Risk management – an Introduction

The purpose of this document is to give an introduction to Risk management seen in a broad perspective. That is we do not limit ourselves to any sector (Financial, Shipping etc) but instead, we are focusing on defining the concept of Risk management.

What is Risk management?

Risk management is an activity directed towards the assessment, mitigating (to an acceptable level) and monitoring of risk[1]. Risks can come from:

- Accidents
- Natural causes
- Disasters

Risk management entails an organized activity to manage uncertainty and threats and involves people following procedures and using tools in order to ensure conformance with Risk management policies.

Risk management strategies include among other things transferring the risk to another party, avoiding the risk, reducing the (negative impact of the) risk, and accepting some or all of the consequences of any given risk.

Some traditional risk management programs (e.g., health risk assessment) are focused on risks stemming from physical or legal causes (e.g. natural disasters or fires, accidents, ergonomics, death and lawsuits), whereas Financial Risk management focuses on risks that can be managed using traded financial instruments[2].

Introduction

This section provides an introduction to the principles of risk management.

In ideal Risk management, a prioritization process is followed where the risks associated with the greatest loss 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 this process can be very difficult, and balancing between risks with a high

[1] Risk is a concept that denotes the probability of specific eventualities. Technically, the notion of risk is independent from the term of value and, as such, eventualities may have both beneficial and adverse (negative) consequences. However, in general usage the convention is to focus on only potential negative impacts to value that may arise from an uncertain future event, see Appendix A for more.
[2] For more see the document: “Financial Risk Management”.

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 risk - a risk that has a 100% probability of occurring but is ignored by the organization (or the indivual), for example due to a lack of identification ability. Death is a logical example, as it it certain to occur, the only question is when – and furthermore it is not transferable!

Another more tangible example is when deficient knowledge is applied to a situation, then a knowledge risk materialises. 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 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 while maximizing the reduction of the negative effects of risks.

Principles of Risk management[3]

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

- Risk management should create value
- Risk management should be an integral part of organizational processes
- Risk management should be part of decision making
- Risk management should explicitly address uncertainty
- Risk management should be systematic and structured
- Risk management should be based on the best available information
- Risk management should be tailored
- Risk management should take into account human factors
- Risk management should be transparent and inclusive
- Risk management should be dynamic, iterative and responsive to change
- Risk management should be capable of continual improvement and enhancement

[3] The main ISO standards on risk management include"Committee Draft of ISO 31000 Risk management", International Organization for Standardization.

The Risk management Process

The Risk management process should be an integral part of management, be embedded in culture and practices and tailored to the business processes of the organization.

The Risk management process include 6 activities:

1. Communication and consultation
2. Establishing of context
3. Identify risk
4. Risk assessment
5. Risk treatment
6. Monitoring and review

These activities will be described below.

1. Communication and consultation

An effective internal and external communication and consultation should take place in order to ensure that those accountable for implementing the Risk management process and the stakeholders understand the basis on which decisions are made, and the reason why particular actions are required.

2. Establishing the context

Establishing the context is concerned with developing a structure for the Risk identification and Risk assessment tasks that follows.

This step includes:

- Establishment of the organizational and project environment in which the Risk assessment is taking place
- Specifying the main objectives and the required outcomes
- Identifying the set of success criteria against which the consequences of the identified risks can be measured
- Defining the set of key elements for structuring the Risk identification and the Risk assessment process

Context inputs include key project documents, such as the project execution strategy, project charter, cost and schedule assumptions, scope definitions, engineering designs and studies, economic analyses, and any other relevant documentation about the project and its purpose.

The output from this stage is a concise statement of the project objectives and specific criteria for success, the objectives and scope for the Risk assessment itself, and a set of key elements for structuring the Risk identification process in the next stage.

