Much of the pleasure in climbing is not in being in a dangerous situation, but being in an amazing, unlikely situation, and being in control, managing the risks through applying simple skills and strong teamwork.
www.planetfear.com

The Complete Risk Assessment and Management Cycle Applying Harvard University Global System™ Tools

Alain Paul Martin

1. Practical Definitions: Risk, Uncertainty and Risk Management

As the kernel of the mission of any business, good opportunities seldom come without challenges and risks. Indeed, risks are omnipresent and inherent in the pursuit of every goal, especially the lofty ones. Even in our daily lives, there is no risk-free environment. Today, there is more at risk than ever with the combined effect of the pace of change, competing priorities, scarce resources, conflicting interests, the might of technology and communications, health and environmental hazards including pathogens and pollutants (chemical, radiological, biological and nuclear), disasters, security threats, intolerance, conflict, crime, greed, safety and workplace issues (skills shortage, labor unrest, negligence, competency and commitment deficits). Risk is a complex subject. Let us start with a simple definition; then dig further to deal with the intricate issues of risk management.

Risk is a liability - an "**exposure to possible loss or injury**."[1] With respect to projects, we define risk as the adverse consequences (security, injury, loss of life, property damage, environmental degradation, social and economic disruption) of a probable event, situation, human activity, phenomenon or a cluster of events on project stakeholders and client objectives including delivery schedule, project budget, and deliverable performance (security, safety, reliability, regulatory acceptance, cost of maintenance and operations).

Bankers define risk as the potential loss from an event that translates into a **cash flow that differs from projections**. Although all major risks ultimately affect the value of a business, we differentiate between balance-sheet risks, which directly impact equity; operations risks, which affect earnings; and off-balance sheet risks, such as latent or contingent liabilities (environment, corporate restructuring and pension liabilities).

Risk requires the **uncertainty** and the **loss** associated with an event. Its magnitude is the product of the probability of an event (uncertainty) times the adverse consequences of such event (loss or consequence) on property (including intellectual property), people, organizations, communities (including countries) and ecosystems, in each of the risk **exposure pathways** (or hazardous zones).

Risk in zone ✍ over a specific time horizon = Loss x Probability of loss

With respect to zones or **exposure pathways**, the following questions are important: What "routes" may expose people, property and other valuable assets (such as the environment) to hazards (causative events)? Can the pathways be avoided to prevent risk? Is the exposure by voluntary choice? Who would be direct or indirect recipient or casualty?

Uncertainty is the absence of information about a phenomenon (an event, a project, a person, or a system). Two sources of uncertainty exist and can vary widely over time.

- ***Descriptive uncertainty*** is the inability to fully identify the assumptions or variables that govern an event, a value chain (defined below), a project or a policy.
- ***Measurement uncertainty*** is the inability to quantify these variables due to the imprecision of instruments, estimating techniques or resource allocation methods (Heisenberg Principle).

"In security risk management, the probability of loss (or frequency element) is separated into two parts as shown in the following equation:

Risk in zone ⁎ over a specific time horizon = Consequence x Threat x Vulnerability

Threat is a measure of the likelihood that a specific type of attack will be initiated against a specific target (i.e., a scenario). Vulnerability is a measure of the likelihood that various types of safeguards against a scenario will fail. Consequence is the magnitude of the negative effects, if the attack is successful."[2]

Security threats include espionage through several forms of intelligence (signals SIGINT, human HUMINT, imagery IMINT and measurement and signature MASINT). Security risk identification requires an extensive battery of analytic and counterintelligence tools including the above forms of intelligence collection, Factional Analysis, Psychographics, Power Scales, Issue/Threat Incubation Frameworks, social wiring diagrams, ePrecision Trees, malware and polymorphic detection algorithms.

2. The Dynamics between Risk, Opportunity and Hazardous Zones

2.1. Risk and Opportunity

The intricate relationship between opportunity and risk can be illustrated by thinking of a child climbing a high tree to pick fruits (opportunity). Staying closer to the trunk is relatively safer than venturing along the branches. But the harvest may be limited. Knowing how far to go to maximize opportunity without unduly over-reaching (risk) requires first awareness, then knowledge and hands-on skills, as well as a disciplined commitment. On a larger scale, innovation, specialization, teamwork and leadership are essential to increase productivity. Lacking these skills, many small business owners cannot maximize opportunity.

Part of that knowledge is to consider whether one should play the game or work to change its rules. Here, a good and stable step ladder, set on a firm level surface, can mitigate the risk of falling from the branches, but introduces other inherent dangers. A professional fruit-picking tool (innovation) eliminates the risk of falling altogether and can vastly increase the harvest (opportunity). At any rate, waiting for the oranges to fall to the ground is an option, but not for a resourceful and enterprising child!

2.2. Risk and Hazard

"The term risk is often confused with hazard. A high voltage power supply, a sample of radioactive metal, or a toxic chemical may present a hazard, meaning that they present the potential for harm. Concentrated acids, for example, clearly present the hazard to the user of serious burns if they are handled incorrectly.

The risk is the probability or chance that the hazard posed by the chemical will lead to injury. Thus, concentrated sulfuric acid is a hazardous chemical; because it is very corrosive and reactive. However, provided it is handled in an appropriate way the risks it poses may be small.

It is thus evident that hazards are associated with something we can do little about. The hazards posed by a carcinogen, a concentrated acid or an explosive substance, are inherent properties of the material. The risks they pose, however, can be (and should be!) minimized by initially preparing a suitable risk assessment, and then following the procedures laid down in that assessment."[3]

2.3. Risk, Hazardous Zones or Exposure Pathways, Bayesian Probabilities and the Pareto Distribution

Note also that a sure loss is not a risk. Thus, risk does not exist when the adverse consequences of an undesirable event are certain, namely when the probability is one; nor does risk exist when the probability is zero. Risk requires uncertainty (chance neither zero nor one) which results from the difficulty to predict the exact probability of a potential event and accurately assess its adverse consequences over various hazardous zones (or exposure pathways).[4]

Each hazardous zone reflects a different level of severity. In earthquakes, the Richter scale is used to measure severity. In a severe accident at a nuclear power plant, a severity of one is the maximum distance for minor injuries while 10 in severity is the lethal zone. In financial crime detection and prevention, hazardous zones can be defined from one for sporadic petty theft, to 10 in a consistent pattern of major systemic corruption, negligence or unfettered greed, that frequently results in receivership or bankruptcy (PG&E, Enron, Anderson, Global Crossing, WorldCom, South California Edison, Bear Stearns, Lehman Brothers, AIG).

The **Pareto distribution** applies to risk, particularly in security, health and safety. Severity zones 9 and 10 tend to suffer 80% of the loss. Furthermore, viewed from another perspective, the first few risks tend to have the potential to cause the majority of adverse consequences. As an example, the World Health Organization (WHO) substantiates, in its World Health Report titled *Reducing Risks, Promoting Healthy Life*, that "a relatively small number of risks cause a huge number of premature deaths." Specifically, the ten leading health risk factors globally "account for more than one third of all deaths worldwide".[5]

For threats that are plausible, but have never occurred, the frequency of occurrence of an event (i.e. its probability) is not available. Here, **Bayesian statistics**[6] can be applied to assign a degree of belief as a proxy for the probability distribution. This would have been helpful to assess the probability of 9/11 terrorist attacks prior to September 2001.

3. Risk Statements

Risk statements are drafted during the hazard-identification phase and finalized during the risk-assessment phase. Both phases are described in this paper.

"A risk statement's aim is to be clear, concise, and sufficiently informative that the risk is easily understood. Risk statements in standard format must contain two parts: the condition and the consequence. The condition/consequence format provides a complete picture of the risk, which is critical during mitigation planning. It is read as follows:

Given the <condition> there is a possibility that <consequence> will occur

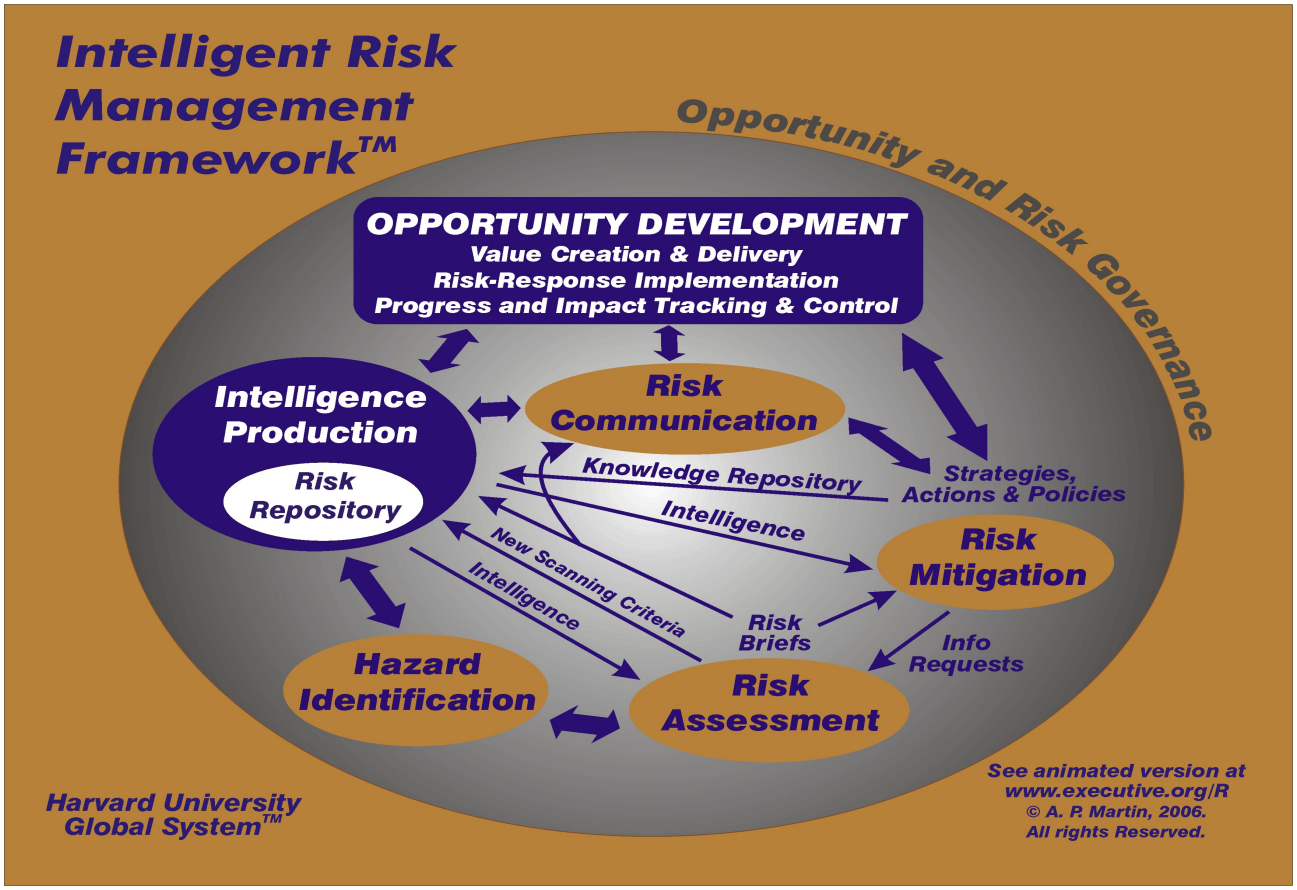
The condition component focuses on what is currently causing concern; it must be something that is true or widely perceived to be true. This component provides useful information when determining how to mitigate a risk. The consequence component focuses on the risk's intermediate and long-term impact. Understanding the depth and breadth of the impact is useful in determining how much time, resources, and effort should be allocated to the mitigation effort. A well-formed risk statement usually has only one condition, but may have more than one consequence… Since the risk statement is to be concise, a context is added to provide enough additional information about the risk to ensure that the original intent of the risk can be understood by other personnel, particularly after time has passed. An effective context captures the what, when, where, how, and why of the risk by describing the circumstances, contributing factors, and related issues (background and additional information not in the risk statement)."[7]

