Assignment 4

Risk Management

Usama Sarwar

FA17-BS(CS)-090-B

Mr. Awais

PPIT (CSC110)

June 21, 2021

COMSATS University Islamabad

Sahiwal Campus

Table of Contents

Risk Management

1. Risk Management

Risk management is the identification, evaluation, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives) followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events [1] or to maximize the realization of opportunities.

Risks can come from various sources including uncertainty in international markets, threats from project failures (at any phase in design, development, production, or sustaining of life cycles), legal liabilities, credit risk, accidents, natural causes and disasters, deliberate attack from an adversary, or events of uncertain or unpredictable root-cause. There are two types of events i.e., negative events can be classified as risks while positive events are classified as opportunities. Risk management standards have been developed by various institutions, including the Project Management Institute, the National Institute of Standards and Technology, actuarial societies, and ISO standards.[2][3] 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.

Strategies to manage threats (uncertainties with negative consequences) typically include avoiding the threat, reducing the negative effect or probability of the threat, transferring all or part of the threat to another party, and even retaining some or all of the potential or actual consequences of a particular threat. The opposite of these strategies can be used to respond to opportunities (uncertain future states with benefits).

Certain risk management standards have been criticized for having no measurable improvement on risk, whereas the confidence in estimates and decisions seems to increase.[1]

1.1 Introduction

A widely used vocabulary for risk management is defined by ISO Guide 73:2009, "Risk management. Vocabulary."[2]

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. 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.

Opportunity cost represents a unique challenge for risk managers. It can be difficult to determine when to put resources toward risk management and when to use those resources elsewhere. Again, ideal risk management minimizes spending (or manpower or other resources) and minimizes the negative effects of risks.

Risk is defined as the possibility that an event will occur that adversely affects the achievement of an objective. Uncertainty, therefore, is a key aspect of risk. Systems like the Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management (COSO ERM) can assist managers in mitigating risk factors. Each company may have different internal control components, which leads to different outcomes. For example, the framework for ERM components includes Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Control Activities, Information and Communication, and Monitoring.

1.1.1 Method

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

1. Identify the threats.
2. Assess the vulnerability of critical assets to specific threats.

3. Determine the risk (i.e., the expected likelihood and consequences of specific types of attacks on specific assets)
4. Identify ways to reduce those risks.
5. Prioritize risk reduction measures.

1.1.2 Principles

The International Organization for Standardization (ISO) identifies the following principles of risk management:[4]

Risk management should:

- Create value – resources expended to mitigate risk should be less than the consequence of inaction.
- Be an integral part of organizational processes.
- Be part of decision-making process.
- Explicitly address uncertainty and assumptions
- Be a systematic and structured process
- 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

1.1.3 Mild Versus Wild Risk

Benoit Mandelbrot distinguished between "mild" and "wild" risk and argued that risk assessment and management must be fundamentally different for the two types of risk.[5] Mild risk follows normal or near-normal probability distributions, is subject to regression to the mean and the law of large numbers, and is therefore relatively predictable. Wild risk follows fat-tailed distributions, e.g., Pareto or power-law distributions, is subject to regression to the tail (infinite mean or variance, rendering the law of large numbers invalid or ineffective), and is therefore difficult or impossible to predict. A common error in risk assessment and management is to underestimate the wildness of risk, assuming risk to be mild when in fact it

is wild, which must be avoided if risk assessment and management are to be valid and reliable, according to Mandelbrot.

1.2 Process

According to the standard ISO 31000 "Risk management – Principles and guidelines on implementation,"[3] the process of risk management consists of several steps as follows:

1.2.1 Establishing the context

This involves:

1. observing the context
    - the social scope of risk management
    - the identity and objectives of stakeholders
    - the basis upon which risks will be evaluated, constraints.
2. defining a framework for the activity and an agenda for identification
3. developing an analysis of risks involved in the process
4. mitigation or solution of risks using available technological, human and organizational resources

1.2.2 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 consequenses.

- Source analysis[6] – 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).

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

- Problem analysis[*citation needed*] – 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[*citation needed*] – Organizations and project teams have objectives. Any event that may prevent an objective from being achieved 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.[7]
- Common-risk checking[8] – In several industries, lists with known risks are available. Each risk in the list can be checked for application to a particular situation.[9]
- Risk charting[10] – 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.