3. Identify Risk

After having established the context, the next step in the process of Risk management is to identify potential risks areas. Risks are about events that when triggered cause problems (=losses). For that reason risk identification can start with the source of problems, or with the problem itself:

- **Source analysis** - Risk sources may be internal or external. Examples of risk sources are: stakeholders of a project, employees of a company and climate (like for example the weather over an airport, a typhoon in the path of an Oil Tanker or a tsunami)
- **Problem analysis** - Risks are related to identified threats[4]. For example: the threat of losing money, the threat of abuse of privacy information or the threat of accidents and casualties. The threats may exist with various entities, most important with shareholders, customers and legislative bodies such as the government

When either the Risk source or Risk problems has been identified, the events that a source may trigger or the events that can lead to a problem can be investigated – or more precisely needs to be investigated.

For example: stakeholders withdrawing during a project may endanger funding of the project; privacy information may be stolen by employees even within a closed network; lightning striking a Boeing 747 during takeoff may make all people onboard immediate casualties; pirates sizing a Bulk Carrier within the Gulf of Aden.

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[5]
- **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
- **Taxonomy-based risk identification** The taxonomy in taxonomy-based risk identification is a breakdown of possible risk sources. Based on the taxonomy and

[4] Risk associated with relevant but (mistakenly) unidentified threats is of course also quite important, one can only hope that this risk (if any) is negligible.
[5] Objective-based risk identification is at the basis of COSO's Enterprise Risk Management - Integrated Framework – for more please refer to the document: “Enterprise Risk Management”.

knowledge of best practices, a questionnaire is compiled. The answers to the questions reveal risks. Taxonomy-based risk identification in software industry can be found in CMU/SEI-93-TR-6[6]

- **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. An example of known risks in the software industry is the Common Vulnerability and Exposures list found at http://cve.mitre.org.
- **Risk charting (risk mapping)** This method combines the above approaches by listing:

    - Resources at risk
    - Threats to those resources
    - Modifying factors that can increase or decrease the risk
    - Consequences that it is of interest (=want) 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.

4. Risk assessment

Once risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. These quantities can be either simple to measure, in for example the case of the value of a lost building or the value of a sunken Bulk Carrier, 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 guesses possible in order to properly prioritize the implementation of the risk management plan.

The fundamental difficulty in Risk assessment[7] is determining the rate of occurrence since statistical information is not available on all kinds of past incidents[8]. Furthermore, evaluating the severity of the consequences (impact) can often be extremely difficult for immaterial assets. This imply that best educated opinions and available statistics – in these cases - are the primary sources of information. Nevertheless, Risk assessment should produce the kind of information for the management of the organization that:

- Makes risks easy to understand
- Allow Risk management decisions to be prioritized

[6] Please refer to: http://www.sei.cmu.edu/publications/documents/93.reports/93.tr.006.html for details.
[7] Risk assessment is the determination of quantitative or qualitative value of risk related to a specific situation and a recognized threat (also called hazard), for more see Appendix B.
[8] One example could be that prior to the stock-crash of October 1987, there was no observable smile/smirk in the market for equity-options.

There has been several theories and attempts to quantify risks. Numerous different risk formulae exist, but perhaps the most widely accepted formula for risk quantification is:

- ***Risk*** *is equal to* ***Rate of occurrence*** *multiplied by the* ***impact of the event***

Actually, 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.

5. Risk treatment

When first risk has been identified and assessed, there is a range of possible actions available. All the techniques to manage risk fall into one of the following 4 major categories:

1. Avoidance
2. Reduction (aka Mitigation)
3. Retention (aka Acceptance)
4. Transfer

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.

5.1.1. Risk avoidance

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 liability that comes with it. Another would be not flying in order to not 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.

Taking risk is a fundamental part of living, living without risking is not living, put in perspective the slogan for SAS[9] is “Who Dares Wins”.

5.1.2. Risk reduction

Involves methods that reduce the impact 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. Another example is the use of helmets when bicycling.

[9] See http://en.wikipedia.org/wiki/Special_Air_Service.

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. Recent software developments technique usely also includes automatic build and Q&A procedures, a good example is Agile software development[10].