Examples	
Conditions	Adverse consequences
Changes or uncertainties in goals, deliverables; staff allocation, suppliers, weather, and client management; ill-defined or unsettled integration of deliverables; cryptic or imprecise communication; new or untested technology, workflow, or process; inadequate controls or attention to drivers of decision value; management complacency; unknown level of performance; competency deficits.	Safety hazards (accidents, injuries, loss of life), schedule slippage, cost overrun, property loss, fraud, sagging personnel morale, brain drain, deficient performance, resistance to change by users or other stakeholders, dissatisfaction or loss of clients, incomplete or cancelled projects, legal ramifications (breach of contract), damaged reputation, penalty imposition, higher insurance costs, restructuring.

4. Risk Management

Risk management is not risk avoidance which is frequently a sign of failure. Avoidance endangers the bottom line. Risk Management is at the heart of responsible conduct of professionals and managers. It addresses both the uncertainty and the loss described above.

Risk management addresses individual risks, their interdependencies and aggregate impact. As shown in Figure 1 and more precisely in the animation at www.executive.org/R, risk management involves six clusters of tasks:



1. **Risk Governance:** Defined below.
2. **Intelligence Production, and Threat and Hazard Identification:** Reduction of descriptive uncertainty by identifying the sources of risk, and assiduously grouping risks sharing similar characteristics (space, constituencies, process, value-chain elements)[8] to facilitate assessment.
3. **Risk Assessment, Estimation and Characterization:** Reduction of measurement uncertainty
4. **Risk Mitigation, Decision-making or Risk-Response Planning:** Strategies for prevention, reduction or acceptance of risk; contingency plans to deal with residual risk i.e. the risk that cannot be eliminated by reduction (worst-case scenario) and which must be addressed through damage-control measures. As an illustration, the risk of loss due to fire can be reduced by 90% by using fire-resistant building materials and design, enforcing construction codes, and clearing flammable vegetation too close to property. For the remaining 10% residual risk, it is vital to have fire insurance, uncluttered and workable escape doors, and good water pressure at the fire hydrant. Fire detectors and extinguishers must be operational, and roads accessible to accommodate fire trucks. Trained fire fighters and responsible homeowners are of paramount importance.[9]
5. **Risk-Response Implementation & Control:** Daily actions to prevent, transfer, share or mitigate risk; manage adverse consequences of uncertainty; and evaluate progress and impact (results).
6. **Risk Communication:** Discussed below.

5. Risk Governance

Risk governance is the set of explicit mechanisms (rules, processes, responsibilities, accountability and organization structure) for policy formulation, disclosure and decision-making about risk, at various levels of gravity, affecting the organization and its stakeholders throughout the business value chain, both under normal and emergency situations. It calls for identifying risks early in the project life cycle before resource mobilization. It defines overall responsibility and accountability, and establishes the strategic corridor of navigation and operational boundaries to maximize opportunity without undue exposure to risk. For this purpose, the leadership formulates the best policies, standards, as well as the required capabilities (talent and other resources) to determine risk tolerances, manage both real and perceived risks, assess the risk governance framework and continually improve risk management knowledge and performance. The leadership also develops policies to (a) prevent, detect and deter inappropriate conduct; (b) reward outstanding contributions to risk management (including risk education and risk communication). The reward portfolio should be a fraction of the accrued net aggregate benefits (gains and savings) attributable to risk management.

At the corporate level, a chief risk-management officer (CRO) leads the exercise, monitors aggregate risk, and act as a watchdog for the board.

Risk governance is covered in my graduate seminar and is beyond the current scope of our workshop.

6. Intelligence Production and Threat Identification

Risk management is a wishful thinking without solid current intelligence to identify risks long before they emerge as a problem, and to shrink the gaps in risk knowledge. The first phase, intelligence production is the set of tasks to continually scan for, and clearly **identify and characterize hazards** i.e. the causes for potential loss or injury, cost overruns, missed deadlines, security and environmental threats (mercury emissions, oil spills, PCB discharge from capacitors), resistance to change, or other undesirable consequences. This phase also involves locating who and what may be exposed to these consequences: people, property (physical, financial, intellectual, and virtual), the environment, partners (clients, supply chain, owners), and public trust.

- **Risk Repository**

Good intelligence production requires a **centralized repository** of strategic and operational hazards (problems and losses) including their respective contexts, individuals involved, and other risk agents. The best repositories also capture the lessons, or risk knowledge, derived from each case or cluster of cases. They cross-reference the entries to risk mitigation situations and risk management literature available elsewhere (e.g. power outage and sharing through rolling blackouts).

In banking, credit-rating repositories help communicate risk, speed up the diagnosis of common causes, and prevent repetitive situations across organizations. The Basel II Charter requires European banks to maintain a central repository for tracking and measuring operational risk.

- **Hazard Identification and Risk Breakdown Structure (RBS)**

Hazard identification is, according to the European Commission, "the identification of risk sources capable of causing adverse effects/events to human or environmental species, together with a qualitative description of the nature of these effects/events."[10]

The causes may be incubated by markets (currency, credit or commodity risk), people (intentionally, accidentally, incidentally) or by nature (lightning). The frequency could be continuous (constant or varying level), or discrete (singular or multiple of a sequential, repetitive or of combinatorial nature).

Most risk management professionals identify hazards and related risks through brainstorming, peer reviews, survey questionnaires and by scouring internal, public and syndicated risk repositories. The ability to connect the dots of a potential risk long before it emerges is paramount to management. Our approach capitalizes on the best available practices. Furthermore, it helps in the discovery of previously unknown risks through a structured intelligence-collection framework which addresses seven specific areas. Together, the areas form the building blocks for a hierarchical risk breakdown structure (RBS).

In order to avoid omissions in risk identification, the following **Risk Breakdown Structure** considers both internal and external elements of a project. It helps provide a depth of identification coverage both in terms of risk quality and quantity. It should be validated, namely benchmarked against, and complemented with, other risk taxonomies,[11] particularly in cases involving catastrophic risks.

1. Value-Chain and Business-Model Risks, and Grey Areas
2. Risk-Incubation or Pre-Project Innate Risks
3. Stakeholder-Related Risks (SRR)
4. Responsibility and Accountability Risks
5. Project Implementation Risks
6. Transition & Commissioning Risks
7. Balance-Sheet and Off Balance-Sheet Risks.

By working with these seven risk-intelligence sources, we endeavor to produce a project-based cumulative risk assessment from dominant contributors.

Here, **cumulative risk** is defined as the combined risk to the entire enterprise from aggregate exposure to multiple sources, agents and stressors.[12]

"**Dominant contributors** are those accident/intentional sequences, starting from the highest risk in terms of quantified values, that, when summed, encompass a majority (usually over 90%) of the risks associated with the given facility or system being analyzed. For example, loss of off-site power combined with the failure of the emergency diesel generators have been shown to be dominant contributors at some boiling water reactors in nuclear facilities."[13] The dominant contributors of intellectual property risks tend to be negligent use of Web publishing combined with inadequately trained staff (or third parties like civil servants) unknowingly facilitating the intelligence collection work of foreign jurisdictions and competitors, both masquerading as friendly allies or potential clients.

6.1. Value-Chain and Business-Model Risks, and Grey Areas

Opportunity identification and planning begin with the definition of the building blocks of the business model or value chain (or value stream). This chain describes the value-creation process (see Figure 2). It consists of a of a means-ends hierarchy.

Execution (or implementation) starts from the mobilization of resources necessary to make the deliverables (products & services), that are in turn required to meet the goals and objectives (expressed in benefits), which are ultimately indispensable for the mission, at the other end of the chain. Missions are based on values, namely what matters most to the leadership of the organization.

Unlike implementation, the planning and strategy formulation exercise is firstly about defining the means of value creation by going backward along the chain. Starting from the ultimate business purpose or organization mission, we define a balanced portfolio of objectives (or goals). Each objective requires end products and services (or deliverables or outputs).[14] Using the concept of **work breakdown structure (WBS)**, each product is further decomposed into tiers of deliverables (systems or sub-assemblies), and so on down to the twigs, i.e. the level of detail where work packages and activities can be crafted. The WBS exercise facilitates the mobilization and allocation of resources at the beginning of the value chain.

