chosen to be mitigated. The purpose of the mitigation plan is to describe how this particular risk will be handled – what, when, by whom and how will it be done to avoid it or minimize consequences if it becomes a liability.

Summarizing planned and faced risks, effectiveness of mitigation activities, and effort spent for the risk management.

Chapter 7

Project management

Project management is the discipline of planning, organizing, motivating, and controlling resources to achieve specific goals. A project is a temporary endeavor designed to produce a unique product, service or result with a defined beginning and end (usually time-constrained, and often constrained by funding or deliverables), undertaken to meet unique goals and objectives, typically to bring about beneficial change or added value. The temporary nature of projects stands in contrast with business as usual (or operations), which are repetitive, permanent, or semi-permanent functional activities to produce products or services. In practice, the management of these two systems is often quite different, and as such requires the development of distinct technical skills and management strategies.

The primary challenge of project management is to achieve all of the project goals and objectives while honoring the preconceived constraints. The primary constraints are scope, time, quality and budget. The secondary —and more ambitious— challenge is to optimize the allocation of necessary inputs and integrate them to meet pre-defined objectives.

As a discipline, project management developed from several fields of application including civil construction, engineering, and heavy defense activity. Two forefathers of project management are Henry Gantt, called the father of planning and control techniques, who is famous for his use of the Gantt chart as a project management tool (alternatively Harmonogram first proposed by Karol Adamiecki; and Henri Fayol for his creation of the five management functions that form the foundation of the body of knowledge associated with project and program management. Both Gantt and Fayol were students of Frederick Winslow Taylor's theories of scientific management. His work is the forerunner to modern project management tools including work breakdown structure (WBS) and resource allocation.

The 1950s marked the beginning of the modern project management era where core engineering fields come together to work as one. Project management became recognized as a distinct discipline arising from the management discipline with engineering model. In the United States, prior to the 1950s, projects were managed on an ad-hoc basis, using mostly Gantt charts and informal techniques and tools. At that time, two mathematical project-scheduling models were developed. The "Critical Path Method" (CPM) was developed as a joint venture between DuPont Corporation and Remington Rand Corporation for managing plant maintenance projects. And the "Program Evaluation and Review Technique" or PERT, was developed by Booz Allen Hamilton as part of the United States Navy's (in conjunction with the Lockheed Corporation) Polaris missile submarine program; These mathematical techniques quickly spread into many private enterprises.

At the same time, as project-scheduling models were being developed, technology for project cost estimating, cost management, and engineering economics was evolving, with pioneering work by Hans Lang and others. In 1956, the American Association of Cost Engineers (now AACE International; the Association for the Advancement of Cost Engineering) was formed by early practitioners of project management and the associated specialties of planning and scheduling, cost estimating, and cost/schedule control (project control). AACE continued its pioneering work and in 2006 released the first integrated process for portfolio, program and project management (Total Cost Management Framework).

The International Project Management Association (IPMA) was founded in Europe in 1967, as a federation of several national project management associations. IPMA maintains its federal structure today and now includes member associations on every continent except Antarctica. IPMA offers a Four Level Certification program based on the IPMA Competence Baseline (ICB).The ICB covers technical, contextual, and behavioral competencies.

In 1969, the Project Management Institute (PMI) was formed in the USA. PMI publishes A Guide to the Project Management Body of Knowledge (PMBOK Guide), which describes project management practices that are common to "most projects, most of the time." PMI also offers multiple certifications.

Approaches

Here are a number of approaches to managing project activities including lean, iterative, incremental, and phased approaches.

Regardless of the methodology employed, careful consideration must be given to the overall project objectives, timeline, and cost, as well as the roles and responsibilities of all participants and stakeholders.

The traditional approach

A traditional phased approach identifies a sequence of steps to be completed. In the "traditional approach", five developmental components of a project can be distinguished (four stages plus control):

- ✓ initiation
- ✓ planning and design
- ✓ execution and construction
- ✓ monitoring and controlling systems
- ✓ completion

Not all projects will have every stage, as projects can be terminated before they reach completion. Some projects do not follow a structured planning and/or monitoring process. And some projects will go through steps 2, 3 and 4 multiple times.

Many industries use variations of these project stages. For example, when working on a brick-and-mortar design and construction, projects will typically progress through stages like pre-planning, conceptual design, schematic design, design development, construction drawings (or contract documents), and construction administration. In software development, this approach is often known as the waterfall model, i.e., one series of tasks after another in linear sequence. In software development many organizations have adapted the Rational Unified Process (RUP) to fit this methodology, although RUP does not require or explicitly recommend this practice. Waterfall development works well for small, well defined projects, but often fails in larger projects of undefined and ambiguous nature. The Cone of Uncertainty explains some of this as the planning made on the initial phase of the project suffers from a high degree of uncertainty. This becomes especially true as software development is often the realization of a new or novel product. In projects where requirements have not been finalized and can change, requirements management is used to develop an accurate and complete definition of the behavior of software that can serve as the basis for software development. While the terms may differ from industry to industry, the actual stages typically follow common steps to problem solving—"defining the problem, weighing options, choosing a path, implementation and evaluation."

Prince2

PRINCE2 is a structured approach to project management released in 1996 as a generic project management method. It combines the original PROMPT methodology (which evolved into the PRINCE methodology) with IBM's MITP (managing the implementation of the total project) methodology. PRINCE2 provides a method for managing projects within a clearly defined framework.

PRINCE2 focuses on the definition and delivery of products, in particular their quality requirements. As such, it defines a successful project as being output-oriented (not activity- or task-oriented) through creating an agreed set of products that define the scope of the project and provides the basis for planning and control, that is, how then to coordinate people and activities, how to design and supervise product delivery, and what to do if products and therefore the scope of the project has to be adjusted if it does not develop as planned.

In the method, each process is specified with its key inputs and outputs and with specific goals and activities to be carried out to deliver a project's outcomes as defined by its Business Case. This allows for continuous assessment and adjustment when deviation from the Business Case is required.

PRINCE2 provides a common language for all participants in the project. The governance framework of PRINCE2 – its roles and responsibilities – are fully described and require tailoring to suit the complexity of the project and skills of the organisation.

Critical chain project management

Main article: Critical chain project management

Critical chain project management (CCPM) is a method of planning and managing project execution designed to deal with uncertainties inherent in managing projects, while taking into consideration limited availability of resources (physical, human skills, as well as management & support capacity) needed to execute projects.

CCPM is an application of the theory of constraints (TOC) to projects. The goal is to increase the flow of projects in an organization (throughput). Applying the first three of the five focusing steps of TOC, the system constraint for all projects is identified as are the resources. To exploit the constraint, tasks on the critical chain are given priority over all other activities. Finally, projects are planned and managed to ensure that the resources are ready when the critical chain tasks must start, subordinating all other resources to the critical chain.

The project plan should typically undergo resource leveling, and the longest sequence of resource-constrained tasks should be identified as the critical chain. In some cases, such as managing contracted sub-projects, it is advisable to use a simplified approach without resource leveling.

In multi-project environments, resource leveling should be performed across projects. However, it is often enough to identify (or simply select) a single "drum". The drum can be a resource that acts as a constraint across projects, which are staggered based on the availability of that single resource.

One can also use a "virtual drum" by selecting a task or group of tasks (typically integration points) and limiting the number of projects in execution at that stage.

Event chain methodology

Event chain methodology is another method that complements critical path method and critical chain project management methodologies.

Event chain methodology is an uncertainty modeling and schedule network analysis technique that is focused on identifying and managing events and event chains that affect project schedules. Event chain methodology helps to mitigate the negative impact of psychological heuristics and biases, as well as to allow for easy modeling of uncertainties in the project schedules. Event chain methodology is based on the following principles.

Probabilistic moment of risk: An activity (task) in most real-life processes is not a continuous uniform process. Tasks are affected by external events, which can occur at some point in the middle of the task.

Event chains: Events can cause other events, which will create event chains. These event chains can significantly affect the course of the project. Quantitative analysis is used to determine a cumulative effect of these event chains on the project schedule.

Critical events or event chains: The single events or the event chains that have the most potential to affect the projects are the “critical events” or “critical chains of events.” They can be determined by the analysis.

Project tracking with events: Even if a project is partially completed and data about the project duration, cost, and events occurred is available, it is still possible to refine information about future potential events and helps to forecast future project performance.

Event chain visualization: Events and event chains can be visualized using event chain diagrams on a Gantt chart.

Process-based management

Also furthering the concept of project control is the incorporation of process-based management. This area has been driven by the use of Maturity models such as the CMMI (capability maturity model integration; see this example of a predecessor) and ISO/IEC15504 (SPICE – software process improvement and capability estimation).

Agile project management

Agile project management approaches, based on the principles of human interaction management, are founded on a process view of human collaboration. It is "most typically used in software, website, technology, creative and marketing industries." This contrasts sharply with the traditional approach. In the agile software development or flexible product development approach, the project is seen as a series of relatively small tasks conceived and executed as the situation demands in an adaptive manner, rather than as a completely pre-planned process. Advocates of this technique claim that:

* It is the most consistent project management technique since it involves frequent testing of the project under development.

* It is the only technique in which the client will be actively involved in the project development.

* The only disadvantage with this technique is that it should be used only if the client has enough time to be actively involved in the project every now and then.

Examples of Agile Project Management tools and techniques include:

Scrum development - A holistic approach to development that focuses on iterative goals set by the Product Owner through a backlog, which is developed by the Delivery Team through the facilitation of the Scrum Master.

Extreme Programming (XP) - Also called "Pair Programming" this method uses small groups and has a highly prescriptive Test Driven Development (TDD) model.

eXtreme Manufacturing (XM) - An agile methodology based on Scrum development, Kanban and Kaizen that facilitates rapid engineering and prototyping.

Crystal Clear (software development) - An agile or lightweight methodology that focuses on colocation and osmotic communication.

Lean project management

Lean project management uses the principles from lean manufacturing to focus on delivering value with less waste and reduced time.

Extreme project management

In critical studies of project management it has been noted that several PERT based models are not well suited for the multi-project company environment of today. Most of them are aimed at very large-scale, one-time, non-routine projects, and currently all kinds of management are expressed in terms of projects.

Using complex models for "projects" (or rather "tasks") spanning a few weeks has been proven to cause unnecessary costs and low maneuverability in several cases. The generalization of Extreme Programming to other kinds of projects is extreme project management, which may be used in combination with the process modeling and management principles of human interaction management.

Benefits realization management

Benefits realization management (BRM) enhances normal project management techniques through a focus on outcomes (the benefits) of a project rather than products or outputs, and then measuring the degree to which that is happening to keep a project on track. This can help to reduce the risk of a completed project being a failure by delivering agreed upon requirements/outputs but failing to deliver the benefits of those requirements.