Outsourcing could be an example of risk reduction if the outsourcer can demonstrate higher capability at managing or reducing risks. In this case companies outsource only some of their departmental needs. 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.

In finance, risk reduction is achived by hedging strategies, for more please refer to "Financial Risk Management".

5.1.3. Risk retention

This involves accepting the loss when it occurs. True or full 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. One example could be the (at least in Denmark) not to get a Collision Damage Waiver (kaskoforsikring) for your car if you are young (first time ensurer) and the car is old (=it has a low sales value).

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.

Furthermore, any amounts of potential loss (risk) over the amount that has been insured is by definition also retained risk. This may be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is deemed to expensive.

5.1.4. Risk transfer

This means causing another party to accept the risk, typically by contract or by hedging.

[10] Please refer to http://en.wikipedia.org/wiki/Agile_software_development for more information.

Insurance is one type of risk transfer that uses contracts. However, technically speaking, the buyer of the insurance contract generally retains the legal responsibility for the losses that has been transferred, meaning that insurance may – more accurately - be described 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[11].

Other times it may involve contract language that transfers a risk to another party without the payment of an insurance premium. Liability among construction or other contractors is very often transferred this way. On the other hand, in financial Risk management taking offsetting positions in derivative securities is a typical method[12].

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.

Creating a Risk management plan

One should select appropriate controls or countermeasures to measure each risk. Risk mitigation needs to be approved by the appropriate level in management. For example, 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 and decision on how to manage/control market risk in the portfolio should be under the authority of the CFO etc.

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. Another example, is that an overall insurance policy has to be implemented, which should be specified as a balance between the potential loss in case of a loss event and the cost for insurance[13].

A good risk management plan should contain a schedule for control implementation and responsible persons for those actions.

[11] However, in general it is not unusual that buying an insurance contract does not completely eliminate the risk that is associated with an accident (event), due to the compulsory excess.
[12] For more please refer to: ”Financial Risk Management”.
[13] That is a tradeoff between the 4 Risk assessment categories.

Implementation

With the planned method for mitigaing the effect of risks in place one should:

- 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
- 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 that allow for 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:

- To evaluate whether the previously selected risk (security) controls are still applicable, effective, relevant and sufficient, and
- To evaluate the possible risk level changes in the business environment

It is importance to recognize the fact that: ***Risk management is not a state but a process!***

Limitations

If risks are improperly assessed and prioritized, time can be wasted in dealing with risk of losses that are not likely to occur or if they occur are of no real relevance.

Spending too much time assessing and managing unlikely (or un-relevant) 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.

Prioritizing too highly the Risk management processes 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.

Lastly, it is also important to keep in mind the distinction between risk and uncertainty:

Risk can be measured by impacts x probability, that is risk is a function of uncertainty!

Areas of Risk management

Applied to corporate finance Risk management is the technique for measuring, monitoring and controlling the financial or operationel risk on a firm's balance sheet.

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

The Solvency II framework, is somewhat similar to the banking regulations Basel II, and is the set of regulatory requirements for insurance firms that operate in the European Union[14].

In enterprise Risk management[15], a risk is defined as a possible event or circumstance that can have negative influences on the whole 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, 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).

Risk management and business continuity

What is Risk management then:

- ***Risk management is simply a practice of systematically selecting cost effective approaches for minimising the effect of threat realization to the organization (or individual)***

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

[14] For more on financial Risk management please refer to the document: "Financial Risk Management".
[15] See the document: "Enterprise Risk Management".

have BCP in place arises because even very unlikely events will occur if given enough time[16].

Risk management and BCP are often mistakenly seen as rivals or overlapping practices. However, these 2 processes are in fact 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. For that reason Risk management covers several areas that are vital for the BCP process. However, the BCP process goes beyond Risk management's preemptive approach and moves on from the assumption that the disaster **will** realize at some point.