Figure 2: Business Model or Value Chain (Value Stream or Means-End Chain)

A good way to reduce planning and strategy-formulation omissions and improve the project value chain is to close the loop by going forward, from left to right in Figure 2, to ensure that:

- All indispensable **resources** and **activities** for the creation of the deliverables (products and services) have been identified and none were overlooked;
- The **products and services** specified are necessary and sufficient to reach the defined objectives;
- Chosen from a number of alternatives, the **objectives** are a pre-requisite for fulfilling the **mission.** They also fit and work together in the organization's overall balanced portfolio of objectives that are necessary to accomplish the mission

This concept is useful in planning particularly in the search for better ways to achieve objectives.

- **Making Assumptions Explicit**

While crafting the value chain and business model; the project team determines simultaneously, at each element of the means-ends hierarchy, the **assumptions** or **grey areas** as the key to the identification of risks related to the value chain. A peer review can validate the teamwork and help uncover neglected assumptions and risk sources especially the high-consequence low-probability hazards and events. It is also essential in mission-critical projects.

Here, an **assumption** is defined as a condition beyond a decision-maker's control, but which must exist in order for a means to yield an end in each of the means-end stages. Each stage is represented by the four horizontal and successive east-bound arrows in Figure 3 below.

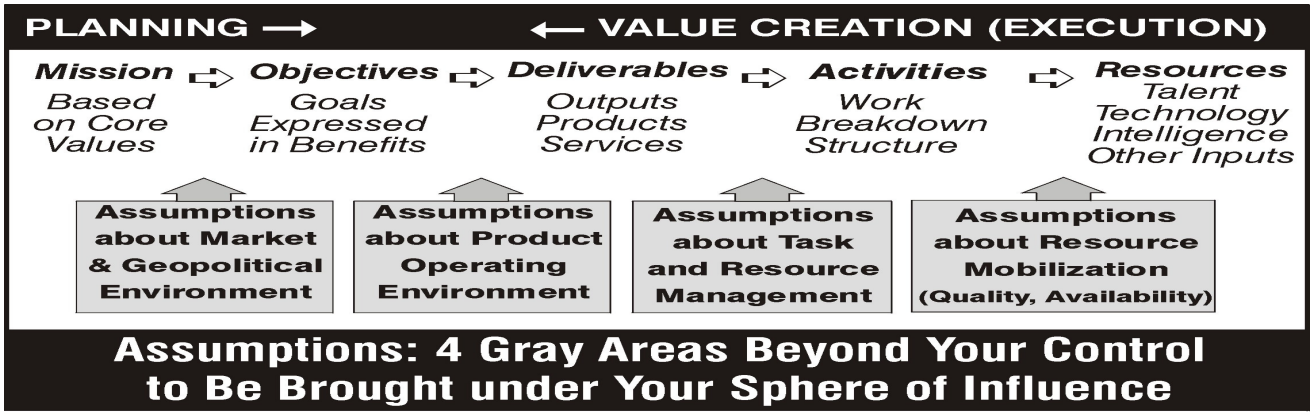


Figure 3: Gray Areas or Assumptions Required for Risk Identification

- **Peeling the Assumption Onion**

This comprehensive representation features four levels of assumptions (gray areas) directly related to the value chain of the project, policy, pilot experiment or business unit under your responsibility:

1. **Resource-Mobilization Assumptions:** At the resource level, assumptions about resource mobilization must be met for work to start. Assumptions about intelligence validity, materials delivered on time, and funding adequacy and timeliness should be made explicit. Also important are the availability, competence, and reliability of the performers. The reliability, limits, maturity and complexity of technology cannot be ignored. Scrutinize projects integrating systems and components independently developed by providers, as acknowledged in the inset below.

> "Software is not manufactured from scratch, but is made from a set of integrated components. We no longer make database management systems, message brokers, search engines, product data management systems, web servers, browsers, etc. Each of these components is developed by vendors, who are under pressure to continually upgrade and enhance their products. Each component has its quirky operations, which change with each version. This destroys chances for stable interfaces, as standards usually are behind the latest "sexy" innovations… Additionally, the way each set or "ensemble" of components is used changes radically depending on our individual needs. We can use a DBMS for data warehousing, e-commerce, configuration management, etc. When combining these sets of components into an "ensemble" of components, nobody, including the component developers, have a clue how they will work… This means that even if we clearly define the requirements as stated in CMM[15], and then fully document the design, we have not addressed the real risk that arises: ***the integration issues associated with combining varied and unstable components.*** It also means we need a cadre of knowledgeable specialists to problem solve the issues associated with component integration… The primary function of system architects should be risk mitigators: they need to engage in exploration and discovery to get a sense of the potential problems prior to deciding on a set of components."[16]

2. **Task-Level Assumptions:** Similarly, we cannot deliver expected products and services unless some assumptions about activities, task management and resource allocation materialize. Good management, no accidents at work, and productive teams and culture, are among the necessary preconditions to integrate resources and turn out the right mix of deliverables. These assumptions about valid **work processes and practices** are a must, especially in IT projects such as the commercially-driven component-based software development. Here, "the focus is on building an interface and behavior set that is validated through iterative usability testing prior to building a line of code. While building the interface and behavior to validate exact requirements, architects can be engaging in exploration and discovery to identify and mitigate potential integration risks. This approach will lead to better-used systems while more closely meeting cost and schedule goals. While more upfront time is spent, it is now planned for."[17]
3. **Product/Service Operating Environment Assumptions:** By the same token, the mere presence of the products is a necessary but not a sufficient prerequisite to achieve the **objectives or goals** unless some assumptions about the product-operating environment hold. One assumption is that the users will be adequately trained to deliver the service and operate the system or products safely and effectively. In a large number of day-to-day operations, "no lightning" is a necessary assumption to trigger operational risk identification. The assumptions about performance requirements (scope uncertainty, ill-defined requirements) should also be made explicit and validated throughout the life cycle of the project. In this context, a significant change in scope can have a domino effect on the value chain.
4. **Market- and Geopolitical Assumptions:** The achievement of the project objectives, although necessary, is not a sufficient condition to fulfill the **client's or organization's mission**, unless the assumptions about other projects, operations, market risk, and the geopolitical environment are met (e.g. reliable allies throughout the power grid).

Each of the above assumptions is a set of conditions beyond the control of a given category of decision-makers. Although more complex in reality, we can view the assumptions about the market and geopolitics as the conditions beyond the client's control. Task and product assumptions are those beyond the control of project managers and operations managers. Resource assumptions represent the conditions beyond the control of functional managers and performers. Making these assumptions explicit is a prerequisite in hazard identification. However, this is much easier said than done. Identifying and validating these assumptions are at the core of risk analysis problems.

- **Identifying Obstacles to Assumptions, Causative Events and Adverse Consequences**

Once these assumptions have been articulated, and validated with team members, clients, users, contractors, and other key stakeholders, we must identify the obstacles to each assumption, their causative events and the outcomes (adverse consequences) which may result from each event. For instance, supplier delivery is prone to transportation hazards, raw material shortages, and unavailability of labor. The **causative events** could be strikes, snowstorms, accidents or surges in the demand for resources. Cost overruns, delays in activity start and slippage in project schedule are among the outcomes that would result from these events.

This exercise often provides clues to the identification of usual risks (health & safety risks, product malfunctions, fluctuations in resource costs, interest rates and foreign exchange) as well as rare risks that are frequently overlooked as the project context and environmental conditions shift. It should be repeated frequently to keep the risk repository up to date.

- **Template to Define the Business Model**

The **Harvard Change Definition Grid** is the template used to define the business model (or value-creation chain), and the grey areas. The back page of this instrument details the risk management scenario for each value-chain related risk.

Exercise:

Take a small project and define the value chain and up to a dozen the grey areas. Pick only one gray area in each of the four columns of the **Change Definition Tool.** Detail, on the back page of the document, the respective risk management scenarios. By risk management scenario, we mean defining the grey area (or making the assumptions explicit); identifying associated risk and the best strategy to reduce it to an acceptable level; defining the remaining residual risk (i.e. the risk that cannot be cost-effectively covered by the strategy); and outlining the contingencies or damage control plan to address residual risk (e.g. insurance).

The brain-stem cells case study in risk management titled **Hygea** illustrates some grey areas and assumptions related to the value chain of a disruptive-technology opportunity.

6.2. Risk-Incubation or Pre-Project Innate Risks

There is a widespread but false belief among decision-makers that projects have a finite start beginning with the formulation of client objectives. In reality, the roots of a project or policy can be traced back to much earlier stages together forming an evolutionary process akin to the biological process of pregnancy and childbirth. This maturing process, referred to as value incubation, risk incubation or pre-project life cycle, begins with an issue's embryo phase, often an isolated event, occurring long before the development of a mature constituency, the formulation of objectives and the definition of the value chain.

A **surprise event** is a key milestone in the cycle. It is defined as an incident that shakes deeply held beliefs. It frequently follows a series of isolated events[18], acting as trigger for the formation of a **critical mass** for a change. Surprise events increase uncertainty. In some rare instances, they set in motion a chain reaction leading to a systemic risk.[19]

Related Reading:

The fate of projects often depends in large measure on the work done before the formal commencement of a project. As demonstrated in Chapters 7 and 8 of the author's book *Harnessing the Power of Intelligence*, understanding the value-incubation cycle and the role of surprise events can help decision-makers identify opportunities, scan for and mitigate related risks, and ultimately build the foundations of success for their projects ahead of adversaries, and frequently before key stakeholders are on board.

Historical experience provides a source of identification of risk-incubations likely to recur.

6.3. Stakeholder-Related Risks (SRR):

An analogy from defensive car driving can help us appreciate the importance of conducting a Stakeholder-Related Risk exercise. Responsible drivers must not only drive safely, they must scan for risks coming from anyone sharing the road, be they bicyclists, pedestrians, vehicle drivers or wandering animals.

"Many times the technical risks are serious but addressed because people tend to look to technical issues first. They are schooled in their identification and solution. The political risks often involve the customer or some outside actor, the prime contractor or some key funding issue… Non-technical risks are more universal and insidious than the technical ones. They are just more difficult to control, estimate, quantify, and resolve. And their resolution can cause trouble for the project. Much better, many people believe, to deny they exist."[20] In this context, John Marczak, Project Manager at the Nuclear Division of Ontario Power Generation kindly reminded me of J.R.R. Tolkien quote: "It doesn't do to leave a live dragon out of your calculations, if you live near him".