An example of delivering a project to requirements might be agreeing to deliver a computer system that will process staff data and manage payroll, holiday and staff personnel records. Under BRM the agreement might be to achieve a specified reduction in staff hours required to process and maintain staff data.

Processes

Traditionally, project management includes a number of elements: four to five process groups, and a control system. Regardless of the methodology or terminology used, the same basic project management processes will be used. Major process groups generally include:

- ✓ Initiation
- ✓ Planning or design
- ✓ Production or execution
- ✓ Monitoring and controlling
- ✓ Closing

In project environments with a significant exploratory element (e.g., research and development), these stages may be supplemented with decision points (go/no go decisions) at which the project's continuation is debated and decided. An example is the Phase–gate model.

Initiating

The initiating processes determine the nature and scope of the project. If this stage is not performed well, it is unlikely that the project will be successful in meeting the business' needs. The key project controls needed here are an understanding of the business environment and making sure that all necessary controls are incorporated into the project. Any deficiencies should be reported and a recommendation should be made to fix them.

The initiating stage should include a plan that encompasses the following areas:

analyzing the business needs/requirements in measurable goals

reviewing of the current operations

financial analysis of the costs and benefits including a budget

stakeholder analysis, including users, and support personnel for the project

project charter including costs, tasks, deliverables, and schedule

Planning and design

After the initiation stage, the project is planned to an appropriate level of detail (see example of a flow-chart). The main purpose is to plan time, cost and resources adequately to estimate the work needed and to effectively manage risk during project execution. As with the Initiation process group, a failure to adequately plan greatly reduces the project's chances of successfully accomplishing its goals.

Project planning generally consists of

determining how to plan (e.g. by level of detail or rolling wave);

developing the scope statement;

selecting the planning team;

identifying deliverables and creating the work breakdown structure;

identifying the activities needed to complete those deliverables and networking the activities in their logical sequence;

estimating the resource requirements for the activities;

estimating time and cost for activities;

developing the schedule;

developing the budget;

risk planning;

gaining formal approval to begin work.

Additional processes, such as planning for communications and for scope management, identifying roles and responsibilities, determining what to purchase for the project and holding a kick-off meeting are also generally advisable.

For new product development projects, conceptual design of the operation of the final product may be performed concurrent with the project planning activities, and may help to inform the planning team when identifying deliverables and planning activities.

Executing

Executing consists of the processes used to complete the work defined in the project plan to accomplish the project's requirements. Execution process involves coordinating people and resources, as well as integrating and performing the activities of the project in accordance with the project management plan. The deliverables are produced as outputs from the processes performed as defined in the project management plan and other frameworks that might be applicable to the type of project at hand.

Execution process group include:

Direct and manage project execution

Quality assurance of deliverables

Acquire, develop and manage Project team

Distribute information

Manage stakeholder expectations

Conduct procurement

Test the deliverables against the initial design

Monitoring and Controlling

Monitoring and controlling consists of those processes performed to observe project execution so that potential problems can be identified in a timely manner and corrective action can be taken, when necessary, to control the execution of the project. The key benefit is that project performance is observed and measured regularly to identify variances from the project management plan.

Monitoring and controlling includes:

Measuring the ongoing project activities ('where we are');

Monitoring the project variables (cost, effort, scope, etc.) against the project management plan and the project performance baseline (where we should be);

Identify corrective actions to address issues and risks properly (How can we get on track again);

Influencing the factors that could circumvent integrated change control so only approved changes are implemented.

In multi-phase projects, the monitoring and control process also provides feedback between project phases, in order to implement corrective or preventive actions to bring the project into compliance with the project management plan.

Project maintenance is an ongoing process, and it includes:

Continuing support of end-users

Correction of errors

Updates of the software over time

In this stage, auditors should pay attention to how effectively and quickly user problems are resolved.

Over the course of any construction project, the work scope may change. Change is a normal and expected part of the construction process. Changes can be the result of necessary design modifications, differing site conditions, material availability, contractor-requested changes, value engineering and impacts from third parties, to name a few. Beyond executing the change in the field, the change normally needs to be documented to show what was actually constructed. This is referred to as change management. Hence, the owner usually requires a final record to show all changes or, more specifically, any change that modifies the tangible portions of the finished work. The record is made on the contract documents – usually, but not necessarily limited to, the design drawings. The end product of this effort is what the industry terms as-built drawings, or more simply, “as built.” The requirement for providing them is a norm in construction contracts.

When changes are introduced to the project, the viability of the project has to be re-assessed. It is important not to lose sight of the initial goals and targets of the projects. When the changes accumulate, the forecasted result may not justify the original proposed investment in the project.

Closing

Closing includes the formal acceptance of the project and the ending thereof. Administrative activities include the archiving of the files and documenting lessons learned.

This phase consists of:

Contract closure: Complete and settle each contract (including the resolution of any open items) and close each contract applicable to the project or project phase.

Project close: Finalize all activities across all of the process groups to formally close the project or a project phase

Project controlling and project control systems

Project controlling should be established as an independent function in project management. It implements verification and controlling function during the processing of a project in order to reinforce the defined performance and formal goals. The tasks of project controlling are also:

the creation of infrastructure for the supply of the right information and its update the establishment of a way to communicate disparities of project parameters

the development of project information technology based on an intranet or the determination of a project key performance index system (KPI)

divergence analyses and generation of proposals for potential project regulations

the establishment of methods to accomplish an appropriate project structure, project workflow organization, project control and governance

creation of transparency among the project parameters

Fulfillment and implementation of these tasks can be achieved by applying specific methods and instruments of project controlling. The following methods of project controlling can be applied:

investment analysis

cost–benefit analyses

value benefit Analysis

expert surveys

simulation calculations

risk-profile analyses

surcharge calculations

milestone trend analysis

cost trend analysis

target/actual-comparison

Project control is that element of a project that keeps it on-track, on-time and within budget. Project control begins early in the project with planning and ends late in the project with post-implementation review, having a thorough involvement of each step in the process. Each project should be assessed for the appropriate level of control needed: too much control is too time consuming, too little control is very risky. If project control is not implemented correctly, the cost to the business should be clarified in terms of errors, fixes, and additional audit fees.

Control systems are needed for cost, risk, quality, communication, time, change, procurement, and human resources. In addition, auditors should consider how important the projects are to the financial statements, how reliant the stakeholders are on controls, and how many controls exist. Auditors should review the development process and procedures for how they are implemented. The process of development and the quality of the final product may also be assessed if needed or requested. A business may want the auditing firm to be involved throughout the process to catch problems earlier on so that they can be fixed more easily. An auditor can serve as a controls consultant as part of the development team or as an independent auditor as part of an audit.

Businesses sometimes use formal systems development processes. These help assure that systems are developed successfully. A formal process is more effective in creating strong controls, and auditors should review this process to confirm that it is well designed and is followed in practice. A good formal systems development plan outlines:

A strategy to align development with the organization's broader objectives

Standards for new systems

Project management policies for timing and budgeting

Procedures describing the process

Evaluation of quality of change

Project managers

A project manager is a professional in the field of project management. Project managers can have the responsibility of the planning, execution, and closing of any project, typically relating to construction industry, engineering, architecture, computing, and telecommunications. Many other fields in production engineering and design engineering and heavy industrial have project managers.

A project manager is the person accountable for accomplishing the stated project objectives. Key project management responsibilities include creating clear and attainable project objectives, building the project requirements, and managing the triple constraint for projects, which is cost, time, and scope.

A project manager is often a client representative and has to determine and implement the exact needs of the client, based on knowledge of the firm they are representing. The ability to adapt to the various internal procedures of the contracting party, and to form close links with the nominated representatives, is essential in ensuring that the key issues of cost, time, quality and above all, client satisfaction, can be realized.

Project management types

While Project management, by itself, is a discipline that can apply to any project intended to deliver solutions for any purpose, it is often tailored to accommodate the specific and repeatable needs of different and highly specialized industries. For example, the construction industry, which focuses on the delivery of things like buildings, roads, and bridges, has developed its own specialized form of project management that it refers to as Construction project management and for which project managers can become trained and certified in. The Information technology industry has also evolved to develop its own form of Project management that is referred to as IT Project management and which specializes in the delivery of technical assets and services that are required to pass through various lifecycle phases such as planning, design, development, testing, and deployment. Biotechnology project management focuses on the intricacies of biotechnology research and development.

For each type of project management, project managers develop and utilize repeatable templates that are specific to the industry they're dealing with. This allows project plans to become very thorough and highly repeatable, with the specific intent to increase quality, lower delivery costs, and lower time to deliver project results.

Project management triangle

The project management triangle

Like any human undertaking, projects need to be performed and delivered under certain constraints. Traditionally, these constraints have been listed as "scope," "time," and "cost". These are also referred to as the "project management triangle", where each side represents a constraint. One side of the triangle cannot be changed without affecting the others. A further refinement of the constraints separates product "quality" or "performance" from scope, and turns quality into a fourth constraint.

The time constraint refers to the amount of time available to complete a project. The cost constraint refers to the budgeted amount available for the project. The scope constraint refers to what must be done to produce the project's end result. These three constraints are often competing constraints: increased scope typically means increased time and increased cost, a tight time constraint could mean increased costs and reduced scope, and a tight budget could mean increased time and reduced scope.

The discipline of project management is about providing the tools and techniques that enable the project team (not just the project manager) to organize their work to meet these constraints.

Work breakdown structure

The work breakdown structure (WBS) is a tree structure that shows a subdivision of effort required to achieve an objective—for example a program, project, and contract. The WBS may be hardware-, product-, service-, or process-oriented (see an example in a NASA reporting structure (2001)).

A WBS can be developed by starting with the end objective and successively subdividing it into manageable components in terms of size, duration, and responsibility (e.g., systems, subsystems, components, tasks, sub-tasks, and work packages), which include all steps necessary to achieve the objective.

The work breakdown structure provides a common framework for the natural development of the overall planning and control of a contract and is the basis for dividing work into definable increments from which the statement of work can be developed and technical, schedule, cost, and labor hour reporting can be established.

Project management framework

The program (investment) life cycle integrates the project management and system development life cycles with the activities directly associated with system deployment and operation. By design, system operation management and related activities occur after the project is complete and are not documented within this guide (see an example of an IT project management framework).

For example, see figure, in the US United States Department of Veterans Affairs (VA) the program management life cycle is depicted and describe in the overall VA IT Project Management Framework to address the integration of OMB Exhibit 300 project (investment) management activities and the overall project budgeting process. The VA IT Project Management Framework diagram illustrates Milestone 4 which occurs following the deployment of a system and the closing of the project. The project closing phase activities at the VA continues through system deployment and into system operation for the purpose of illustrating and describing the system activities the VA considers part of the project. The figure illustrates the actions and associated artifacts of the VA IT Project and Program Management process.