1.2.3 Assessment

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 an unlikely event, the probability of occurrence of which is unknown. 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 and is particularly scanty in the case of catastrophic events, simply because of their infrequency. 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 senior executives of the organization that the primary risks are easy to understand and that the risk management decisions may be prioritized within overall company goals. 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."[*vague*]

1.3 Risk options

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

1. Design a new business process with adequate built-in risk control and containment measures from the start.
2. Periodically re-assess risks that are accepted in ongoing processes as a normal feature of business operations and modify mitigation measures.
3. Transfer risks to an external agency (e.g. an insurance company)
4. Avoid risks altogether (e.g. by closing down a particular high-risk business area)

Later research[11] 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 (annualized loss expectancy) and compares the expected loss value to the security control implementation costs (cost-benefit analysis).

1.3.1 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:[12]

- Avoidance (eliminate, withdraw from or not become involved)
- Reduction (optimize – mitigate)
- Sharing (transfer – outsource or insure)
- Retention (accept and budget)

Ideal use of these risk control 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.

1.3.1.1 Risk avoidance

This includes not performing an activity that could present risk. Refusing to purchase a property or business to avoid legal liability is one such example. Avoiding airplane flights for fear of hijacking. Avoidance may seem like 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 favor of patients presenting with lower risk.[13]

1.3.1.2 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 effectively applying Health, Safety and Environment (HSE) management standards, organizations can achieve tolerable levels of residual risk.[14]

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 sharing strategy if the outsourcer can demonstrate higher capability at managing or reducing risks.[15] 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 center.

1.3.1.3 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 with the suffering/damage.

Methods 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.

1.3.1.4 Risk retention

Risk retention involves accepting the loss, or benefit of gain, from a risk when the incident 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 either they 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 to 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 that it would hinder the goals of the organization too much.

1.3.2 Risk management plan

Select appropriate controls or countermeasures to mitigate 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.

1.3.3 Implementation

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

1.3.4 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.

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

1. to evaluate whether the previously selected security controls are still applicable and effective

2. to evaluate the possible risk level changes in the business environment. For example, information risks are a good example of rapidly changing business environment.

1.4 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 × 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 is to be avoided. 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.

1.5 Areas

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, a traditional measure is the value at risk (VaR), but there also other measures like profit at risk (PaR) or margin 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.

In Information Technology, risk management includes "Incident Handling", an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. According to the SANS Institute,[16] it is a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

1.5.1 Contractual risk management

The concept of "contractual risk management" emphasises the use of risk management techniques in contract deployment, i.e. managing the risks which are accepted through entry into a contract. Norwegian academic Petri Keskitalo defines "contractual risk management" as

"a practical, proactive and systematical contracting method that uses contract planning and governance to manage risks connected to business activities".[17] In an article by Samuel Greengard published in 2010, two US legal cases are mentioned which emphasise the importance of having a strategy for dealing with risk:[18]

- UDC v. CH2M Hill, which deals with the risk to a professional advisor who signs an indemnification provision including acceptance of a duty to defend, who may thereby pick up the legal costs of defending a client subject to a claim from a third party,[19]
- Witt v. La Gorce Country Club, which deals with the effectiveness of a limitation of liability clause, which may, in certain jurisdictions, be found to be ineffective.[20]

Greengard recommends using industry-standard contract language as much as possible to reduce risk as much as possible and rely on clauses which have been in use and subject to established court interpretation over a number of years.[18]

1.5.2 Cultural property institutions (museums, libraries and archives)

1.5.3 Enterprise

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 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.

1.5.4 Enterprise Security

ESRM is a security program management approach that links security activities to an enterprise's mission and business goals through risk management methods. The security leader's role in ESRM is to manage risks of harm to enterprise assets in partnership with the business leaders whose assets are exposed to those risks. ESRM involves educating business leaders on the realistic impacts of identified risks, presenting potential strategies to mitigate those impacts, then enacting the option chosen by the business in line with accepted levels of business risk tolerance[21]

1.5.5 Medical device

For medical devices, risk management is a process for identifying, evaluating and mitigating risks associated with harm to people and damage to property or the environment. Risk management is an integral part of medical device design and development, production processes and evaluation of field experience, and is applicable to all types of medical devices. The evidence of its application is required by most regulatory bodies such as the US FDA. The management of risks for medical devices is described by the International Organization for Standardization (ISO) in ISO 14971:2019, Medical Devices—The application of risk

management to medical devices, a product safety standard. The standard provides a process framework and associated requirements for management responsibilities, risk analysis and evaluation, risk controls and lifecycle risk management. Guidance on the application of the standard is available via ISO/TR 24971:2020.