- **Who is a Stakeholder?**

Dealing with these risks involves identifying the project stakeholders and determining their stakes and behavior. Here, a **stakeholder** can be a risk source (i.e. a real or potential threat to the project), a risk recipient (a casualty), both or neither

(beneficiary). In mergers & acquisitions, we know that the higher the stakes and the number of strategic partners, the greater the likelihood of disputes and other stakeholder-related risk of failure. The bankruptcy of one partner (risk source) can adversely affect the remaining partners (risk casualties).

In projects where corporate reputation or national pride is at stake, important stakeholders who fall in love for a powerful vision may turn a blind eye on major risks; thus, endangering the project and the bottom line. In the case of the supersonic Concord, both the French and British policy makers were captivated by the idea that "speed sells seats" that they discounted the worst-case risk scenarios of large jet-fuel consumption, high friction, supersonic shock waves and other challenging assumptions about the operating environment.

Risk managers should also be alert to the fact that while most stakeholders endeavor to maximize their utilities, there is a substantial body of evidence that demonstrates otherwise.[21] In fact, recent developments in psychographics and regret theory show that individuals who tend to be risk-averse have specific profiles. Many are more concerned with perceptions than reality (facts, logic and reason). The fear of looking incompetent, or being framed as a loser, weighs heavily in their choice, even when the risk is small compared with the magnitude of the potential gain.

The stakeholder universe is a complex web of relationships. Yet, grasping just a fraction of its dynamics can be rewarding in risk management. It includes direct and indirect customers, direct and indirect suppliers and creditors, layers of regulators and other government players, direct and indirect competitors, board members, institutional and other shareholders, executives and other permanent and temporary employees, unions, educational and research institutions, licensees, licensors and other partners and allies, media, non-governmental organizations, neighbors, and communities with a vested interest in your mission. Do not underestimate the risk related to undesirable stakeholders (e.g. misguided individuals, criminal elements), particularly when the visibility, importance or stakes are high.

- **Partner-Governance Risk: Banks and Rating Agencies under Fire**

Along with the housing boom, millions of hard-to-sell subprime 15- to 30-year residential mortgages were converted by U.S. banks, most notably Citi, into short-term debt packages securitized by adjustable-rate loans for low-credit home buyers. The debt packages were bundled, overrated with the banks own AAA credit rating and aggressively resold to global investors (banks, insurance companies and mutual funds) who neither questioned the banks huge risk miscalculations nor the rating agencies. In July 2007, both Moody's and Standard & Poor downgraded billions of dollars of securities, in haste, when the losses hit Main Street.

This systemic mispricing of risk goes far beyond the subprime risky residential mortgages. It affects most classes of risky assets in global markets and will result in unprecedented aggregate losses ranging from hundred to perhaps trillions of dollars. The Buyer Beware argument is alas alive in the wild global securities market.

Decision-makers must question the risk-assessment, not only of their clients and suppliers throughout their value chain, but also the systemic risk exposure of their sector and other partners involved in their business as in the case of the electricity grid. The author worked with that sector to establish advanced risk mitigation processes following the August-2003 massive power blackout. The brief below provides insights into the systemic partner risk in the integrated power grid.

August 2003 Massive Power Blackout

In the electrical power grid, most utilities focused on value-chain risks within their respective organization. Except for the readiness to disconnect from the grid in the case of overload, they paid less attention to the incubation of the risks caused by other utilities, generally assuming every partner on the grid was doing its job for its own share of responsibility. Costing at least $6 billion in financial losses and no less than eight fatalities[22], the massive power blackout that struck major Canadian and U.S. cities in August 2003 was a rude awakening. Its likelihood and the severity of the cascading power failure could have been lessened had everyone paid attention to stakeholder-related risks, specifically partner-governance risk. This exercise involves intelligence production and sharing, cross-training, transparency, inter-utility peer reviews and an effective risk-governance authority at the alliance level.

Nuclear-power producers must pay more attention to partner-governance and other stakeholder-related risks than other energy providers, given their disproportionate cost-burden and the longer time to restart their plants after a shutdown. They should neither ignore the risks related to anti-nuclear activists nor those latent in the factional attitudes within parliament and the government machinery. In fact, public oversight is a maze of overlapping, and sometimes conflicting, jurisdictions of provincial and federal regulators (Canadian Nuclear Safety Commission or CNSC, Environment Canada, Fisheries & Oceans, Ontario Ministry of Environment, Ministry of Labour).

In this environment, projects and day-to-day operations face omnipresent stakeholder-related risks. They can be paralyzed by a veto or the threat of regulator veto. Decision-makers in this industry should also use the nuclear fuel cycle to determine and manage risks. This cycle comprises the value-chain activities to produce nuclear energy including plant commissioning, ore mining and enrichment, fuel creation and transformation into electricity, nuclear waste management and disposal, and facility decontamination and de-commissioning.

- **Factional Analysis and Other SRR Tools**

The identification of Stakeholder-Related Risks (SRR) goes beyond the fuel cycle to include tiers of stakeholders, such as users and grid partners, both upstream and downstream. SRR tools like Factional Analysis and the Power Scale go beyond the battleground of accountability to map the sphere of vulnerability, by taking into account the power and perception of opportunities and risks by each stakeholder.

The tools used to identify the cluster of SRR risks by mapping the project neighborhood and external environment include intelligence collection tools, Factional Analysis, the Power Scale, psychographic profiles (VALS, FIRO-B, SDI, Issue/Threat Incubation Frameworks, social wiring diagrams, ePrecision Trees, malware and polymorphic detection algorithms.). The focus is on risks that were not identified during the Value-Chain Risk exercise above. Chapters 9 and 10 of *Harnessing the Power of Intelligence* describe some of the instruments we use to identify stakeholder-related risks. This material will be discussed at a great length in the seminar.

Managing stakeholder-related risks starts with prevention. It means targeting the right stakeholders (clients, suppliers, staff, bankers) based on expected added value to each party, and valid intelligence about their suitability profile. Suitability requires appropriate knowledge of the dominant contributors of cumulative risk (or at least the top 10 risks) facing each key stakeholder. It cannot be assessed without understanding the stakeholder's managerial and financial strengths, market, alliances, value chain, transparency and traceability of revenue and costs, and integrity (in dealing with regulators, investors and clients). The objective is to gage at least the cumulative top-10-risk exposure of each player to her own stakeholders.

The duration of the project affects stakeholder-related risks in many ways, particularly when government plays an important role. Be they East or West, North or South, governments can abruptly change direction in mid-course, sometimes severely handicapping the project.

Project teams can waste substantial time in fruitless interactions with peers and outsiders who may not even realize the damage they inflict on the project by their time-wasting behavior. The *Harvard Time & Productivity Diagnosis Log*™ tracks the pattern of frequent interactions with specific people to document unexpected interruptions, detect incipient time-wasting behavior early, and take corrective action before a significant project loss occurs in safety, security, environmental impact, privacy, quality, reliability, time and cost.

6.4 Responsibility & Accountability Risks

Responsibility Charting is at the heart of **internal controls** and core governance issues (accountability, ethics, transparency and public trust). An integral part of the Project Execution Plan, a Responsibility and Accountability chart is a two-dimensional tool defining for each participant in a project or a business operation, the exact **role, accountability and sequence**, if any, in each task. The chart lists tasks or decisions horizontally. Both internal and external stakeholders are listed vertically, with their respective role in the row-column intersection cells. Figure 4 describes the four generic roles (Responsible, Approves, Supports and Must be Informed) and the four types of accountabilities (Professional, Managerial, Regulatory, and Governance). The roles are based on work needs and the principle of locating responsibility as close as possible to sources of expertise and intelligence.

Responsibility charting focuses on role clarity and on risks related to responsibility and veto. It helps **prevent and adjudicate role conflicts**, particularly those related to mergers, reorganizations, and projects teams from different organizations. Users can also **spot early signs of delays**; thus, act promptly to redress the situation. The tool also helps the prevention and prompt management of risks related to executive support and user involvement.

Activities Decisions or Phases ⇩ / Participants ⇨	Project Manager	Chief Engineer	Procurement Officer	Client	Regulatory (CNSC)	Suppliers	Contractor	Board	Press	Alternate R
Engineering	A^{M}_{1}	R^{P}	S	A_{2}	A^{C}	S	I_{3}	I^{G}		**John Lee**
Procurement	A^{M}_{2}	S	A^{P}_{1}	I		S	R	I^{G}		**Jean Roy**
Construction	A^{M}_{2}	A^{P}_{1}	S	A_{3}	A^{C}	S	R	I^{G}	$I_{0\text{-}3W}$	**Sarah Wang**

Responsible (R): You see to it that the job gets done whether you do it or not. Skills deficit is among the risks.
Approval (A): Must either approve or veto. The less Approvals the better. "A" are early warnings for delays.
Support (S): Must provide support, knowledge or expertise. Not responsible. Cannot approve.
Must be informed only (I): None of the above. Watch it. Those to be informed may act as hidden veto!

Superscripts denote **Accountability**: Managerial (M), Professional (P), Compliance/Regulatory (C), Governance (G)
Subscripts denote Sequence, Deadlines or Embargoes: A^{M}_{2} specifies 2nd Approval for Managerial Accountability.
I^{G} Means the Board should be kept informed regularly (no sequence) for Governance (G) reasons.
Note that the Press should be informed (I). The subscript 0-3W means 3 weeks before the end of construction.

Figure 4: Responsibility & Accountability Chart

Accountability is legally based. Its principles should be clearly communicated to project team members.

The first and most-common form of accountability applies to all citizens is **individual accountability.** It requires everyone to account for her/his ethical and responsible behavior. Anyone committing or helping others to commit an offense can be prosecuted. Offenses range over a wide spectrum from possessing illegal materials or substances; endangering property; putting people's lives, safety or security at risk; to counseling and providing information for an unlawful purpose. Individual accountability requires everyone to account for ethical and responsible behavior.