International standards

There have been several attempts to develop project management standards, such as:

Capability Maturity Model from the Software Engineering Institute.

GAPPS, Global Alliance for Project Performance Standards – an open source standard describing COMPETENCIES for project and program managers.

A Guide to the Project Management Body of Knowledge from the Project Management Institute (PMI)

HERMES method, Swiss general project management method, selected for use in Luxembourg and international organizations.

The ISO standards ISO 9000, a family of standards for quality management systems, and the ISO 10006:2003, for Quality management systems and guidelines for quality management in projects.

PRINCE2, PRojects IN Controlled Environments.

Association for Project Management Body of Knowledge

Team Software Process (TSP) from the Software Engineering Institute.

Total Cost Management Framework, AACE International's Methodology for Integrated Portfolio, Program and Project Management.

V-Model, an original systems development method.

The Logical framework approach, which is popular in international development organizations.

IAPPM, The International Association of Project & Program Management, guide to project auditing and rescuing troubled projects.

Project portfolio management

An increasing number of organizations are using, what is referred to as, project portfolio management (PPM) as a means of selecting the right projects and then using project management techniques as the means for delivering the outcomes in the form of benefits to the performing private or not-for-profit organization.

Project management software

Project management software has a capacity to help plan, organize, and manage resource pools and develop resource estimates. Depending the sophistication of the software, resource including estimation and planning, scheduling, cost control and budget management, resource allocation, collaboration software, communication, decision-making, quality management and documentation or administration systems. Today, numerous PC-based project management software packages exist, and they are finding their way into almost every type of business. Software may range from the high-end Microsoft Project to a simple spreadsheet in Microsoft Excel.

Virtual project management

Virtual program management (VPM) is management of a project done by a virtual team, though it rarely may refer to a project implementing a virtual environment It is noted that managing a virtual project is fundamentally different from managing traditional projects, combining concerns of telecommuting and global collaboration (culture, timezones, language)

Risk analysis is a technique to identify and assess factors that may jeopardize the success of a project or achieving a goal. This technique also helps to define preventive measures to reduce the probability of these factors from occurring and identify countermeasures to successfully deal with these constraints when they develop to avert possible negative effects on the competitiveness of the company.

One of the more popular methods to perform a risk analysis in the computer field is called facilitated risk analysis process (FRAP).

FRAP analyzes one system, application or segment of business processes at time.

FRAP assumes that additional efforts to develop precisely quantified risks are not cost effective because:

such estimates are time consuming

risk documentation becomes too voluminous for practical use

specific loss estimates are generally not needed to determine if controls are needed.

without assumptions there is little risk analysis

After identifying and categorizing risks, a team identifies the controls that could mitigate the risk. The decision for what controls are needed lies with the business manager. The team's conclusions as to what risks exists and what controls needed are documented along with a related action plan for control implementation.

Three of the most important risks a software company faces are: unexpected changes in revenue,

unexpected changes in costs from those budgeted and the amount of specialization of the software planned. Risks that affect revenues can be: unanticipated competition, privacy, intellectual property right problems, and unit sales that are less than forecast. Unexpected development costs also create risk that can be in the form of more rework than anticipated, security holes, and privacy invasions.

Narrow specialization of software with a large amount of research and development expenditures can lead to both business and technological risks since specialization does not necessarily lead to lower unit costs of software.Combined with the decrease in the potential customer base, specialization risk can be significant for a software firm. After probabilities of scenarios have been calculated with risk analysis, the process of risk management can be applied to help manage the risk.

Methods like applied information economics add to and improve on risk analysis methods by introducing procedures to adjust subjective probabilities, compute the value of additional information and to use the results in part of a larger portfolio management problem.

Risk analysis results and management plans should be updated periodically. There are two primary reasons for this:

- ✓ to evaluate whether the previously selected security controls are still applicable and effective
- ✓ to evaluate the possible risk level changes in the business environment. For example, information risks are a good example of rapidly changing business environment.

Limitations

Prioritizing the risk management processes too highly could keep an organization from ever completing a project or even getting started. This is especially true if other work is suspended until the risk management process is considered complete.

It is also important to keep in mind the distinction between risk and uncertainty. Risk can be measured by impacts x probability.

If risks are improperly assessed and prioritized, time can be wasted in dealing with risk of losses that are not likely to occur. Spending too much time assessing and managing unlikely risks can divert resources that could be used more profitably. Unlikely events do occur but if the risk is unlikely enough to occur it may be better to simply retain the risk and deal with the result if the loss does in fact occur. Qualitative risk assessment is subjective and lacks consistency. The primary justification for a formal risk assessment process is legal and bureaucratic.

Chapter 8

Risk Management For Megaprojects

Megaprojects (sometimes also called "major programs") are extremely large-scale investment projects, typically costing more than US$1 billion per project. Megaprojects include bridges, tunnels, highways, railways, airports, seaports, power plants, dams, wastewater projects, coastal flood protection schemes, oil and natural gas extraction projects, public buildings, information technology systems, aerospace projects, and defence systems. Megaprojects have been shown to be particularly risky in terms of finance, safety, and social and environmental impacts. Risk management is therefore particularly pertinent for megaprojects and special methods and special education have been developed for such risk management.

A megaproject is an extremely large-scale investment project. Megaprojects are typically defined as costing more than US$1 billion and attracting a lot of public attention because of substantial impacts on communities, environment, and budgets. Megaprojects can also be defined as "initiatives that are physical, very expensive, and public". Care in the project development process may be needed to reduce any possible optimism bias and strategic misrepresentation. The logic on which many of the typical mega-projects are built is on its collective benefits, for example electricity for everybody (who can pay), road access (for those that have cars), etc. Mega-projects have undergone a wide criticism for its top down planning process and for its ill effects on certain communities. From the 1960s on, mass mobilization took place against the building of inner city freeways in North America (for example in New York City, Toronto, Seattle, San Francisco), or nuclear power plants in the US and Germany, or proposal for new airports such as Mexico City in 2001. More recently, new types of mega-projects have been identified that no longer follow the old models of being singular and monolithic in their purposes, but now have become quite flexible and diverse, such as waterfront redevelopment schemes that seem to offer something to everybody. However, just like the old mega-project, the new ones also foreclose "upon a wide variety of social practices, reproducing rather than resolving urban inequality and disenfranchisement".Because of its plethora of land uses "these mega-projects inhibits the growth of oppositional and contestational practices".The collective benefits that are often the underlying logic of a mega-project, are here reduced to an individualized form of public benefit.

Megaprojects include bridges, tunnels, highways, railways, airports, seaports, power plants, dams, wastewater projects, Special Economic Zones, oil and natural gas extraction projects, public buildings, information technology systems, aerospace projects, weapons systems and, more recently, large-scale mixed use waterfront redevelopments; however, the most common megaprojects are in the categories of hydroelectric facilities, nuclear power plants and large public transportation projects.

Investing in megaprojects in order to stimulate the general economy has been a popular policy measure since the economic crisis of the 1930s. Recent examples are the 2008-2009 Chinese economic stimulus program, the 2008 European Union stimulus plan, and the American Recovery and Reinvestment Act of 2009.

his is a list of megaprojects, i.e., extremely large-scale investment projects. The number of such projects is so large that the list may never be fully completed.

Definitions

Megaprojects may be defined as:

Projects that cost more than US$1 billion and attract a lot of public attention because of substantial impacts on communities, environment, and budgets

Projects can also be "initiatives that are physical, very expensive, and public"

Megaprojects require care in the project development process to reduce any possible optimism bias and strategic misrepresentation. Examples of megaprojects include bridges, tunnels, highways, railways, airports, seaports, power plants, dams, wastewater projects, Special Economic Zones (SEZ), oil and natural gas extraction projects, public buildings, information technology systems, aerospace projects, and weapons systems.

This list identifies a wide variety of examples of major historic and contemporary projects that meet one or both megaproject criteria identified above.

Aerospace projects

Airbus A380, a double-deck, wide-body, four-engine jet airliner manufactured by Airbus, a subsidiary of EADS.

Airbus A350, a single deck, wide-body, two-engine, jet airliner produced by the European company Airbus. The A350 will be the first Airbus with both fuselage and wing structures made primarily of carbon fibre-reinforced polymer.

Antonov An-225 (1988), the longest and heaviest aircraft in the world in service.

Rockwell B-1 Lancer, a supersonic bomber with a variable-sweep wing built in the 1980s as a strategic bomber. It has since acquired conventional and multi-role capabilities.

Northrop Grumman B-2 Spirit, also known as the Stealth Bomber, a US heavy bomber with "low observable" stealth.

Boeing B-29 Superfortress, the first nuclear bomber, which cost 50% more than the development of the bombs in the Manhattan Project.

Boeing B-52 Stratofortress, the longest-running bomber program in the world with decades of service, one of the largest military aircraft ever built.

Boeing 2707 and Lockheed L-2000 supersonic aircraft projects, initiated in 1963 via a US government-funded competition to build the United States' first Supersonic Transport (SST), prototypes never built, ultimately canceled due to political, environmental and economic reasons in 1971.

Boeing 747, a wide-body commercial airliner first produced in 1970, often referred to by the nickname Jumbo Jet, is among the world's most recognizable aircraft.

Boeing 787, made in the United States with local and globally sourced parts, is the first major aircraft to be made largely out of composite materials

Concorde, a supersonic passenger airliner, a product of an Anglo-French government treaty that combined the manufacturing efforts of Aérospatiale and the British Aircraft Corporation, first flown in 1969, Concorde entered service in 1976 and continued commercial flights for twenty-seven years.

Eurofighter Typhoon, a twin-engine canard–delta wing multirole aircraft designed and built by a consortium of three separate partner companies -- Alenia Aeronautica, BAE Systems, and EADS—working through a holding company, Eurofighter GmbH, that was formed in 1986.

F-22 Raptor, a single seat, twin-engine fifth-generation fighter aircraft manufactured by Lockheed Martin that uses stealth technology.

Rafale, a French twin-engine delta-wing fighter aircraft designed and built by Dassault Aviation. The Rafale is a multirole combat aircraft capable of simultaneously undertaking air supremacy, interdiction, reconnaissance, and the airborne nuclear deterrent missions.

Sukhoi PAK FA/HAL FGFA, two variants of fifth-generation single and twin-engine stealth jet fighters jointly being developed by Sukhoi OKB and Hindustan Aeronautics Limited for the Russian and the Indian Air Forces, respectively.