The European version of the risk management standard was updated in 2009 and again in 2012 to refer to the Medical Devices Directive (MDD) and Active Implantable Medical Device Directive (AIMDD) revision in 2007, as well as the In Vitro Medical Device Directive (IVDD). The requirements of EN 14971:2012 are nearly identical to ISO 14971:2007. The differences include three "(informative)" Z Annexes that refer to the new MDD, AIMDD, and IVDD. These annexes indicate content deviations that include the requirement for risks to be reduced *as far as possible*, and the requirement that risks be mitigated by design and not by labeling on the medical device (i.e., labeling can no longer be used to mitigate risk).

Typical risk analysis and evaluation techniques adopted by the medical device industry include hazard analysis, fault tree analysis (FTA), failure mode and effects analysis (FMEA), hazard and operability study (HAZOP), and risk traceability analysis for ensuring risk controls are implemented and effective (i.e. tracking risks identified to product requirements, design specifications, verification and validation results etc.). FTA analysis requires diagramming software. FMEA analysis can be done using a spreadsheet program. There are also integrated medical device risk management solutions.

Through a draft guidance, the FDA has introduced another method named "Safety Assurance Case" for medical device safety assurance analysis. The safety assurance case is structured argument reasoning about systems appropriate for scientists and engineers, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment. With the guidance, a safety assurance case is expected for safety critical devices (e.g. infusion devices) as part of the pre-market clearance submission, e.g. 510(k). In 2013, the FDA introduced another draft guidance expecting medical device manufacturers to submit cybersecurity risk analysis information.

1.5.6 Project management

Project risk management must be considered at the different phases of acquisition. In the beginning of a project, the advancement of technical developments, or threats presented by a

competitor's projects, may cause a risk or threat assessment and subsequent evaluation of alternatives (see Analysis of Alternatives). Once a decision is made, and the project begun, more familiar project management applications can be used:[22][23][24]

- 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.

1.5.7 Megaprojects (infrastructure)

Megaprojects (sometimes also called "major programs") are large-scale investment projects, typically costing more than $1 billion per project. Megaprojects include major 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 defense 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.[25]

1.5.8 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.[26][27] The Sendai Framework for Disaster Risk Reduction is a 2015 international accord that has set goals and targets for disaster risk reduction in response to natural disasters.[28] There are regular International Disaster and Risk Conferences in Davos to deal with integral risk management.

Several tools can be used to assess risk and risk management of natural disasters and other climate events, including geospatial modeling, a key component of land change science. This modeling requires an understanding of geographic distributions of people as well as an ability to calculate the likelihood of a natural disaster occurring.

1.5.9 Wilderness

The management of risks to persons and property in wilderness and remote natural areas has developed with increases in outdoor recreation participation and decreased social tolerance for loss. Organizations providing commercial wilderness experiences can now align with national and international consensus standards for training and equipment such as ANSI/NASBLA 101-2017 (boating),[29] UIAA 152 (ice climbing tools),[30] and European Norm 13089:2015 + A1:2015 (mountaineering equipment).[31][32] The Association for Experiential Education offers accreditation for wilderness adventure programs.[33] The Wilderness Risk Management Conference provides access to best practices, and specialist organizations provide wilderness risk management consulting and training.[34][35][36][37]

In his book, *Outdoor Leadership and Education*, climber, outdoor educator, and author Ari Schneider, notes that outdoor recreation is inherently risky, and there is no way to completely eliminate risk. However, he explains how that can be a good thing for outdoor education programs. According to Schneider, optimal adventure is achieved when real risk is managed and perceived risk is maintained in order to keep actual danger low and a sense of adventure high.[38]

The text Outdoor Safety - Risk Management for Outdoor Leaders,[39] published by the New Zealand Mountain Safety Council, provides a view of wilderness risk management from the

New Zealand perspective, recognizing the value of national outdoor safety legislation and devoting considerable attention to the roles of judgment and decision-making processes in wilderness risk management.

Risk Management for Outdoor Programs: A Guide to Safety in Outdoor Education, Recreation and Adventure,[40] published by Viristar, breaks down wilderness and experiential risk management into eight "risk domains" such as staff and equipment, and eleven "risk management instruments" such as incident reporting and risk transfer, before combining them all in a systems-thinking framework.[41]

One popular models for risk assessment is the Risk Assessment and Safety Management (RASM) Model developed by Rick Curtis, author of The Backpacker's Field Manual.[38] The formula for the RASM Model is: Risk = Probability of Accident × Severity of Consequences. The RASM Model weighs negative risk—the potential for loss, against positive risk—the potential for growth.