The second level of accountability is mostly legislated by states and provinces. Engineers, physicians and accountants are subject to **professional accountability**, in addition to general accountability. Auditors and chartered accountants are accountable to their client boards and doctors to their patients. Both are also accountable to their respective professional accreditation authorities.

Located at the third level, **managerial accountability** is vested with managers and project leaders. Responsibility can be delegated, accountability cannot, nor can it be shared. Chief Commissioner J. Grant Glassco's famous judicial dictum "Let the managers manage"[23], meant delegate responsibility as close as possible to the sources of knowledge and information. But, managers cannot be held accountable unless they have the authority and degrees of freedom necessary to fulfill the obligations associated with managerial accountability. These degrees of freedom include the devolution or provision of:

- Authority to mobilize the best resources for the task and the right to dispose of these resources when necessary,
- Adequate leverage to fairly reward achievers and discipline poor performers, including veto power on fast-track promotions and grace period on the timing of lateral transfers
- Means to upgrade and maintain up-to-date the skills of their work force
- Adequate budget
- Reasonable power to acquire and discard equipment, tools and facilities based on needs
- Some latitude on deadlines and schedules

– Access to prompt and accurate decision support systems.

Presidential or Ministerial Accountability is the fourth level of accountability. It is vested with the President and Chief Executive Officer of the firm. In the U.S. government, the President is accountable. In Canada and the United Kingdom, this type of accountability is called ministerial accountability and is clearly left with the minister. We must keep in mind that the top political leaders in British-parliamentary democracies govern as if they represent a majority of their citizens even though most have held office without securing at least 50% of their electoral constituents.

At the fifth level, the **social, moral or collective accountability** acts as a safety valve by closing the loopholes left by the other accountability classes. It marshals all human resources located in proximity to risk sources. These resources composed mostly of professionals and support staff (plus regular vendors and clients) are most likely the first to witness accountability violations by individuals who fail to meet their obligations namely professional, managerial or presidential accountability. Furthermore, collective accountability goes some way to redress the gap created by managers and executives who are not privy to the violations of accountability at the general, professional, managerial or presidential level. It is also the mechanism to address (cross-examine, validate and secure fair resolution) allegations of wrongdoings.

Collective accountability is based on the belief that each of us has civil duties to behave as a responsible citizen. These duties include a genuine contribution to foster fair play, minimize suffering, reduce violence, prevent mischief and not condone wrongdoings, in both our organization and the community. Collective accountability holds anyone privy to mischief, or to a serious potential risk, responsible for alerting the appropriate authorities. However, this is easier said than done. Collective accountability requires strict policies, a sound training program and a relatively autonomous structure, at arms-length of management.

Since individual and collective accountability are everyone's business, there is no need to display them in responsibility accountability chart (figure 4). Chief executives are ultimately accountable for governance and compliance. But these legal obligations frequently transcend the above levels and can be vested with management, professionals, chief executives or the board. Judging from the judicial investigative work related to Exxon Valdez,[24] Mobile Oil Ocean Ranger,[25] these obligations must be differentiated as indicated in Figure 4 and communicated to everyone in a project team.

Responsibility and accountability risks will be discussed during the seminar.

Accountability in the Public Service: Frequently used to denote professional, managerial or ministerial accountability, public-service accountability goes far beyond the simplistic notion of ensuring that public money is spent wisely. It is a socio-legal process that has been the subject of intense debates for decades in many countries, frequently following scandals, misconduct news and other negative surprise events. The Report of the Task Force on Public Service Values and Ethics states that public-service accountability "requires all those in authority to render an account of how they exercise their authority, of how well they are doing and of what they are doing to correct problems and make things better… We are accountable — and not only for what we achieve but how we achieve it. Our information must be accurate, our advice objective, our service even-handed. Accuracy, objectivity, fairness, balance are also part of our professional ethic. There are no doubt too many rules, too many procedures which serve no clear public purpose, and public servants must continue to challenge these rules, eliminating unnecessary procedures, barriers to change. But even as they challenge the rules, public servants must recognize that the rule of law protects Canadians from arbitrariness at the hands of officials. And, as we move to more empowerment to individual public servants and more authority to public service agencies, clarity about authorities, obligations, performance measures and, above all, values becomes increasingly important."[26]

6.5. Project Implementation (or Execution) Risks

Project Execution occasions the work-in-progress risks of loss or injury due to the human failure or inadequacy of internal controls, systems, technology or processes. Many of these risks should have been identified in the Value-Chain Risk exercise. In banking and insurance, these risks include all external risks but exclude three risks: reputation, strategic and systemic risks.

Project implementation risks are the traditional areas of focus of most risk managers and providers. There is no shortage of risk management tools. But many are inadequate. As an illustration, **Critical Path Analysis** should be applied with caution, as it is frequently an unreliable indicator of risk exposure pathways.

Among the instruments that can help predict and track project implementation risks: **Global Control Ratios** are effective for setting project milestones for risk identification and tracking. **Schedule Validity Tests** assist in determining the risk of slippage and the adequacy of time contingencies. **Earned Value** (CSCS) charting is good but difficult to establish for soft projects. **Global Projection-Reliability Tests** provide early warning signals about potential delays, cost overruns and the adequacy of financial reserves. The **Failure Review** and **Change Logs** can help track the sources of errors, rejects, defects, complaints, and prevent reoccurrences.

6.6. Transition & Commissioning Risks

Even when project strategy is clear, its execution can be fraught with roadblocks including resistance to change particularly during commissioning. The **Harvard Transition Risk** instrument provides a step-by-step scenario to reduce the risks associated with resistance to change, turn the resistance into constructive engagement, and mitigate residual risk and collateral damage.

This instrument will be introduced and discussed during the seminar.

> **Exercise:**
>
> Please read the one-page Globe & Mail article titled *"Alcan Case Study - Lobbies Aim to Make Dent in Can Market"* at the end of this document. Summarize how Alcan orchestrated strategic change in the face of major transition obstacles and stakeholder-related risks. What are the critical success factors used by Alcan in its journey to capture the new pop-can market? How does Alcan strategy compare with the intense lobbying by the steel industry and union pressuring the Government of Ontario to maintain pop-can regulations, as a roadblock to Alcan objectives? Note this case study illustrates how working on stakeholders' risk (among others) in advance can frequently make the difference between success and failure in a capital project.

6.7. Balance-Sheet and Off Balance-Sheet Risks

Balance-sheet risks comprise money risks (liquidity, credit, and sovereign), market risk (pricing, terms & conditions, interest rate, tax credits), legal and financial-covenant risk (contractual obligations, and collaterals). Off-balance sheet risks include latent environmental risks, corporate restructuring risks and pension risk, and other contingent liabilities. With the help of CFO, project managers should discuss these risks and their impact on their projects. These important risks are the focus of financial analysts and are beyond the scope of this paper.

7. Risk Assessment

"Risk assessment is the scientific process of investigation to estimate the level of risk."[27] It is about quantifying, or at least range-estimating, the impact (both gravity and likelihood) of the undesirable consequences on those exposed. This is done after determining the population, ecosystems, property and other resources at risk (i.e. that could be affected by the above outcomes) and the specific context and conditions (time, space) under which they would be exposed (exposure pathways). Risk assessment is probabilistic. It requires tools to simulate alternative risk scenarios using uncertainty and sensitivity analysis, stress-testing[28] the value-chain ingredients, Value at Risk (VAR)[29], and other quantitative approaches.[30]

Risk statements are validated and completed during the risk-assessment phase.

In commenting the August 2003 Blackout, Frank Felder argued for a need to conduct **Probabilistic Risk Assessment (PRA)** to "systematically identifies the basic events that form accident sequences which result in undesirable consequences, the probability of these basic events, and the overall probability of these accident sequences. Since PRA is comprehensive and systematic, it accounts for the fact that some basic events may contribute to multiple accident sequences or lead to common-cause failures. When first applied to the commercial nuclear power industry, PRA identified some important accident sequences that had never been considered.

Another benefit of PRA is that it can be used to quantify the level of uncertainty of its results. We may be able to estimate precisely the probability of some accident sequences occurring precisely, but not others. This discrepancy, in consideration with other factors, may suggest the need for additional data collection or investigation. By being able to characterize our "ignorance," PRA can help direct us in the best use of our resources to increase our knowledge."[31]

In regulated industries and projects impacting health, safety, and the environment, an **independent team** is mandated to conduct risk assessment. In all cases, a **peer review**, led by a credible and impartial evaluator, is essential when the stakes are high. This form of risk assessment audit is now considered a best practice in commercial software development and mission-critical IT projects. Its purpose is, at the least, to validate the method, investigative work, and findings of the risk assessment team.

Risk assessment is driven by facts, logic, science, and judgment. While controversial, it is gradually emerging as a codified discipline. On the other hand, **risk mitigation is context driven.** It determines importance and urgency by considering the risk-assessment findings in the context of various interests, of communities and stakeholders. These interests are reflected in a host of economic, legal, social, and geopolitical considerations. Risk decisions are ultimately based on policy, judgment, values, and knowledge.

In its report titled *Understanding Risk*, the National Academy of Sciences "recognized scientific analysis as the best source of reliable, replicable information about hazards and exposures and as being essential for good risk characterization. Relevant analysis, in quantitative or qualitative form, strengthens the knowledge base for deliberations; without good analysis, stakeholder processes can arrive at agreements that are unwise, not feasible, or simply a reflection of who possesses greater political power. The chief challenges are to follow, in practice, analytic principles that are widely accepted and to recognize the limitations of analysis."[32]

Consider the health risks to the population of Salzburg (Austria) due to exposure to mercury discharged by the city's main power house. In order to map out the probability distribution of these risks, an Austro-American team began by raising the following questions to identify the hazards caused by mercury emanating from the smokestacks of the co-generation plant: What kinds of effects appear and how severe are they? At what ages might an individual be particularly sensitive to these effects? Are there any special subpopulations in which the effects will be more likely and/or more severe? Are there any routes of exposure, such as eating fish in this case, which are more likely to cause the effects? How strong is the evidence for these effects? [33]

In the same power plant study, exposure to mercury was characterized by "breathing contaminated air, contact with contaminated soil, ingesting contaminated water and food, and from certain medical procedures. Exposure to mercury can have serious health effects. The main health effects associated with acute mercury exposure are hallucinations, delirium, and tremors (EPA 2001). According to the EPA, long-term mercury exposure also damages the nervous system, stomach, intestines, lungs, kidneys, and brain. Blood pressure and heart rates can also be elevated by exposure to the substance. Unborn children are also at risk of permanent damage if their mothers are exposed."[34]

Risk assessment comprises hazard characterization and exposure assessment (risk characterization).