F-35 Lightning II, a fifth-generation, single-seat, single-engine stealth multirole fighter manufactured by Lockheed Martin. Variants of the F-35 are planned to replace five classes of combat aircraft that are presently in use with roles as varied as close air support, tactical bombing, and air defense missions.

F/A-18 Hornet, a twin-engine supersonic, all-weather carrier-capable multirole fighter jet, designed to intercept air threats and attack ground targets.

KH-11 reconnaissance satellite, manufactured by Lockheed Corporation and launched between 1976 and 1990.

Saab JAS 39 Gripen, a Swedish 4.5 generation Multirole Jet Fighter developed by SAAB since 1978. Estimated project cost is 19 billion USD.

Tupolev Tu-144, the first supersonic transport aircraft, made by the Russian aircraft company Tupolev, first flown on 31 December 1968 and entered service on 26 December 1970.

Chengdu J-20, a fifth-generation, stealth, twin-engine fighter aircraft prototype developed by Chengdu Aircraft Industry Group for the Chinese People's Liberation Army Air Force (PLAAF).

Tusaş TFX (Turkey), a Fifth-generation jet fighter being developed by Turkish Aerospace Industries (TAI) with design assistance from Saab AB

Rail and rapid transit projects

Grand Central Terminal

Thessaloniki Metro map

Dubai Metro

Chicago Metro

Delhi Metro, New Delhi, India

Taiwan High Speed Rail, Taiwan, Republic of China

Tehran Metro, Tehran, Iran

Thessaloniki Metro, Thessaloniki, Greece. The initial stage of construction is set at 1.052 billion euro, or 1.5 billion dollars.

Toronto subway and RT, Toronto, Canada

Transcontinental railroads

The Big Move (succeeded Transit City), Greater Toronto Area, Canada

Vienna U-Bahn, Vienna, Austria

Metro Warszawskie, Warsaw, Poland

Washington Metro, Washington, D.C., United States

Bridge and highway projects

Rio–Antirrio bridge, Greece, Europe's largest cable-stayed bridge

Rio–Niterói bridge, Rio de Janeiro, Brazil

Roman road system of antiquity

Vasco da Gama Bridge, Portugal, Europe's largest bridge

WestConnex, Sydney, New South Wales, Australia

Verrazano-Narrows Bridge, New York City, United States

Woodrow Wilson Bridge, United States

Øresund Bridge and its connections on land, like the City Tunnel (Malmö), Sweden and Denmark.

Yavuz Sultan Selim Bridge İstanbul, Turkey

Algeria East-West Highway, Algeria

Science projects

Envisat, an Earth observation satellite of European Space Agency (2002–2012)

European Extremely Large Telescope,

European x-ray free electron laser, in Germany, plan operating in 2015.

Facility for Antiproton and Ion Research, in Germany (2012–)

India-based Neutrino Observatory

Spaceflight projects

Apollo Program Saturn V awaiting launch

Alpha Magnetic Spectrometer, a particle physics experiment module that is mounted on the International Space Station (2011–)

Apollo program (1960–1975)

Biak Space Port, Biak, Indonesia

International Space Station, multinational space station in low Earth orbit (1998–2020)

Mars Science Laboratory

Mir, Russian space station (1986–2001)

Dam and hydroelectric projects

Below are dam and hydroelectric projects throughout the world that produce significant amounts of electricity, irrigate large areas of land, create some of the world's largest man-made lakes or have had significant social, environmental, political implications that reached international dimensions. Being some of the most expensive, innovative and difficult engineering feats, these projects include some of the tallest and largest dams in the world.

The Hoover Dam, United States

The Three Gorges Dam, People's Republic of China

The Itaipu Dam, Brazil/Paraguay

Akosombo Dam, Ghana

Chapter 9

IT Risk Management

The IT risk management is the application of risk management to Information technology context in order to manage IT risk, i.e.:

The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise

IT risk management can be considered a component of a wider enterprise risk management system.

The establishment, maintenance and continuous update of an ISMS provide a strong indication that a company is using a systematic approach for the identification, assessment and management of information security risks.

Different methodologies have been proposed to manage IT risks, each of them divided in processes and steps.

According to Risk IT,it encompasses not just only the negative impact of operations and service delivery which can bring destruction or reduction of the value of the organization, but also the benefit\value enabling risk associated to missing opportunities to use technology to enable or enhance business or the IT project management for aspects like overspending or late delivery with adverse business impact.

Because risk is strictly tied to uncertainty, Decision theory should be applied to manage risk as a science, i.e. rationally making choices under uncertainty.

Generally speaking, risk is the product of likelihood times impact (Risk = Likelihood * Impact).

The measure of an IT risk can be determined as a product of threat, vulnerability and asset values:

Risk = Threat * Vulnerability * Asset

A more current Risk management framework for IT Risk would be the TIK framework: Risk = ((Vulnerability * Threat) / Counter Measure) * Asset Value at Risk IT Risk

Definitions

The Certified Information Systems Auditor Review Manual 2006 provides the following definition of risk management: "Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."

There are two things in this definition that may need some clarification. First, the process of risk management is an ongoing iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerability emerge every day. Second, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives.

The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real world threats. Most organizations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

Risk management in the IT world is quite a complex, multi faced activity, with a lot of relations with other complex activities. The picture show the relationships between different related terms.

National Information Assurance Training and Education Center defines risk in the IT field as:

The total process to identify, control, and minimize the impact of uncertain events. The objective of the risk management program is to reduce risk and obtain and maintain DAA approval. The process facilitates the management of security risks by each level of management throughout the system life cycle. The approval process consists of three elements: risk analysis, certification, and approval.

An element of managerial science concerned with the identification, measurement, control, and minimization of uncertain events. An effective risk management program encompasses the following four phases:

A Risk assessment, as derived from an evaluation of threats and vulnerabilities.

Management decision.

Control implementation.

Effectiveness review.

The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review.

The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. lt includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

Risk management as part of enterprise risk management

Some organizations have, and many others should have, a comprehensive Enterprise risk management (ERM) in place. The four objectives categories addressed, according to Committee of Sponsoring Organizations of the Treadway Commission (COSO) are:

Strategy - high-level goals, aligned with and supporting the organization's mission

Operations - effective and efficient use of resources

Financial Reporting - reliability of operational and financial reporting

Compliance - compliance with applicable laws and regulations

According to Risk It framework by ISACA, IT risk is transversal to all four categories. The IT risk should be managed in the framework of Enterprise risk management: Risk appetite and Risk sensitivity of the whole enterprise should guide the IT risk management process. ERM should provide the context and business objectives to IT risk management

Risk management methodology

The term methodology means an organized set of principles and rules that drive action in a particular field of knowledge. A methodology does not describe specific methods; nevertheless it does specify several processes that need to be followed. These processes constitute a generic framework. They may be broken down in sub-processes, they may be combined, or their sequence may change. However, any risk management exercise must carry out these processes in one form or another, The following table compare the processes foreseen by three leading standards. ISACA Risk IT framework is more recent. The Risk IT Practitioner-Guide compares Risk IT and ISO 27005.

Due to the probabilistic nature and the need of cost benefit analysis, the IT risks are managed following a process that accordingly to NIST SP 800-30 can be divided in the following steps:

Risk assessment,

Risk mitigation, and

Evaluation and assessment.

Effective risk management must be totally integrated into the Systems Development Life Cycle.

Information risk analysis conducted on applications, computer installations, networks and systems under development should be undertaken using structured methodologies.

Context establishment

This step is the first step in ISO ISO/IEC 27005 framework. Most of the elementary activities are foreseen as the first sub process of Risk assessment according to NIST SP 800-30. This step implies the acquisition of all relevant information about the organization and the determination of the basic criteria, purpose, scope and boundaries of risk management activities and the organization in charge of risk management activities. The purpose is usually the compliance with legal requirements and provide evidence of due diligence supporting an ISMS that can be certified. The scope can be an incident reporting plan, a business continuity plan.

Another area of application can be the certification of a product.

Criteria include the risk evaluation, risk acceptance and impact evaluation criteria. These are conditioned by:

Legal and regulatory requirements

The strategic value for the business of information processes

Stake holder expectations

Negative consequences for the reputation of the organization

Establishing the scope and boundaries, the organization should be studied: its mission, its values, its structure; its strategy, its locations and cultural environment. The constraints (budgetary, cultural, political, technical) of the organization are to be collected and documented as guide for next steps.

Organization for security management

The set up of the organization in charge of risk management is foreseen as partially fulfilling the requirement to provide the resources needed to establish, implement, operate, monitor, review, maintain and improve an ISMS. The main roles inside this organization are:

Senior Management

Chief information officer (CIO)

System and Information owners

the business and functional managers

the Information System Security Officer (ISSO) or Chief information security officer (CISO)

IT Security Practitioners

Security Awareness Trainers

Risk assessment

Risk Management is a recurrent activity that deals with the analysis, planning, implementation, control and monitoring of implemented measurements and the enforced security policy. On the contrary, Risk Assessment is executed at discrete time points (e.g. once a year, on demand, etc.) and – until the performance of the next assessment - provides a temporary view of assessed risks and while parameterizing the entire Risk Management process. This view of the relationship of Risk Management to Risk Assessment is depicted in figure as adopted from OCTAVE.

Risk assessment is often conducted in more than one iteration, the first being a high-level assessment to identify high risks, while the other iterations detailed the analysis of the major risks and other risks.

According to National Information Assurance Training and Education Center risk assessment in the IT field is:

A study of the vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. Managers use the results of a risk assessment to develop security requirements and specifications.

The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

An identification of a specific ADP facility's assets, the threats to these assets, and the ADP facility's vulnerability to those threats.

An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. The purpose of a risk assessment is to determine if countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level.

A management tool which provides a systematic approach for determining the relative value and sensitivity of computer installation assets, assessing vulnerabilities, assessing loss expectancy or perceived risk exposure levels, assessing existing protection features and additional protection alternatives or acceptance of risks and documenting management decisions. Decisions for implementing additional protection features are normally based on the existence of a reasonable ratio between cost/benefit of the safeguard and sensitivity/value of the assets to be protected. Risk assessments may vary from an informal review of a small scale microcomputer installation to a more formal and fully documented analysis (i. e., risk analysis) of a large scale computer installation. Risk assessment methodologies may vary from qualitative or quantitative approaches to any combination of these two approaches.

ISO 27005 framework

Risk assessment receives as input the output of the previous step Context establishment; the output is the list of assessed risks prioritized according to risk evaluation criteria. The process can divided in the following steps:

Risk analysis, further divided in:

Risk identification

Risk estimation

Risk evaluation

The ISO/IEC 27002:2005 Code of practice for information security management recommends the following be examined during a risk assessment:

Security policy,

Organization of information security,

Asset management,

Human resources security,

Physical and environmental security,

Communications and operations management,

Access control,

Information systems acquisition, development and maintenance, (see Systems Development Life Cycle)

Information security incident management,

Business continuity management, and

Regulatory compliance.