Claus Madsen
22. January 2009

[16] One example is the break-down of the U.S. sub-prime market in 2008 (http://en.wikipedia.org/wiki/United_States_housing_bubble), or the 1973 oil crisis (http://en.wikipedia.org/wiki/1973_oil_crisis).

Appendix A: The concept of Risk

There exist many different definitions of risk. One is that risk is an issue, which can be avoided or mitigated (wherein an issue is a potential problem that has to be fixed now.) Risk is described both qualitatively and quantitatively.

Qualitatively, risk is proportional to both the expected losses which may be caused by an event and to the probability of this event. Greater loss and greater event likelihood result in a greater overall risk.

In general we can define risk as follows[17]:

Risk = (Probability of Event Occuring) times (Impact of Event Occuring)

There are more sophisticated definitions, however. Measuring engineering risk is often difficult, especially in potentially dangerous industries such as nuclear energy. Often, the probability of a negative event is estimated by using the frequency of past similar events or by event-tree methods, but probabilities for rare failures may be difficult to estimate if an event tree cannot be formulated[18].

Financial risk[19] is often defined as the unexpected variability or volatility of returns and thus includes both potential worse-than-expected as well as better-than-expected returns. As with all risk calculations it is the worse-than-expected case that are the focus – or more generally the left tail (-distribution) of the return distribution.

In statistics, risk is often mapped to the probability of some event which is seen as undesirable. Usually, the probability of that event and some assessment of its expected impact needs to be combined into a believable scenario (an outcome), which combines the set of risk, regret and reward probabilities into an expected value for that outcome.

Risk versus Uncertainty

In his seminal work Risk, Uncertainty, and Profit, Frank Knight[20] (1921) established the distinction between risk and uncertainty.

" ... Uncertainty must be taken in a sense radically distinct from the familiar notion of Risk, from which it has never been properly separated. The term "risk," as loosely used in

---

[17] One of the first major uses of this concept was at the planning of the Delta Works in 1953, a flood protection program in the Netherlands, with the aid of the mathematician David van Dantzig (http://www.wired.com/science/planetearth/magazine/17-01/ff_dutch_delta?currentPage=3). The kind of risk analysis pioneered here has become common today in fields like nuclear power, aerospace and chemical industry.

[18] One of the failures of CDOs during the 2008- sub-prime crisis was among other things that the pricing method utilized for CDOs written on a portfolio of sub-primes loans was lacking data on the frequency of past credit events.

[19] For more please see the document: "Financial Risk Management".

[20] Please refer to: http://en.wikipedia.org/wiki/Frank_Knight.

everyday speech and in economic discussion, really covers two things which, functionally at least, in their causal relations to the phenomena of economic organization, are categorically different. ... The essential fact is that "risk" means in some cases a quantity susceptible of measurement, while at other times it is something distinctly not of this character; and there are far-reaching and crucial differences in the bearings of the phenomenon depending on which of the two is really present and operating. ... It will appear that a measurable uncertainty, or "risk" proper, as we shall use the term, is so far different from an unmeasurable one that it is not in effect an uncertainty at all. We ... accordingly restrict the term "uncertainty" to cases of the non-quantitive type. ”

A solution to this ambiguity is proposed in by Hubbard[21]:

- Uncertainty: The lack of complete certainty, that is, the existence of more than one possibility. The "true" outcome/state/result/value is not known
- Measurement of uncertainty: A set of probabilities assigned to a set of possibilities. Example: "There is a 60% chance this market will double in five years"
- Risk: A state of uncertainty where some of the possibilities involve a loss, catastrophe, or other undesirable outcome
- Measurement of risk: A set of possibilities each with quantified probabilities and quantified losses. Example: "There is a 40% chance the proposed oil well will be dry with a loss of $12 million in exploratory drilling costs"

In this sense, Hubbard uses the terms so that one may have uncertainty without risk but not risk without uncertainty. We can be uncertain about the winner of a contest, but unless we have some personal stake in it, we have no risk. If we bet money on the outcome of the contest, then we have a risk. In both cases there are more than one outcome. The measure of uncertainty refers only to the probabilities assigned to outcomes, while the measure of risk requires both probabilities for outcomes and losses quantified for outcomes.