7.1. Hazard Characterization

Hazard characterization is the quantitative or semi-quantitative evaluation of the nature of the adverse consequences to humans, the environment and organizations following an exposure to risk sources. This must, where possible, include a dose-response or exposure-response assessment.[35]

7.2. Exposure Assessment

Insurance companies work with a team of actuaries, scientists and engineers to assess exposure and characterize risks.

In environmental risk studies, "**exposure assessment** is used to produce estimates of the degree of a local population's exposure through the environment, identifies the most important exposure pathways, and estimates the variability of exposure for the population in question. Several stages of exposure assessment are considered:

- Determining the sources of the pollutant;
- Determining the source strength or amount of pollutant;
- Determining the dispersion of the pollutant in the environment;
- Determining any transformation of the pollutant in the environment;
- Determining the state of the environment;
- Determining the exposure to defined populations;
- Characterizing exposure so it can be combined most effectively with exposure-assessment to perform risk characterization."[36]

Banks, insurance companies and utilities produce impact rating grids to provide guidance about risk characterization of several risk factors.

- **The Precautionary Principle**

When either the probability or the severity of the consequences cannot be accurately quantified, the precautionary principle should apply. It errs on the side of caution by reasonably overestimating risk and placing a greater emphasis on risk mitigation over assessment. But "excessive precaution may cripple incentives and new applications. The discipline of risk management will help demonstrate the proper balance between possible benefits and potential harms."[37]

- **Mitigation Can Be Imperative Without a Precise Quantitative Assessment**

There are also instances where observation, anecdotal evidence, reason and common sense dictate the adoption a risk-mitigation strategy, without a quantitative assessment.

As an illustration, negotiating a narrow driveway of a residential garage is always hazardous when driving in reverse, without a camera or an audible backup warning system. Car and SUV drivers tend to be more in a hurry when going to work (or running errands), than when returning home. Among others, children walking on the sidewalk, particularly those going to school, are at risk. It is therefore more prudent to reverse drive into the home garage so as to exit it, with a greater visibility, in drive mode. Many responsible drivers, who constantly think about risk, will change their behavior, even in the absence of a quantitative risk assessment. Here, communication through awareness and education is the prerequisite to risk mitigation.

7.3. Threat Integration

Since 9/11, new risk-assessment policies were borrowed by business corporations from the field of national security. Among them, the importance of setting a corporate *Threat Integration Center* under the direction of the chief risk-management officer (CRO). Serving as risk-management hubs working under one roof, these centers merge and validate risk-related information from all sources and provide the enterprise an aggregate picture of the threats and total risk exposure facing the organization. They must also ensure "that intelligence information from all sources is shared, integrated, and analyzed seamlessly -- and then acted upon quickly."[38]

8. Risk Mitigation or Risk-Response Planning

Risk mitigation is the result of the commitment by management and project teams to rank risks based on gravity and risk tolerance, and to undertake the most effective measures, including contingencies, to combat identified risks, and prevent and manage related conflicts. "The objective of **risk mitigation at the corporate level** is to achieve the best combination of cumulative risk (reduction, retention and transfer), consistent with the optimum effect on the firm's overall value."[39]

For the organization, **risk tolerance** is the level of risk its leadership is prepared to take in pursuit of a project or a given opportunity. Clients, performers and other key stakeholders should not only consider the cost-benefits, but also the cumulative risk exposure to their business portfolio (or enterprise). Thus, the importance of the opportunity (or project) is an element in determining risk tolerance, in addition to acceptable risk policies, which depend upon the operating environment (technical, economic, regulatory), and corporate and political considerations (for risks with social or geopolitical implications). A project would not be undertaken when risk tolerance is exceeded for any deliverable. However, between maximizing benefits (expected monetary value or, generically speaking, utility) and minimizing regret, the threshold of tolerance can vary widely from one decision maker to the next.

The selected strategy for mitigating identified risks should differentiate and integrate one or more of the following four fundamental interventions from multiple perspectives including **time** (present, plus short, medium, and long-term future), **space** (distance and territory including the virtual world), and **constituencies** (individuals and groups):

8.1. Prevent the Risk

This option is often the product of brainstorming and innovation. It can call for changing the nature of the game or the value-creation chain. It may also point to ways of achieving the same function or purpose with a different solution including paths never taken before. As an illustration, swimming outdoor increases exposure to sun ultra-violet radiation and consequently to skin-cancer risk. This risk can be reduced by applying a water-resistant sunscreen every two hours. However, swimming indoor prevents it altogether.

8.2. Retain the Risk

Called self-insurance, this option requires adequate reserves supported by actuarial studies to absorb losses of retained risk (firm risk). It should neither be prescribed for high impact risks nor for those affecting mission-critical deliverables or relationships. Retained risk can lead to insolvency, when it exceeds risk tolerance, particularly in undercapitalized companies.

8.3. Reduce Risk to an Acceptable Level and Deal with Residual Risk

Reduce the risk to an acceptable level through innovation, redundancy, and accepted practices. This is done by lessening the probability of occurrence of the hazard, or its impact if it happens, or both. In banking, passwords restrict unauthorized access to client accounts. Limits on withdrawal lessen the impact of such access. In construction, safety clothing (hard hats, steel reinforced shoes) and barriers (fences, signs) restrict access to dangerous areas; and reduce the impact of falling objects on workers.

Since sooner or later, an unprecedented event can defy even the best precautionary principle, we must now estimate the residual risk and prepare contingency and damage control plans to face the adverse consequences of residual risk (emergency system, fire service requirements). Buying insurance against unlikely losses (residual risk) is a form of contingency. It would not be prudent to ignore concession or graceful exit strategies should the risk management scenario and contingency plans fail, particularly in hostile or tragic situations.

Within this strategy, there is a cluster of generic choices available to project managers. These choices will be discussed after introducing *Harvard Strategy Grid.*

8.4. Transfer the Risk to a Third Party

This option should be considered either as a contingency or a preferred choice when it is cost effective. Here, the transfer cost of each risk is the premium paid less expected losses. Hedging, outsourcing, insurance, waivers and export credit are

among the vehicles to share or transfer risk to a third party. Insurers, re-insurer syndicates, export credit agencies (Export Development Canada), and other underwriters transfer risk.

> "**Insurance** is a means for dealing with the economic uncertainty associated with chance occurrences. It does so by exchanging the uncertainty of the occurrence, the timing, and the financial impact of a particular event for a predetermined price. To establish a fair price for insuring an uncertain event, estimates must be made of the probabilities associated with the occurrence, timing, and magnitude of such an event. These estimates are normally made through the use of past experience, coupled with projections of future trends, for groups with similar risk characteristics. The grouping of risks with similar risk characteristics for the purpose of setting prices is a fundamental precept of any workable private, voluntary insurance system. This process, called **risk classification**, is necessary to maintain a financially sound and equitable system… Risk classification is intended simply to group individual risks having reasonably similar expectations of loss."[40]

Finally, a cost-benefit analysis is required before moving to the next phase: Risk Response Implementation and Control.

9. Risk-Response Implementation, Progress Tracking & Control

This phase requires a risk-management team supported by robust information and intelligence systems for risk-indicator data collection, tracking the progress of mitigation plans, analyzing deviations, and taking corrective action. Risks change over time, with the emergence of new risks, and the tendency of the uncertainty of existing risks to recede as completion nears. **Regular progress reviews** with an adequate frequency of control are essential to keep a firm grasp on risk management, and project future progress and impact.

"A key issue to consider in risk management planning of attack scenarios is how **variability** in selected risk management controls across the organization for similar scenarios would be perceived. For example, what is the implication of one airport hand-searching all baggage, while another airport only samples a small fraction of the baggage by hand? Do the different strategies really provide comparable levels of risk control? How will stakeholders and the general public perceive the apparent inconsistencies in risk management controls (especially if an attack does take place)? How will potentially large differences in requests for resources be handled?"[41]

10. Risk Communication

There is an obligation to continually inform and educate the project team and anyone who may be impacted in any way by the project. Risk communication is both formal and informal. It is about user-friendly information dissemination, awareness (risk-response drills), education and training. It is an ongoing and vital function that spans over all aspects of policy formulation, decision-making, and day-to-day operations. It affects intelligence production, hazard identification, risk assessment, mitigation, and governance. Giving feedback and praising the dedicated and capable project team members in a genuine and professional manner is also an integral part of risk communication.

In large-scale endeavors like nuclear power generation, the vast majority of citizens tend to ignore or underestimate risk prior to, and overestimate it after, an undesirable event. An important element of risk communication is to target these so-called soft stakeholders to head-off or bridge, this frequent gap between real and perceived risks. Concurrent media education and broader risk literacy campaigns are instrumental for this purpose.

Such education and awareness sessions are more effective when they are clear and meaningful; and when the call for action uses powerful analogies, metaphors, and examples pertinent to each audience. That is how the Health & Safety Communication team at Anheuser-Busch gets an entertaining and persuasive risk prevention message across to plant workers.

Anheuser-Busch

"The Jacksonville Brewery wellness team added a racing theme to its activities in 2002. From "Start Your Engines" to the "Finish Line," participants made healthy improvements to their lifestyles… Some of the specific initiatives during the year included Check Your Oil (cholesterol), Top Fuel (nutrition), Yellow Flag (cancer prevention) and Preventive Maintenance (flu shots)."

Anheuser-Busch message with closer to home illustrations and well-crafted visual aids have proven effective in preventive visits to primary care physicians, in decreasing the incidence of high blood pressure, diabetes screening and stress management in the workplace.[42]

11. Risk in Project Management

The Project Execution Plan cannot be complete without a detailed description of risk management undertaking.