Risk identification

Risk identification states what could cause a potential loss; the following are to be identified:

Assets, primary (i.e. Business processes and related information) and supporting (i.e. hardware, software, personnel, site, organization structure)

Threats

Existing and planned security measures

Vulnerabilities

Consequences

Related business processes

The output of sub process is made up of:

list of asset and related business processes to be risk managed with associated list of threats, existing and planned security measures

list of vulnerabilities unrelated to any identified threats

list of incident scenarios with their consequences.

Risk estimation

There are two methods of risk assessment in information security field, qualitative and quantitative.

Purely quantitative risk assessment is a mathematical calculation based on security metrics on the asset (system or application). For each risk scenario, taking into consideration the different risk factors a Single loss expectancy (SLE) is determined. Then, considering the probability of occurrence on a given period basis, for example the annual rate of occurrence (ARO), the Annualized Loss Expectancy is determined as the product of ARO X SLE. It is important to point out that the values of assets to be considered are those of all involved assets, not only the value of the directly affected resource.

For example, if you consider the risk scenario of a Laptop theft threat, you should consider the value of the data (a related asset) contained in the computer and the reputation and liability of the company (other assets) deriving from the lost of availability and confidentiality of the data that could be involved. It is easy to understand that intangible assets (data, reputation, liability) can be worth much more than physical resources at risk (the laptop hardware in the example). Intangible asset value can be huge, but is not easy to evaluate: this can be a consideration against a pure quantitative approach.

Qualitative risk assessment (three to five steps evaluation, from Very High to Low) is performed when the organization requires a risk assessment be performed in a relatively short time or to meet a small budget, a significant quantity of relevant data is not available, or the persons performing the assessment don't have the sophisticated mathematical, financial, and risk assessment expertise required. Qualitative risk assessment can be performed in a shorter period of time and with less data. Qualitative risk assessments are typically performed through interviews of a sample of personnel from all relevant groups within an organization charged with the security of the asset being assessed. Qualitative risk assessments are descriptive versus measurable. Usually a qualitative classification is done followed by a quantitative evaluation of the highest risks to be compared to the costs of security measures.

Risk estimation has as input the output of risk analysis and can be split in the following steps:

Assessment of the consequences through the valuation of assets

Assessment of the likelihood of the incident (through threat and vulnerability valuation)

Assign values to the likelihood and consequence of the risks

The output is the list of risks with value levels assigned. It can be documented in a risk register

During risk estimation there are generally three values of a given asset, one for the loss of one of the CIA properties: Confidentiality, Integrity, Availability.

Risk evaluation

The risk evaluation process receives as input the output of risk analysis process. It compares each risk level against the risk acceptance criteria and prioritise the risk list with risk treatment indications.

NIST SP 800 30 framework

To determine the likelihood of a future adverse event, threats to an IT system must be in conjunction with the potential vulnerabilities and the controls in place for the IT system.

Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. The level of impact is governed by the potential mission impacts and produces a relative value for the IT assets and resources affected (e.g., the criticality sensitivity of the IT system components and data). The risk assessment methodology encompasses nine primary steps:

Step 1 System Characterization

Step 2 Threat Identification

Step 3 Vulnerability Identification

Step 4 Control Analysis

Step 5 Likelihood Determination

Step 6 Impact Analysis

Step 7 Risk Determination

Step 8 Control Recommendations

Step 9 Results Documentation

Risk mitigation

Risk mitigation, the second process according to SP 800-30, the third according to ISO 27005 of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission.

ISO 27005 framework

The risk treatment process aim at selecting security measures to:

Reduce

Retain

Avoid

Transfer

Risk and produce a risk treatment plan, that is the output of the process with the residual risks subject to the acceptance of management.

There are some list to select appropriate security measures, but is up to the single organization to choose the most appropriate one according to its business strategy, constraints of the environment and circumstances. The choice should be rational and documented. The importance of accepting a risk that is too costly to reduce is very high and led to the fact that risk acceptance is considered a separate process.]

Risk transfer apply were the risk has a very high impact but is not easy to reduce significantly the likelihood by means of security controls: the insurance premium should be compared against the mitigation costs, eventually evaluating some mixed strategy to partially treat the risk. Another option is to outsource the risk to somebody more efficient to manage the risk.

Risk avoidance describe any action where ways of conducting business are changed to avoid any risk occurrence. For example, the choice of not storing sensitive information about customers can be an avoidance for the risk that customer data can be stolen.

The residual risks, i.e. the risk reaming after risk treatment decision have been taken, should be estimated to ensure that sufficient protection is achieved. If the residual risk is unacceptable, the risk treatment process should be iterated.

NIST SP 800 30 framework

Risk mitigation is a systematic methodology used by senior management to reduce mission risk.

Risk mitigation can be achieved through any of the following risk mitigation options:

Risk Assumption. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level

Risk Avoidance. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)

Risk Limitation. To limit the risk by implementing controls that minimize the adverse impact of a threat’s exercising a vulnerability (e.g., use of supporting, preventive, detective controls)

Risk Planning. To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls

Research and Acknowledgement. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability

Risk Transference. To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities: this is the suggestion contained in

Risk communication

Risk communication is a horizontal process that interacts bidirectionally with all other processes of risk management. Its purpose is to establish a common understanding of all aspect of risk among all the organization's stakeholder. Establishing a common understanding is important, since it influences decisions to be taken.

Risk monitoring and review

Risk management is an ongoing, never ending process. Within this process implemented security measures are regularly monitored and reviewed to ensure that they work as planned and that changes in the environment rendered them ineffective. Business requirements, vulnerabilities and threats can change over the time.

Regular audits should be scheduled and should be conducted by an independent party, i.e. somebody not under the control of whom is responsible for the implementations or daily management of ISMS.

IT evaluation and assessment

Security controls should be validated. Technical controls are possible complex systems that are to tested and verified. The hardest part to validate is people knowledge of procedural controls and the effectiveness of the real application in daily business of the security procedures.

Vulnerability assessment, both internal and external, and Penetration test are instruments for verifying the status of security controls.

Information technology security audit is an organizational and procedural control with the aim of evaluating security. The IT systems of most organization are evolving quite rapidly. Risk management should cope with this changes through change authorization after risk re evaluation of the affected systems and processes and periodically review the risks and mitigation actions.

Monitoring system events according to a security monitoring strategy, an incident response plan and security validation and metrics are fundamental activities to assure that an optimal level of security is obtained.

It is important to monitor the new vulnerabilities, apply procedural and technical security controls like regularly updating software, and evaluate other kinds of controls to deal with zero-day attacks.

The attitude of involved people to benchmark against best practice and follow the seminars of professional associations in the sector are factors to assure the state of art of an organization IT risk management practice.

Integrating risk management into system development life cycle

Effective risk management must be totally integrated into the SDLC. An IT system's SDLC has five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. The risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC.

NIST SP 800-64 is devoted to this topic.

Early integration of security in the SDLC enables agencies to maximize return on investment in their security programs, through:

Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation;

Awareness of potential engineering challenges caused by mandatory security controls;

Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques; and

Facilitation of informed executive decision making through comprehensive risk management in a timely manner.

This guide focuses on the information security components of the SDLC. First, descriptions of the key security roles and responsibilities that are needed in most information system developments are provided. Second, sufficient information about the SDLC is provided to allow a person who is unfamiliar with the SDLC process to understand the relationship between information security and the SDLC. The document integrates the security steps into the linear, sequential (a.k.a. waterfall) SDLC. The five-step SDLC cited in the document is an example of one method of development and is not intended to mandate this methodology. Lastly, SP 800-64 provides insight into IT projects and initiatives that are not as clearly defined as SDLC-based developments, such as service-oriented architectures, cross-organization projects, and IT facility developments.

Security can be incorporated into information systems acquisition, development and maintenance by implementing effective security practices in the following areas.

Security requirements for information systems

Correct processing in applications

Cryptographic controls

Security of system files

Security in development and support processes

Technical vulnerability management

Information systems security begins with incorporating security into the requirements process for any new application or system enhancement. Security should be designed into the system from the beginning. Security requirements are presented to the vendor during the requirements phase of a product purchase. Formal testing should be done to determine whether the product meets the required security specifications prior to purchasing the product.

Correct processing in applications is essential in order to prevent errors and to mitigate loss, unauthorized modification or misuse of information. Effective coding techniques include validating input and output data, protecting message integrity using encryption, checking for processing errors, and creating activity logs.

Applied properly, cryptographic controls provide effective mechanisms for protecting the confidentiality, authenticity and integrity of information. An institution should develop policies on the use of encryption, including proper key management. Disk Encryption is one way to protect data at rest. Data in transit can be protected from alteration and unauthorized viewing using SSL certificates issued through a Certificate Authority that has implemented a Public Key Infrastructure.

System files used by applications must be protected in order to ensure the integrity and stability of the application. Using source code repositories with version control, extensive testing, production back-off plans, and appropriate access to program code are some effective measures that can be used to protect an application's files.

Security in development and support processes is an essential part of a comprehensive quality assurance and production control process, and would usually involve training and continuous oversight by the most experienced staff.

Applications need to be monitored and patched for technical vulnerabilities. Procedures for applying patches should include evaluating the patches to determine their appropriateness, and whether or not they can be successfully removed in case of a negative impact.

Critique of risk management as a methodology

Risk management as a scientific methodology has been criticized as being shallow. Major programs that implies risk management applied to IT systems of large organizations as FISMA has been criticized.

The risk management methodology is based on scientific foundations of statistical decision making: indeed, by avoiding the complexity that accompanies the formal probabilistic model of risks and uncertainty, risk management looks more like a process that attempts to guess rather than formally predict the future on the basis of statistical evidence. It is highly subjective in assessing the value of assets, the likelihood of threats occurrence and the significance of the impact.

Having considered this criticisms the risk management is a very important instrument in designing, implementing and operating secure information systems because it systematically classifies and drives the process of deciding how to treat risks. Its usage is foreseen by legislative rules in many countries. A better way to deal with the subject has not emerged.