1.5.10 Information technology

IT risk is a risk related to information technology. This is a relatively new term due to an increasing awareness that information security is simply one facet of a multitude of risks that are relevant to IT and the real world processes it supports. "Cybersecurity is tied closely to the advancement of technology. It lags only long enough for incentives like black markets to evolve and new exploits to be discovered. There is no end in sight for the advancement of technology, so we can expect the same from cybersecurity."[42]

ISACA's *Risk IT* framework ties IT risk to enterprise risk management.

Duty of Care Risk Analysis (DoCRA)[43] evaluates risks and their safeguards and considers the interests of all parties potentially affected by those risks.

1.5.11 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 Health, Safety and

Environment (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** (see Network theory in risk assessment). The technique is also used by organisations and regulators in mining, aviation, health, defence, industrial and finance.

1.5.12 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.[44]

1.6 Risk communication

Risk communication is a complex cross-disciplinary academic field related to core values of the targeted audiences.[45][46] Problems for risk communicators involve how to reach the intended audience, how 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, but there are clear distinctions. Risk communication deals with possible risks and aims to raise awareness of those risks to encourage or persuade changes in behavior to relieve threats in the long term. On the other hand, crisis communication is aimed at raising awareness of a specific type of threat, the magnitude, outcomes, and specific behaviors to adopt to reduce the threat.[47] Some experts coincide that risk is not only enrooted in the communication process but also it cannot be dissociated from the use of language. Though each culture develops its own fears and risks, these construes apply only by the hosting culture.

Risk communication and community engagement (RCCE) is a method that draws heavily on volunteers, frontline personnel and on people without prior training in this area.[48]

2. References

1. Hubbard, Douglas (2009). The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons. p. 46.
2. ISO/IEC Guide 73:2009 (2009). Risk management — Vocabulary. International Organization for Standardization.
3. ISO/DIS 31000 (2009). Risk management — Principles and guidelines on implementation. International Organization for Standardization.
4. "Committee Draft of ISO 31000 Risk management" (PDF). International Organization for Standardization. 2007-06-15. Archived from the original (PDF) on 2009-03-25.
5. Mandelbrot, Benoit and Richard L. Hudson (2008). The (mis)Behaviour of Markets: A Fractal View of Risk, Ruin and Reward. London: Profile Books. ISBN 9781846682629.
6. "Risk Identification" (PDF). Comunidad de Madrid. p. 3.
7. CMU/SEI-93-TR-6 Taxonomy-based risk identification in software industry. Sei.cmu.edu. Retrieved on 2012-04-17.
8. "Risk Management Systems Checklist (Common Items)" (PDF). www.fsa.go.jpn.
9. Common Vulnerability and Exposures list. Cve.mitre.org. Retrieved on 2012-04-17.
10. Crockford, Neil (1986). An Introduction to Risk Management (2 ed.). Cambridge, UK: Woodhead-Faulkner. p. 18. ISBN 0-85941-332-2.
11. "CRISC Exam Questions". Retrieved 23 Feb 2018.
12. Dorfman, Mark S. (2007). Introduction to Risk Management and Insurance (9 ed.). Englewood Cliffs, N.J: Prentice Hall. ISBN 978-0-13-224227-1.
13. McGivern, Gerry; Fischer, Michael D. (1 February 2012). "Reactivity and reactions to regulatory transparency in medicine, psychotherapy and counseling" (PDF). Social Science & Medicine. 74 (3): 289–296. doi:10.1016/j.socscimed.2011.09.035. PMID 22104085.
14. IADC HSE Case Guidelines for Mobile Offshore Drilling Units 3.2, section 4.7
15. Roehrig, P (2006). "Bet On Governance To Manage Outsourcing Risk". Business Trends Quarterly.
16. SANS Glossary of Security Terms Retrieved on 2016-11-13
17. University of Tromsø, Contractual Risk Management (C-RM), accessed 6 January 2021
18. Greengard, S. (2010), The Difference Is in the Details, Engineering Inc., September/October 2010, pages 13-15