Project risk results from both expected and unexpected adverse consequences of a probable event on the project mandate, the human and ecological environment, and key stakeholders and their property. Key stakeholders are the client and end users, the performers, the supply chain, the neighboring community, and anyone who perceives the project or its deliverables as a threat or an opportunity.

Here, the mandate includes the goals (benefits) and deliverables of the project, financial metrics (project cost and operating & maintenance cost, cash flow, market value and credit rating), deadlines (strategic, functional, fiscal, ceremonial), quality, safety, security and reputations (negative impact on alliance options and future business).

Thus, in addition to safety, security, requirements volatility, and general risks facing their organization, project managers have to manage five specific risk clusters: resistance to change and related conflicts, failure to meet the specifications (accomplish objectives through the required deliverables), missed timelines, cost overruns, and collateral damage (disruption of other projects or activities, loss of valuable clients, talent, allies, intelligence, or other property). To this end, the tools introduced above are instrumental to study project risks as indicated in Figure 5 below.

Project risk must be determined and managed continuously during the project and throughout the life cycle of its deliverables. In the aerospace and nuclear industries, the risk per year of operation must be established and rigorously managed for each system and its components.

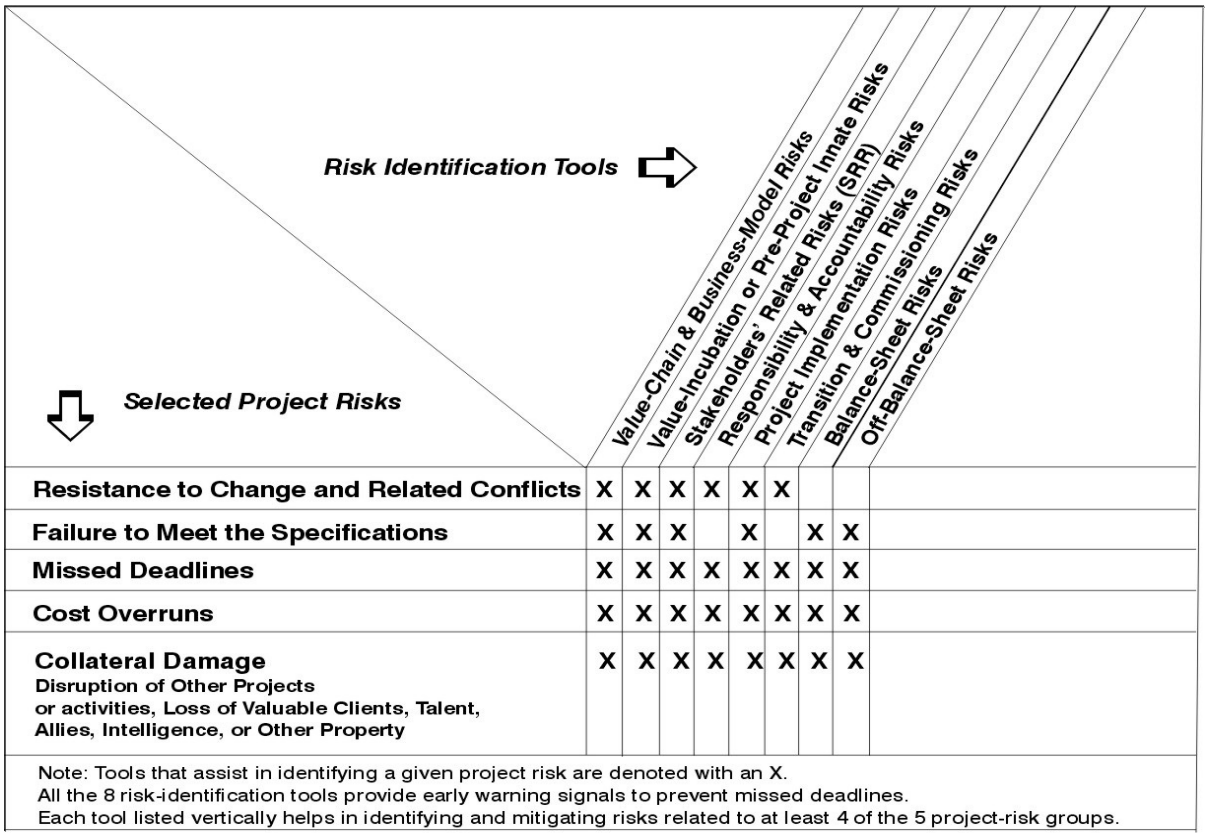


Figure 5: Tools to Study Five Clusters of Project Risks

Each project risk is estimated based on the probability and severity of undesirable events, with due regards to the effectiveness of existing controls and risk tolerance (fitness for purpose). Internal controls should be established to address all risk-prone processes and activities. External risks should be managed with the support of the continuous intelligence monitoring and analysis network.

Although collaboration is vital in complex risk management, each member of the project team must be trained, continuously briefed on the risk exposure, risk management and communication; and assigned a clear mandate with precise responsibility. The team and its leadership should be individually and collectively held accountable for their contribution to all aspects of risk management.

12. Illustration of the Framework in Space Shuttle Risk

Consider the February 2003 disaster that struck Columbia STS-107 scientific mission. Using the **risk-incubation** tool, we can observe repeated early warning signals including a remarkable study led by Professor Elisabeth Paté-Cornell, who currently chairs management science and engineering at Stanford University. This probabilistic risk analysis (PRA) study of the tile protective system (TPS) was originally undertaken in 1990 with a report to NASA the same year and updates published subsequently, up to 1994.[43]

Professor Paté-Cornell repeatedly warned NASA that, if not properly installed, a small number of protective tiles could account for most of the risk of triggering a chain reaction of catastrophic failures. Incidentally, this illustrates again the Pareto distribution found in most risk assessments. "The contributions of different tiles to the overall probability of failure (defined here as "risk-criticality") vary widely according to their location on the orbiter's surface. A large percentage (85%) of the probability of loss (LOV[44]) as a result of failure of the orbiter's TPS can be attributed to a small fraction of the tiles (15%). Because there will always be resource constraints, setting priorities is a first critical step towards ensuring that the most risk-critical tiles receive maximum care and quality control to minimize the probability of failure."[45]

Furthermore, Professor Paté-Cornell made important technical and organizational recommendations addressing each of the causative events illustrated below.

She characterized the dynamics of **value-chain operational risks.** "The processing of the tile between flights is labor intensive and time consuming and, because it is often on the critical path to the next launch, the work is sometimes done under severe time constraints. Although great attention is dedicated to the tile work, its quality is occasionally affected by this demanding schedule." Professor Paté-Cornell went on to identify the technical and human aspects that lead to poor performance: shortcuts due to inelastic deadlines, high turnover among tile technicians, and "a reward system that is based mostly on productivity and which encourages myopia or critical information (bad news) that never reaches the decision-maker." For example, to speed up bonding, water (and sometimes saliva!), were wrongfully used; thus, decreasing the long-term reliability of tile bonding.

Professor Paté-Cornell also outlined **stakeholder-related risks (SRR)**: rivalries among managers competing for limited funds; main contractors withholding vital information from each other for competitive reasons and sometimes fear of liability; excessive optimism of senior NASA managers and pressure to create good impression (to secure funds, among other interests), all of which leading to imprudent decisions.[46]

Adjunct to these stakeholder risks were several **responsibility and accountability** risks trickling from senior management down to the shop floor. "The low status of the tile workers, grounded in the pay scale, may have had several detrimental effects: (1) a waste of money in training tile technicians who left the job as quickly as possible [because training qualified them for a better pay elsewhere], (2) low morale for some of them, which is seldom conducive to high-quality work, and (3) the 'no respect" syndrome on the part of other technicians [those veterans in the job], who carelessly damaged the tiles, before increasing again the TPS workload."

Although NASA adopted most recommendations, upgrading tile protection and maintenance, many stakeholder problems remained. As for **intelligence production**, there is, so far, no evidence that NASA sought the help of the military or other space partners. Using powerful ground or spy-satellite cameras at their disposal, these allies could have provided mission-control engineers with a closer look at the damage suffered by Columbia. Even if the content of the spy-satellite pictures were alarming, there were no **contingency measures** to dock the shuttle with the space station for this type of emergency. Dealing with this kind **residual risk** is now the focus of several teams working on the future of the space shuttle.

13. Conclusion

Risk is omnipresent. Yet, our attention to it is surprise-event driven. This complacency is incarnated in the widely-held attitude: "If it isn't broke, don't fix it". Most of us tend to underestimate risk prior to a surprise-event and to overestimate it afterwards as witnessed after market corrections, the Columbia and the Challenger space missions, SARS, BSE and Foot & Mouth diseases, Chernobyl, Valdez, Tylenol, September 11 and Katrina. The challenges risk poses to management are immense. Measuring the probability and outcome (loss) is a difficult task, even for events with a historic track record. Furthermore, a host of future events are unknown. Some will remain unknowable, and elude us in spite of all our endeavors.

Tested and improved over the years, the framework discussed here has been proven to assist users shrink the set of unknown events to deal with the harsh economic realities of risk. Its effectiveness accounts for its acceptance in leading companies, financial institutions, utilities and defense establishments. In these organizations, the stakes are high. Jobs, reputations, people's health, safety, security, market share and substantial capital are frequently on the line. The framework can also lessen measurement complexity, when used in conjunction with effective risk estimating techniques. Yet, we must constantly resist the temptation to fall in love with a project dream, risk-management tools or one framework to the exclusion of others. We must relentlessly look out the window, go to the field, meet the stakeholders and validate intelligence.

As NASA's David Hall noted, "Risk Management provides a greater opportunity to enable relatively high-risk acquisition approaches (such as NASA's faster, cheaper, better) to be successful. The ultimate success of a project within the ever-tightening triple constraints of time, cost and scope depends heavily on how the project deals with the ever-present risks."[47]

Risk is embedded in every complex decision and must be managed adequately. Those who fail to act, before the challenge is present, forego opportunities. By waiting for the problems to occur, they are left with limited choices, and no lead time to adequately plan and test cost-effective problem-solving options. They pay high stress and cost premiums for negligence, and may even endanger the survival of their organization.

References & Notes

[1] The Merriam Webster Dictionary, 11th Edition, Springfield, MA. 2003.