Risk managements methods

It is quite hard to list most of the methods that at least partially support the IT risk management process. Efforts in this direction were done by:

NIST Description of Automated Risk Management Packages That NIST/NCSC Risk Management Research Laboratory Has Examined, updated 1991

ENISA in 2006; a list of methods and tools is available on line with a comparison engine. Among them the most widely used are:

CRAMM Developed by British government is compliant to ISO/IEC 17799, Gramm–Leach–Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA)

EBIOS developed by the French government it is compliant with major security standards: ISO/IEC 27001, ISO/IEC 13335, ISO/IEC 15408, ISO/IEC 17799 and ISO/IEC 21287

Standard of Good Practice developed by Information Security Forum (ISF)

Mehari developed by Clusif Club de la Sécurité de l'Information Français

Octave developed by Carnegie Mellon University, SEI (Software Engineering Institute) The Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE) approach defines a risk-based strategic assessment and planning technique for security.

IT-Grundschutz (IT Baseline Protection Manual) developed by Federal Office for Information Security (BSI) (Germany); IT-Grundschutz provides a method for an organization to establish an Information Security Management System (ISMS). It comprises both generic IT security recommendations for establishing an applicable IT security process and detailed technical recommendations to achieve the necessary IT security level for a specific domain

Enisa report classified the different methods regarding completeness, free availability, tool support; the result is that:

EBIOS, ISF methods, IT-Grundschutz cover deeply all the aspects (Risk Identification, Risk analysis, Risk evaluation, Risk assessment, Risk treatment, Risk acceptance, Risk communication),

EBIOS and IT-Grundschutz are the only ones freely available and

only EBIOS has an open source tool to support it.

The Factor Analysis of Information Risk (FAIR) main document, "An Introduction to Factor Analysis of Information Risk (FAIR)", Risk Management Insight LLC, November 2006; outline that most of the methods above lack of rigorous definition of risk and its factors. FAIR is not another methodology to deal with risk management, but it complements existing methodologies.

FAIR has had a good acceptance, mainly by The Open Group and ISACA.

ISACA developed a methodology, called Risk IT, to address various kind of IT related risks, chiefly security related risks. It is integrated with COBIT, a general framework to manage IT. Risk IT has a broader concept of IT risk than other methodologies, it encompasses not just only the negative impact of operations and service delivery which can bring destruction or reduction of the value of the organization, but also the benefit\value enabling risk associated to missing opportunities to use technology to enable or enhance business or the IT project management for aspects like overspending or late delivery with adverse business impact.

The "Build Security In" initiative of Homeland Security Department of USA, cites FAIR. The initiative Build Security In is a collaborative effort that provides practices, tools, guidelines, rules, principles, and other resources that software developers, architects, and security practitioners can use to build security into software in every phase of its development. So it chiefly address Secure coding.

Chapter 10

Risk management regarding natural disasters

It is important to assess risk in regard to natural disasters like floods, earthquakes, and so on. Outcomes of natural disaster risk assessment are valuable when considering future repair costs, business interruption losses and other downtime, effects on the environment, insurance costs, and the proposed costs of reducing the risk. There are regular conferences in Davos to deal with integral risk management.

Risk management techniques in petroleum and natural gas

For the offshore oil and gas industry, operational risk management is regulated by the safety case regime in many countries. Hazard identification and risk assessment tools and techniques are described in the international standard ISO 17776:2000, and organisations such as the IADC (International Association of Drilling Contractors) publish guidelines for HSE Case development which are based on the ISO standard. Further, diagrammatic representations of hazardous events are often expected by governmental regulators as part of risk management in safety case submissions; these are known as bow-tie diagrams. The technique is also used by organisations and regulators in mining, aviation, health, defence, industrial and finance.

Risk management as applied to the pharmaceutical sector

The principles and tools for quality risk management are increasingly being applied to different aspects of pharmaceutical quality systems. These aspects include development, manufacturing, distribution, inspection, and submission/review processes throughout the lifecycle of drug substances, drug products, biological and biotechnological products (including the use of raw materials, solvents, excipients, packaging and labeling materials in drug products, biological and biotechnological products). Risk management is also applied to the assessment of microbiological contamination in relation to pharmaceutical products and cleanroom manufacturing environments.

Protection of patient by managing risk in the quality systems and manufacturing process is being given prime importance in the pharmaceutical industry. Every product and every process associated with risks. It is important that product quality should be maintained throughout the product lifecycle.

In earlier days risk in the product quality and process had been assessed in the following informal ways.

Trends review

Check lists

Flow charts

Observations compilation

Changes review

Now the risk management approach initiated by regulatory agencies with recognized management tools along with support of statistical tools in combination, which make easy for application of quality risk management principles across the industry.

A Risk Management Program starts with identifying the possible risks associated with a product or with the process used to develop, manufacture, and distribute the product.An effective quality risk management ensures the high quality of drug product to the patient. Inaddition quality risk management improves decision making if a quality problem arises. It should include systemic processes designated to co-ordinate, facilitate and improve science-based decision-making with respect to risk.

The Fda’s Initiative On Risk Management Approach

The FDA defines a Risk Management as, “a strategic safety program designed to decrease product risk by using one or more interventions or tools.” The FDA proposes that: “…the sponsor of every product submitted for approval considers how to minimize risks from the product’s use. Risk management planning generally encompasses all efforts by a sponsor to minimize the risk from its product’s use and may include product labeling, risk assessment, pharmacovigilance, and special studies or interventions.”

The FDA expects the Risk management to follow a basic process of:

1. Learning about and interpreting a product’s benefits and risks,

2. Designing and implementing interventions to minimize a product’s risks,

3. Evaluating interventions in light of new knowledge that is acquired over time, and

4. Revising interventions when appropriate.

FDA Guideline

Learning about and interpreting a products benefits and risks

Designing and Implementing Interventions

Evaluating and Revising Interventions

Risk Management Elements

Risk and Issue Management Strategy, Risk Identification Technique, Risk Evaluation Technique.

Risk Response Planning, Risk and Issue Management Plan

Risk and Issue Management Plan

Risk Management Methods

To make risk-based decisions, a systematic approach is essential. The ICH Q9 guideline, Quality Risk Management, provides a structure to initiate and follow a risk management process. The following methods widely used in the industry for risk management.

Basic risk management facilitation methods (flowcharts, check sheets, etc.)

Failure Mode Effects Analysis (FMEA)

Failure Mode, Effects, and Criticality Analysis (FMECA)

Fault Tree Analysis (FTA)

Hazard Analysis and Critical Control Points (HACCP)

Hazard Operability Analysis (HAZOP)

Preliminary Hazard Analysis (PHA)

Risk ranking and filtering

Supporting statistical tools

	Method	Area of Application
	Basic risk management methods	Data organization to facilitate decision making in the areas of
	Flow charts/Process mapping, Check lists, Cause & Effect diagrams	Failure investigations
		Root cause analysis
	Failure Mode Effects Analysis (FMEA)	Equipments and facilities which are involved in the
	Failure Mode, Effects, and Criticality Analysis (FMECA)	Risks associated with manufacturing process
	Fault Tree Analysis (FTA)	Root cause analysis and failure investigation
	Hazard Analysis and Critical Control Points (HACCP	Monitoring of critical points not only in the manufacturing process but also in other lifecycle phase -
	Hazard Operability Analysis (HAZOP)	Manufacturing processes, evaluating process safety hazards
	Preliminary Hazard Analysis (PHA)	Analyzing existing systems or prioritizing hazards and commonly used early in the development
	Risk ranking and filtering	Prioritize manufacturing sites for inspection/audit by Regulators or industry, to evaluate both quantitatively-assessed and qualitatively-assessed risks within the same organizational framework.
	Supporting Statistical Tools	Data assessment

Four Major Components

The risk management program consists of four major components: risk assessment, risk control, risk review, and risk communication. All four components are essential. All the above methods should address the mentioned four basic components.

Team selection and method selection are also plays a vital role in the risk management process, so care should be taken while selection of risk management team and method.

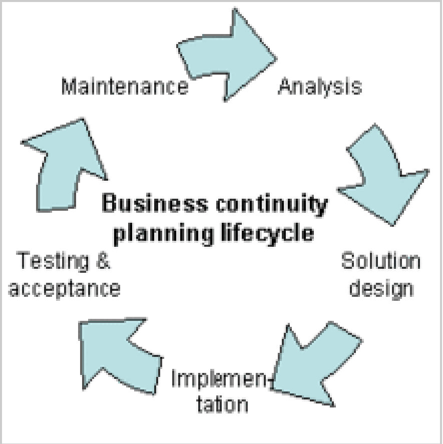
FMEA is the preferable method for risk management in the pharmaceutical industry as FMEA analysis include higher reliability, better quality, increased safety and its contribution towards cost saving includes decreased development time and reduced waste and non value added operations.

Chapter 11

Risk management and business continuity

Risk management is simply a practice of systematically selecting cost-effective approaches for minimising the effect of threat realization to the organization. All risks can never be fully avoided or mitigated simply because of financial and practical limitations. Therefore all organizations have to accept some level of residual risks.

Whereas risk management tends to be preemptive, business continuity planning (BCP) was invented to deal with the consequences of realised residual risks. The necessity to have BCP in place arises because even very unlikely events will occur if given enough time. Risk management and BCP are often mistakenly seen as rivals or overlapping practices. In fact these processes are so tightly tied together that such separation seems artificial. For example, the risk management process creates important inputs for the BCP (assets, impact assessments, cost estimates etc.). Risk management also proposes applicable controls for the observed risks. Therefore, risk management covers several areas that are vital for the BCP process. However, the BCP process goes beyond risk management's preemptive approach and assumes that the disaster **will** happen at some point.



Business continuity planning life cycle

Business continuity planning (BCP) "identifies an organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, while maintaining competitive advantage and value system integrity”. It is also called business continuity and resiliency planning (BCRP). A business continuity plan is a roadmap for continuing operations under adverse conditions such as a storm or a crime. In the US, governmental entities refer to the process as continuity of operations planning (COOP).

Any event that could impact operations is included, such as supply chain interruption, loss of or damage to critical infrastructure (major machinery or computing/network resource). As such, risk management must be incorporated as part of BCP

In December 2006, the British Standards Institution (BSI) released an independent standard for BCP — BS 25999-1. Prior to the introduction of BS 25999, BCP professionals relied on information security standard BS 7799, which only peripherally addressed BCP to improve an organization's information security procedures. BS 25999's applicability extends to all organizations. In 2007, the BSI published BS 25999-2 "Specification for Business Continuity Management", which specifies requirements for implementing, operating and improving a documented business continuity management system (BCMS).

Business continuity management is standardised across the UK by British Standards (BS) through BS 25999-2:2007 and BS 25999-1:2006. BS 25999-2:2007 business continuity management is the British Standard for business continuity management across all organizations. This includes industry and its sectors. The standard provides a best practice framework to minimize disruption during unexpected events that could bring business to a standstill. The document gives you a practical plan to deal with most eventualities – from extreme weather conditions to terrorism, IT system failure and staff sickness. (British Standards Institution, 2006)

This document was superseded in November 2012 by the British standard BS ISO22301:2012. (British Standards Institution, 2012)

In 2004, following crises in the preceding years, the UK government passed the Civil Contingencies Act 2004 (The Act). This provides the legislation for civil protection in the UK.