Insurance and Economic Risk

Insurance can be considered as a risk-reducing investment in which the buyer pays a relative small fixed amount to be protected from a potential large loss.

Gambling on the other hand is a risk-increasing investment, wherein money is risked for a possible large return, but with the possibility of losing it all. Purchasing a lottery ticket is a very risky investment with a high chance of no return and a small chance of a very high return. In contrast, putting money in a bank at a defined rate of interest is a risk-averse action that gives a guaranteed return of a small gain and precludes other investments with possibly higher gain.

[21] For more see Hubbard (2007) "How to Measure Anything: Finding the Value of Intangibles in Business" page 46, John Wiley & Sons, 2007.

In finance, risk is the probability that an investment's actual return will be different than expected – or more precisely lower than expected. This includes the possibility of losing some or (in the extreme case) all of the original investment, for more please refer to “Financial Risk Management”.

Some industries manage risk in a highly quantified and numerate way. These include for example the nuclear power and aircraft industries, where the possible failure of a complex series of engineered systems could result in highly undesirable outcomes.

There can of course be thought of other examples, so the above constitutes as a few examples for different businesses/activities.

Appendix B: Risk Assessment

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.

Risk assessment consists of an objective evaluation in which assumptions and uncertainties are clearly considered and defined. One of the difficulties of Risk management is that the measurement of both of these quantities in which Risk assessment is concerned - potential loss and probability of occurrence - can be very difficult to measure.

The chance of error in the measurement of these two concepts is large – and in general to be expected. A 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.

Financial decisions, such as insurance, express loss in terms of 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[22]. For public health and environmental decisions, loss is normally 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".

Risk assessment in auditing

In auditing, Risk assessment is a very crucial stage before accepting an audit engagement.

According to ISA315 Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement, "the auditor should perform Risk assessment procedures to obtain an understanding of the entity and its environment, including its internal control."[23]

The main purpose of Risk assessment procedures is to help the auditor understand the audit client. Aspects like client's business nature, management structure and internal control system are good examples. The procedures will provide audit evidence relating to the auditor’s Risk assessment of a material misstatement in the client’s financial statements. Then, auditor obtains initial evidence regarding the classes of transactions at

[22] However that is to be defined!
[23] For more please refer to: http://www.aicpa.org/download/members/div/auditstd/SAS109.PDF.

the client and the operating effectiveness of the client's internal controls. In auditing, audit risk includes:

- Inherent risk
- Control risk
- Detection risk

Criticisms of quantitative Risk assessment

Nassim Nicholas Taleb[24] consider Risk managers little more than "blind users" of statistical tools and methods.

One example is the following 2006 quote from "The Black Swan"[25]:

"Globalization creates interlocking fragility, while reducing volatility and giving the appearance of stability. In other words it creates devastating Black Swans. We have never lived before under the threat of a global collapse. Financial Institutions have been merging into a smaller number of very large banks. Almost all banks are interrelated. So the financial ecology is swelling into gigantic, incestuous, bureaucratic banks – when one fails, they all fall. The increased concentration among banks seems to have the effect of making financial crisis less likely, but when they happen they are more global in scale and hit us very hard. We have moved from a diversified ecology of small banks, with varied lending policies, to a more homogeneous framework of firms that all resemble one another. True, we now have fewer failures, but when they occur ….I shiver at the thought.

The government-sponsored institution Fannie Mae, when I look at its risks, seems to be sitting on a barrel of dynamite, vulnerable to the slightest hiccup. But not to worry: their large staff of scientists deem these events "unlikely"."

[24] For more on Dr. Taleb, please refer to: http://en.wikipedia.org/wiki/Nassim_Nicholas_Taleb.
[25] Please see: http://www.fooledbyrandomness.com/imbeciles.htm.