19. UDC–UNIVERSAL DEVELOPMENT, L.P., Cross–Complainant and Respondent, v. CH2M HILL, Cross–Defendant and Appellant, Court of Appeal, Sixth District, California, 15 January 2010, accessed 7 January 2021
20. State of Florida, Witt v. La Gorce Country Club, Third District Court of Appeal, 10 June 2009, accessed 6 January 2021
21. ASIS https://www.asisonline.org/publications--resources/news/blog/esrm-an-enduring-security-risk-model/
22. Lev Virine and Michael Trumper. Project Decisions: The Art and Science. (2007). Management Concepts. Vienna. VA. ISBN 978-1-56726-217-9
23. Lev Virine and Michael Trumper. ProjectThink: Why Good Managers Make Poor Project Choices. Gower Pub Co. ISBN 978-1409454984
24. Peter Simon and David Hillson, Practical Risk Management: The ATOM Methodology (2012). Management Concepts. Vienna, VA. ISBN 978-1567263664
25. Oxford BT Centre for Major Programme Management
26. Berman, Alan. Constructing a Successful Business Continuity Plan. Business Insurance Magazine, March 9, 2015. http://www.businessinsurance.com/article/20150309/ISSUE0401/303159991/constructing-a-successful-business-continuity-plan
27. Craig Taylor; Erik VanMarcke, eds. (2002). Acceptable Risk Processes: Lifelines and Natural Hazards. Reston, VA: ASCE, TCLEE. ISBN 9780784406236. Archived from the original on 2013-12-03.
28. Rowling, Megan (2015-03-18). "New global disaster plan sets targets to curb risk, losses | Reuters". Reuters. Retrieved 2016-01-13.
29. "American National Standard ANSI/NASBLA 101-2017: Basic Boating Knowledge--Human Propelled" (PDF). Retrieved 2018-11-01.
30. "UIAA Standard 152: Ice Tools" (PDF). Retrieved 2018-11-01.
31. "EN 13089 Mountaineering equipment - Ice-tools - Safety requirements and test methods (includes Amendment A1:2015)". Retrieved 2018-11-01.
32. "Irish Standard I.S.EN 13089:2011+A1:2015 Mountaineering equipment - Ice-tools - Safety requirements and test methods" (PDF). Retrieved 2018-11-01.
33. "Association for Experiential Education". Retrieved 2018-11-01.
34. "NOLS Risk Services". Retrieved 2018-11-01.
35. "Outdoor Safety Institute". Retrieved 2018-11-01.
36. "Viristar". Retrieved 2018-11-01.

37. "Adventure Risk Management". Retrieved 2018-11-01.
38. Schneider, Ari (23 May 2018). Outdoor Leadership and Education. ISBN 9781732348202.
39. Haddock (2013). Outdoor safety : risk management for outdoor leaders. Wellington, NZ: New Zealand Mountain Safety Council. ISBN 9780908931309.
40. Baierlein, Jeff (2019). Risk Management for Outdoor Programs: a Guide to Safety in Outdoor Education, Recreation and Adventure. Seattle, WA: Viristar LLC. ISBN 978-1733349116.
41. Jeff A. Baierlein (March 21, 2019). "Risk Management for Outdoor Programs: A Guide to Safety in Outdoor Education, Recreation and Adventure". Viristar.
42. Arnold, Rob (2017). Cybersecurity: A Business Solution. Threat Sketch. p. 4. ISBN 978-0692944158.
43. "Duty of Care Risk Analysis Standard (DoCRA)". DoCRA.
44. Saghee M, Sandle T, Tidswell E (editors) (2011). Microbiology and Sterility Assurance in Pharmaceuticals and Medical Devices (1st ed.). Business Horizons. ISBN 978-8190646741.
45. Risk Communication Primer—Tools and Techniques. Navy and Marine Corps Public Health Center
46. Understanding Risk Communication Theory: A Guide for Emergency Managers and Communicators. Report to Human Factors/Behavioral Sciences Division, Science and Technology Directorate, U.S. Department of Homeland Security (May 2012)
47. REYNOLDS, BARBARA; SEEGER, MATTHEW W. (2005-02-23). "Crisis and Emergency Risk Communication as an Integrative Model". Journal of Health Communication. 10 (1): 43–55. doi:10.1080/10810730590904571. ISSN 1081-0730. PMID 15764443. S2CID 16810613.
48. "Risk Communication and Community Engagement (RCCE) Considerations: Ebola Response in the Democratic Republic of the Congo". WHO. 2018. Retrieved 1 May 2020.