The Act was separated into two distinct parts: Part 1 focuses on local arrangements for civil protection, establishing a statutory framework of roles and responsibilities for local responders. Part 2 focused on emergency powers, establishing a modern framework for the use of special legislative measures that might be necessary to deal with the effects of the most serious emergencie.

The Act is telling responders and planners that businesses need to have continuity planning measures in place in order to survive and continue to thrive whilst working towards keeping the incident as minimal as possible. (Cabinet Office, 2004)

Analysis

The analysis phase consists of impact analysis, threat analysis and impact scenarios.

Business impact analysis (BIA)

A Business impact analysis (BIA) differentiates critical (urgent) and non-critical (non-urgent) organization functions/activities. Critical functions are those whose disruption is regarded as unacceptable. Perceptions of acceptability are affected by the cost of recovery solutions. A function may also be considered critical if dictated by law. For each critical (in scope) function, two values are then assigned:

Recovery Point Objective (RPO) – the acceptable latency of data that will not be recovered

Recovery Time Objective (RTO) – the acceptable amount of time to restore the function

The recovery point objective must ensure that the maximum tolerable data loss for each activity is not exceeded. The Recovery Time Objective must ensure that the Maximum Tolerable Period of Disruption (MTPoD) for each activity is not exceeded.

Next, the impact analysis results in the recovery requirements for each critical function. Recovery requirements consist of the following information:

The business requirements for recovery of the critical function, and/or

The technical requirements for recovery of the critical function

Threat and risk analysis (TRA)

After defining recovery requirements, each potential threat may require unique recovery steps. Common threats include:

Epidemic

Earthquake

Fire

Flood

Cyber attack

Sabotage (insider or external threat)

Hurricane or other major storm

Utility outage

Terrorism/Piracy

War/civil disorder

Theft (insider or external threat, vital information or material)

Random failure of mission-critical systems

The impact of an epidemic can be regarded as purely human, and may be alleviated with technical and business solutions. However, if people behind these plans are affected by the disease, then the process can stumble.

During the 2002–2003 SARS outbreak, some organizations grouped staff into separate teams, and rotated the teams between primary and secondary work sites, with a rotation frequency equal to the incubation period of the disease. The organizations also banned face-to-face intergroup contact during business and non-business hours. The split increased resiliency against the threat of quarantine measures if one person in a team was exposed to the disease.

Impact scenarios

After defining threats, impact scenarios form the basis of the business recovery plan. In general, planning for the most wide-reaching impact is preferable. A typical impact scenario such as "building loss" encompasses most critical business functions. A BCP may document scenarios for each building. More localized impact scenarios – for example loss of a specific floor in a building – may also be documented.

Recovery requirement

After the analysis phase, business and technical recovery requirements precede the solutions phase. Asset inventories allow for quick identification of deployable resources. For an office-based, IT-intensive business, the plan requirements may cover desks, human resources, applications, data, manual workarounds, computers and peripherals.

Other business environments, such as production, distribution, warehousing etc. will need to cover these elements, but likely have additional issues.

Solution design

The solution design phase identifies the most cost-effective disaster recovery solution that meets two main requirements from the impact analysis stage. For IT purposes, this is commonly expressed as the minimum application and data requirements and the time in which the minimum application and application data must be available.

Outside the IT domain, preservation of hard copy information, such as contracts, skilled staff or restoration of embedded technology in a process plant must be considered. This phase overlaps with disaster recovery planning methodology. The solution phase determines:

crisis management command structure

secondary work sites

telecommunication architecture between primary and secondary work sites

data replication methodology between primary and secondary work sites applications and data required at the secondary work site, and

physical data requirements at the secondary work site.

Implementation

The implementation phase involves policy changes, material acquisitions, staffing and testing.

Testing and organizational acceptance

The purpose of testing is to achieve organizational acceptance that the solution satisfies the recovery requirements. Plans may fail to meet expectations due to insufficient or inaccurate recovery requirements, solution design flaws or solution implementation errors. Testing may include:

Crisis command team call-out testing

Technical swing test from primary to secondary work locations

Technical swing test from secondary to primary work locations

Application test

Business process test

At minimum, testing is conducted on a biannual schedule.

The 2008 book Exercising for Excellence, published by The British Standards Institution identified three types of exercises that can be employed when testing business continuity plans.

Tabletop exercises

Tabletop exercises typically involve a small number of people and concentrates on a specific aspect of a BCP. They can easily accommodate complete teams from a specific area of a business.

Another form involves a single representative from each of several teams. Typically, participants work through simple scenario and then discuss specific aspects of the plan. For example, a fire is discovered out of working hours.

The exercise consumes only a few hours and is often split into two or three sessions, each concentrating on a different theme.

Medium exercises

A medium exercise is conducted within a "Virtual World" and brings together several departments, teams or disciplines. It typically concentrates on multiple BCP aspects, prompting interaction between teams. The scope of a medium exercise can range from a few teams from one organisation co-located in one building to multiple teams operating across dispersed locations. The environment needs to be as realistic as practicable and team sizes should reflect a realistic situation. Realism may extend to simulated news broadcasts and websites.

A medium exercise typically lasts a few hours, though they can extend over several days. They typically involve a "Scenario Cell" that adds pre-scripted "surprises" throughout the exercise.

Complex exercises

A complex exercise aims to have as few boundaries as possible. It incorporates all the aspects of a medium exercise. The exercise remains within a virtual world, but maximum realism is essential. This might include no-notice activation, actual evacuation and actual invocation of a disaster recovery site.

While start and stop times are pre-agreed, the actual duration might be unknown if events are allowed to run their course.

Maintenance

Biannual or annual maintenance cycle maintenance of a BCP manual is broken down into three periodic activities.

Confirmation of information in the manual, roll out to staff for awareness and specific training for critical individuals.

Testing and verification of technical solutions established for recovery operations.

Testing and verification of organization recovery procedures.

Issues found during the testing phase often must be reintroduced to the analysis phase.

Information/targets

The BCP manual must evolve with the organization. Activating the call tree verifies the notification plan's efficiency as well as contact data accuracy. Types of changes that should be identified and updated in the manual include:

Staffing

Important clients

Vendors/suppliers

Organization structure changes

Company investment portfolio and mission statement

Communication and transportation infrastructure such as roads and bridges

Technical

Specialized technical resources must be maintained. Checks include:

Virus definition distribution

Application security and service patch distribution

Hardware operability

Application operability

Data verification

Data application

Testing and verification of recovery procedures

As work processes change, previous recovery procedures may no longer be suitable. Checks include:

Are all work processes for critical functions documented?

Have the systems used for critical functions changed?

Are the documented work checklists meaningful and accurate?

Do the documented work process recovery tasks and supporting disaster recovery infrastructure allow staff to recover within the predetermined recovery time objective?

Chapter 12

Positive Risk

‘Managing risk positively’ is: weighing up the potential benefits and harms of exercising one choice of action over another, identifying the potential risks involved, and developing plans and actions that reflect

the positive potential and stated priorities of the service user. It involves using available resources and support to achieve the desired outcomes, and minimising the potential harmful outcomes. It is not negligent ignorance of the potential risks…it is usually a very carefully thought out strategy for managing a specific situation or set of circumstances.” For community based services, this means:

- ✓ empowering people
- ✓ working in partnership with adults who use services or direct their own support, family carers and advocates
- ✓ developing an understanding of the responsibilities of each party
- ✓ helping people to access opportunities and take worthwhile chances
- ✓ developing trusting working relationships
- ✓ helping adults who use services to learn from their experiences
- ✓ understanding the consequences of different actions
- ✓ making decisions based on all the choices available and accurate information
- ✓ being positive about potential risks
- ✓ understanding a person’s strengths
- ✓ knowing what has worked or not in the past
- ✓ where problems have arisen, understanding why
- ✓ ensuring support and advocacy is available to all users of services,
- ✓ particularly if things begin to go wrong for someone
- ✓ sometimes tolerating supported short-term risks in consultation with the service user, for long-term gains

Risk is generally assumed to have negative impact. However, a ‘risk’ can also have a positive impact. PMBOK 4/e talks of positive risks and calls them ‘opportunities’. Given that most project managers only have a passing knowledge of managing risks proactively (our industry still seems to reward crisis management notwithstanding the fact that most often people who fix a crisis were responsible for it in the first place!), it is extremely likely that most such opportunities are wasted.

A risk is just a future event with probability of occurance between 0% and 100%. If such probability is 100%, surely that is a certainty, and hence can be put on the plan. If it is 0%, again it is a certainty and hence you can plan accordingly. Risks are also known as ‘known unknowns’ because we know about those events – just that we don’t know what it exact outcome will be. So, it quite likely that the outcome could be positive, and need not always be negative. Sample the following examples of events that could have a positive impact:

You have made an offer to a manager whose company is fast running out of cash. The grapevine has it that they might not get any funding, and have just weeks before they fold up. If that happens, there is a strong likelihood that the manager whom you have made an offer will join you. Even though this is a negative event par se for that company, but for you, that is a positive event.

Your competitor initially undercut his prices and won the bid, but now he is in the danger of being disqualified on technical grounds. His loss means business for you, and hence that is a positive risk.

You offer “no-questions asked product replacement warranty” within 60 days of purchase. You allocate 5% of your your operating margin. Your new product has proved to be a great hit among teenages, and is flying off the shelves, and you expect that cost of product replacement might be within just 2%, thereby improving your overall profit margins on this product.

You need to arrive at airport on-time, and your commute is through the rush hour. You leave home well in-time, but it is tough and go. However, there is a football match that evening, and it is likely that you find the traffic very thin – possibly because most people are glued to their TV sets.

Your new software provides a workflow for managing personal finances. An NGO needs a low-cost software to manage its micro-finance product, but best-matching product is out of their reach. Your product *might* meet most of the requirements, including being in the budget, if only they can tweak their workflow a bit.

You are in construction business, and learn that government is toying with the proposal to reduce duties on cement and steel by 20%.

A major competitor who is also a large employer in the city is likely to announce lay-offs.

Because of an early delivery of an input component, you might be able to shave-off weeks from your delivery schedule.

City administration is likely to announce construction of a new flyover that will cut down city commute and decongest the downtown.

You are a tour operator and the international travel association is likely to name your region in "Top Ten Places to visit before you die" list.

Surely, these are simple examples, but demonstrate there are always positive risks in pretty much any project. However, we generally ignore them, and hence are not able to capitalize on them In addition to identifying positive risks, these four risk response strategies are identified to maximize the risk or impact of such positive risks:

Exploit - this strategy aims to eliminate the uncertainty associated with a particular upside risk by ensuring the opportunity definitely happens. Since this is a positive risk, the outcome is likely to be positive. However, there is an uncertainty to it, so if there is a way to eliminiate such uncertainty and make it a certainty, it ensures that you reap the benefits of such a positive risk. The idea is to virtually guarantee that a given risk becomes a certainty! Let's consider some examples:

Suppose you are developing a prototype. If your customer likes it, your order book could be full for next few years! You have been diligent so far, and now have the prototype ready a week before delivery date. You are 70% sure that the customer will like your prototype, but instead of deliverying early, you decide to subject the prototype to even more stringent testing and analysis. Ideally, you will want to raise such probability to 100%, but that might not always happen. However, you put all efforts to make such event a certainty.

Another example – you have to make product release next weekend – if that happens, your customer might be able to roll out new services to its customers.Â You pull out some of the best technical folks on other projects and put them on this task to ensure that it happens.

Your biggest customer might be willing to give you 2x, or even 3x business if only you stopped working for his biggest competitor. You take the call to stop working with the competitor and make that event happen.

Share - Sharing a positive risk involves allocating some or all of the ownership of the opportunity to a third party who is best able to capture the opportunity for the benefit of a project. Â Here, the idea is to involves more players who also becomes stakeholders so thatÂ collectively raise the winnings. This strategy might be handy for some types of risks that might have have a positive uncertainty, but chances are that by yourself, you might by constrained in how much you can win. By involving other complementary players, you not only push the envelope, you get others to the game, make the game bigger and help everyone win, thereby also maintaining your own interest.

You are building a cool product that you expect to be a best seller. However, you lack the product design or marketing expertize to fully explout this opportunity. Instead of home-growing those capabilities, you decide to get experts on this project who are fired up with this challenge.

Apple uses this extremely well. By making its iPhone APIs available to larger developer community, it has been able to ensure that there is a dedicated army of developers constantly working to create highly innovate apps. This has resulted in over 100,000 such apps being available on iPhone!

You have developed a new intellectual property that promises to be a revolution. Instead of patenting it, you decide to open-source it to create a major eco-system of other vendors who might get interested to develop tools and apps around that technology thereby pushing the envelope.

Enhance - the idea is to increase the probability or impact of a positive risk. Increasing probability might not make it a certainty, but does improve the chances of the positive event happening. Improving the impact might not be necessarily associated Â with an increase in the probability itself, but might lead to a higher yield should the event happen. Of course, there is also an opportunity to do both of them simultaneously!

Let’s assume there is a cloud cover over a drought-hit region and there is a 20% possibility of rain. What do you do? You can utilize scientific methods like cloud-seeding to improve the possibility of rain to, say, 40%. In this example, you can’t increase the impact, but you are able to increase the possibility of that event.

This strategy is used quite well by retailers, especially in apparels industry. Studies have shown that home labels (or we can just call them the unbranded stuff) has a higher chances of being bought when carefully placed alongside branded apparels than standalone. This simple placement trick increases the chances of customers picking up home labels.

Companies and industry trade association hire lobby firms to influence lawmakers and citizens to look at some important regulation more favorably, thereby maximising chances of its adoption and eventual success.

While pushing for a new idea, sometimes you want to socialize it with a key voice in the organization, or perhaps get some industry references that generally extol benefits of that idea, thereby increasing the chances that your idea gets accepted.

This story illutsrates a great example of how one can both increase the probability and the impact simultaneously. I blooged about it in a different context, but you can read the story Are you helping your competitors succeed?

Accept - Accepting the opportunity is being willing to take advantage of it if it comes along, but not actively pursuing it. When I earlier said most of us ignoreÂ positive risks, we probably work in a passive mode, and pick up those low-hanging fruits. While this might not be a bad idea, in some cases, you might not want to incur the cost of ensuring that a certain risk does happen. So, this is like a zero-cost effort where if the positive risk happens, you are willing to grab it.

For example, you have just started out your consulting venture and are busy doing the legwork for it, and don’t want to take up an assignment for the coming month lest it interferes with your initial preparations. You hear about a business in distress that needs exactly the kind of consulting that you are offering, but decide not to actively pursue it. However, when they call you up, you are willing to take the call.

A competitor is likely to go out of business and you might benefit when that happens, but you don’t want to be seen as a bad rival trying to accelerate his downfall. So, you decide to take it easy and monitor the situation, but when that happens, you gladly step in.

You want to take homeloan. There is a chance that interest rates will come down in the coming quarter. Instead of waiting for that to happen (or, it might not even happen), you decide to take the loan right now. If the interest rates go down, you benefit.

Identifying and exploiting positive risks doesn’t require any special talent, but it does require a systematic effort to spot such opportunities. While negative risks are typically more dangerous and hence it makes great sense to avoid, transfer or mitigate them, positive risks could make a significant difference to your project’s chances of success. As we see in these examples above, many of these opportunities will fly under your radar if not proactively pursued. A holistic risk management strategy should always consider all types of risks and identify appropriate responses.

Positive Risk Management

Positive Risk Management is an approach that recognizes the importance of the human factor and of individual differences in propensity for risk taking. It draws from the work of a number of academics and professionals who have expressed concerns about scientific rigor of the wider risk management debate, or who have made a contribution emphasizing the human dimension of risk.

Firstly, it recognizes that any object or situation can be rendered hazardous by the involvement of someone with an inappropriate disposition towards risk; whether too risk taking or too risk averse.

Secondly, it recognizes that risk is an inevitable and ever present element throughout life: from conception through to the point at the end of life when we finally lose our personal battle with life threatening risk.

Thirdly, it recognizes that every individual has a particular orientation towards risk; while at one extreme people may by nature be timid, anxious and fearful, others will be adventurous, impulsive and almost oblivious to danger. These differences are evident in the way we drive our cars, in our diets, in our relationships, in our careers.

Finally, Positive Risk Management recognizes that risk taking is essential to all enterprise, creativity, heroism, education, scientific advance – in fact to any activity and all the initiatives that have contributed to our evolutionary success and civilization. It is worth noting how many enjoyable activities involve fear and willingly embrace risk taking.

Within the entire Risk Management literature you will find little or no reference to the human part of the risk equation other than what might be implied by the term 'compliant'. This illustrates the narrow focus that is a hall mark of much current risk management practice. This situation arises from the basic premises of traditional risk management and the practices associated with health and safety within the working environment. There is a basic logic to the idea that any accident must reflect some kind of oversight or situational predisposition that, if identified, can be rectified. But, largely due to an almost institutionalized neglect of the human factor, this situationally focused paradigm has grown tendrils that reach into every corner of modern life and into situations where the unintended negative consequences threaten to outweigh the benefits.

Positive Risk Management views both risk taking and risk aversion as complementary and of equal value and importance within the appropriate context. As such, it is seen as complementary to the traditional risk management paradigm. It introduces a much needed balance to risk management practices and puts greater onus on management skills and decision making. It is the dynamic approach of the football manager who appreciates the offensive and defensive talents within the available pool of players. Every organisation has roles better suited to risk takers and roles better suited to the risk averse. The task of management is to ensure that the right people are placed in each job.

Positive Risk Management relies on the ability to identify individual differences in propensity for risk taking. The science in this area has been developing rapidly over the past decade within the domain of personality assessment. Once an area of almost tribal allegiance to different schools of thought, today there is wide spread consensus about the structure of personality assessment and its status within the framework of the cross disciplinary progress being made in our understanding of Human Nature. The Five Factor Model (FFM) of personality has been shown to have relevance across many different cultures, to remain consistent over adult working life and to be significantly heritable. Within this framework there are many strands which have a clear relationship to risk tolerance and risk taking. For example, Eysenck (1973) reports that personality influences whether we focus on what might go wrong or on potential benefits; Nicholson et al. (2005) report that higher extroversion is related to greater risk tolerance; McCrae and Costa (1997) link personality to tolerance of uncertainty, innovation and willingness to think outside the box; Kowert, 1997) links personality to adventurousness, imagination, the search for new experiences and actively seeking out risk. Building from these foundations of well validated assessment practices, more specialized assessments have been developed, including assessment of Risk Type.

Criticisms

However, researchers at the University of Oxford and King's College London found that the notion of complementarity may be a concept that does not work in practice. In a four-year organizational study of risk management in a leading healthcare organization, Fischer & Ferlie (2013) found major contradictions between rules-based risk management required by managers, and ethics-based self-regulation favoured by staff and clients. This produced tensions that led neither to complementarity nor to hybrid forms, but produced instead a heated and intractable conflict which escalated, resulting in crisis and organizational collapse.

The graveyard of former greats is littered with examples where the balance of risk went seriously awry; the ENRON and RBS stories have become iconic references in the pantheon of corporate governance and corporate mortality. Eastman Kodak might be a nominee for the opposite pole – the corporately risk averse.

Risk communication

Risk communication is a complex cross-disciplinary academic field. Problems for risk communicators involve how to reach the intended audience, to make the risk comprehensible and relatable to other risks, how to pay appropriate respect to the audience's values related to the risk, how to predict the audience's response to the communication, etc. A main goal of risk communication is to improve collective and individual decision making. Risk communication is somewhat related to crisis communication.

Seven cardinal rules for the practice of risk communication

(as expressed by the U.S. Environmental Protection Agency and several of the field's founders)

Accept and involve the public/other consumers as legitimate partners (e.g. stakeholders).

Plan carefully and evaluate your efforts with a focus on your strengths, weaknesses, opportunities, and threats (SWOT).

Listen to the stakeholders specific concerns.

Be honest, frank, and open.

Coordinate and collaborate with other credible sources.

Meet the needs of the media.

Speak clearly and with compassion.

Potential Areas For Risk Management Application

The following areas are identified as potential in the pharmaceutical industry for quality risk management application.

Documentation

Training

Quality defects

Audits

Periodic reviews

Change controls

Development reports

Facilities, Equipment and Utilities

Material management

Packaging and labeling

Conclusion

The use of a risk-based approach provides a consistent method for decision making which was easily associated with resource allocation and ensuring patient safety. Ultimately, applying risk management to pharmaceutical industry should reduce the number of threats or minimize their impact through the consistent use of the tools/methods and periodic review. The output of the risk management supports to the organization to meets the defined goals.

“The lesson content has been compiled from various sources in public domain including but not limited to the internet for the convenience of the users. The university has no proprietary right on the same.”

NIILM University

9, Km Milestone, NH-65, Kaithal - 136027, Haryana
Website: www.niilmuniversity.in