[2] Vernon Guthrie and David Walker: Modeling Security Risk, ABS Consulting Risk Consulting Division, 10301 Technology Drive, Knoxville, TN 37932-3392, Phone: 865-966-5232. http://www.jbfa.com/about.htmln.

[3] Physical and Theoretical Chemistry Laboratory: Glossary Definition: Risk & Hazard, Oxford University, Oxford. 2003. http://ptcl.chem.ox.ac.uk/MSDS/glossary/risk.html

[4] As an illustration, car lights including brake and emergency lights reduce the likelihood of accidents while safety belt and airbags lessen the severity of the consequences (loss). In another example, passive immobilizers, brake pedal locks and steering wheel locks reduce the probability of car thefts. Vehicle tracking using Global Positioning System (GPS) reduces the gravity of the consequences of a theft by improving the likelihood and speed of stolen-car recovery. Insurance companies estimate car-theft risk as the product of the probability of a theft times its severity i.e. the magnitude of both expected and unexpected loss due to theft.

[5] World Health Organization: Reducing Risks, Promoting Healthy Life, World Health Report, October 2002, WHO, Geneva. The report confirms that ten leading risk factors globally account for one third of the world deaths.

[6] For an introduction to and further Web links about Bayesian probabilities, consult Wikipedia http://en.wikipedia.org/wiki/Bayesian_probability

[7] Al Gallo, Ted Hammer, Frank Parolek, Linda H. Rosenberg: Continuing Risk Management at NASA, The Journal of Defense Software engineering, February, 2000. www.stsc.hill.af.mil/crosstalk/2000/02/rosenberg.html

[8] For more on risk grouping, study Robert J. Finger's Risk Classification, Chapter 6, Admission, Casualty Actuarial Society, www.casact.org/admissions/syllabus/2003/ch6.pdf.

[9] The statistics 90% and 10% are based on the author 10-year consulting work with Desjardins Casualty Insurance Group.

[10] European Commission – Health & Consumer Protection Directorate-General: First Report on the Harmonization of Risk Assessment Procedures, 2000. http://europa.eu.int/comm/food/fs/sc/ssc/out84_en.pdf.

[11] Other approaches to Risk Breakdown Structures can be found in:
– R. J. Chapman: The Controlling Influences on Effective Risk Identification and Assessment for Construction design Management, International Journal of Project management, Volume 19(3), 147-160. In the first level of the risk breakdown structure, Chapman considers the environment, the industry, the client and the project.
– Audrey J. Dorofee, Julie A. Walker, Christopher J. Alberts, Ronald P. Higuera, Richard L. Murphy, and Ray C. Williams: Continuous Risk Management Guidebook, Software Engineering Institute, Carnegie-Mellon University, 1996. The focus is on software projects. The taxonomy breaks software development risk into three classes: product engineering, development environment, and program constraints. Each class is further broken down into elements. For product engineering, the elements comprise requirements, design, code and unit test, integration and test, and engineering specialties. Within each element, attributes constitute the third level. For product engineering requirements, they include stability, completeness, clarity, validity, feasibility, precedent, and scale. Design attributes comprise functionality, difficulty, interfaces, performance, testability, and hardware constraints. For engineering specialties, Dorofee et al cite maintainability, reliability, safety, security, human factors, and specifications (page 508).
– David Hall and David Hulett: Universal Risk Project, 2003. www.risksig.com/articles/UR%20Project%20Report.doc
– Donald Lessard and Roger Miller: Understanding and Managing Risks in Large Engineering Projects, International Journal of Project Management 19 (8) (2001) pp. 437-443.

[12] Definition adapted for project-based risk from U.S. Environmental Protection Agency: Framework for Cumulative Risk Assessment, EPA/630/P-02/001F, EPA, Washington, DC. May 2003. http://oaspub.epa.gov/eims/eimscomm.getfile?p_download_id=36941

[13] U.S. department of Energy: Problem Analysis and Risk Assessment, Self-Study Guide, Technical Qualification program, 1996. http://cted.inel.gov/cted/learn_resource/para.pdf

[14] Brainstorming and tools such as the Strategy Grid, from Harvard University Global System, help us craft the deliverables as will be demonstrated during the workshop.

[15] The Capability Maturity Model (CMM) for Software (SW-CMM) "is a model for judging the maturity of the software processes of an organization and for identifying the key practices that are required to increase the maturity of these processes… It is intended to help software organizations improve the maturity of their software processes in terms of an evolutionary path from ad hoc, chaotic processes to mature, disciplined software processes." www.sei.cmu.edu/cmm/cmm.sum.html

[16] David Hall and David Hulett: Universal Risk Project, 2002. www.risksig.com/articles/UR%20Project%20Report.doc

[17] David Hall & David Hulett. See above.

[18] The incubation of human-resource risks can be revealed by tracking the pattern of isolated events like absenteeism, stress, mean-time between grievances, transfer requests and resignations.

[19] A systemic risk is a series of losses across projects, organizations or markets comprising a system. Think of SARS in Toronto in 2003 or the loss of electricity across a substantial part of the Northeastern power grid caused by the Great Blackout of 1965 or the August 2003 Blackout. Consider the chain reaction caused by the discovery, in 2003, of Mad Cow disease, in two cows, one in Alberta and the other in Washington State.

[20] David Hall & David Hulett. See above.

[21] Rich Harbaugh: Skill Signaling, Prospect Theory, and Regret Theory, Claremont Colleges Working Papers, www.iupui.edu/~econ/courses/skillsignaling1.pdf

[22] Wikipedia is the source for the cost estimates and death toll is http://en.wikipedia.org/wiki/2003_North_America_blackout

[23] Canada: Royal Commission on Government Organization, Royal Commission on Government Organization [Glassco Commission]. Queen's Printer, Ottawa, 1962.

[24] Exxon Valdez: http://en.wikipedia.org/wiki/Exxon_Valdez

[25] Ocean Ranger: http://en.wikipedia.org/wiki/Ocean_Ranger

[26] John C. Tait: A Strong Foundation Report of the Task Force on Public Service Values and Ethics, Canada School of Public Service, 1996, reprinted in 2000. ISBN 0-662-64491-3.

[27] Samuel L. Brock: Planning Risk Assessments, DVM, MPH Headquarters Air Force Center for Environmental Excellence 3300 Sidney Brooks, Building 532 Brooks City-Base, TX 78235-5112. www.afcee.brooks.af.mil/products/techtrans/workshop/postworkshop03/tuesday/pm/riskassessmentprocess/Brock_abstPlanning.pdf

[28] "Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results." Reference: Wikipedia – The Free Encyclopedia at http://en.wikipedia.org/wiki/Stress_testing.

[29] Value at Risk (VAR) was pioneered by Harry M. Markowitz in 1952 to optimize a basket of investment instruments and later introduced by J.P. Morgan to measure "the downside risk of a portfolio position in assets and liabilities". VAR is a prospective, rather than historical, approach to estimate "the size and probability of a portfolio loss" over a specific short-term horizon. VAR applies only to the market risk of liquid-asset portfolios. "VAR is the basis for setting minimum capital requirements (net worth) for large international banks." These endnote excerpts are adapted from www.business.uiuc.edu/gpennacc/f461n10.ppt.

[30] In addition to Value at Risk (VAR) and stress-testing, Fault-Tree Analysis, Accident Progression Event tree (APET), Monte-Carlo Simulation, and Cross-Impact Analysis are among the most widely used tools.

[31] Frank A. Felder: The Importance of Reevaluating the Reliability Analysis of the Electric Power Grid, 2003. http://www.ksg.harvard.edu/hepg/Standard_Mkt_dsgn/Felder_Reliability_Analysis_081903.pdf

[32] Gail Charnley: Enhancing the Role of Science in Stakeholder-Based Risk Management Decision-Making, Health Risk Strategies, Washington, DC, July 2000. www.riskworld.com/Nreports/2000/Charnley/NR00GC03.htm

[33] Brian Carroll et al: International Environmental Risk Assessment and Energy Policy (Final Paper); a cooperative project of the UNC-Chapel Hill Carolina Environmental Program and the Institute of Physics and Biophysics of the University of Salzburg; Summer 2002.

[34] International Environmental Risk Assessment and Energy Policy (Final Paper), Summer 2002.

[35] Adapted from International Environmental Risk Assessment and Energy Policy (Final Paper), Summer 2002. See above.

[36] International Environmental Risk Assessment and Energy Policy (Final Paper), Summer 2002.

[37] H. Felix Kloman: Risk Management Reports, January 2003, Volume 30, Number 1, H. Felix Kloman and Seawrack Press, Inc.

[38] The White House news release January 28, 2003. www.whitehouse.gov/news/releases/2003/01/20030128-12.html

[39] Allen Monroe: The Evolving Role of the Chief Risk Officer, Risk Info, Larkspur, CA

[40] Vernon Guthrie and David Walker: Modeling Security Risk, ABS Consulting Risk Consulting Division, 10301 Technology Drive, Knoxville, TN 37932-3392, Phone: 865-966-5232. http://www.jbfa.com/about.htmln.

[41] Vernon Guthrie and David Walker: Modeling Security Risk, ABS Consulting Risk Consulting Division, 10301 Technology Drive, Knoxville, TN 37932-3392, Phone: 865-966-5232. http://www.jbfa.com/about.htmln.

[42] Adapted from Anheuser-Busch: Environmental Health & Safety (EHS) Report, 2002. www.abehsreport.com/index.html

[43] Elisabeth Paté-Cornell and Paul S. Fishbeck: Probabilistic Risk Assessment and Risk-based Priority Scale for the Tile of the Space Shuttle, Reliability Engineering & System Safety, 40. pp. 221-238, 1993.

[44] In NASA parlance, LOV means Loss Vehicle.

[45] Elisabeth Paté-Cornell and Paul S. Fishbeck: see above

[46] Elisabeth Paté-Cornell and Paul S. Fishbeck: PRA as a Management Tool: Organizational Factors and Risk-Based Priorities for the Maintenance of the Tile of the Space Shuttle Orbiter, Reliability Engineering & System Safety, 40 pp. 239-257, 1993. Square bracket text added by A. P. Martin to reflect context.

[47] David Hall and David Hulett: Universal Risk Project, 2002. www.risksig.com/articles/UR%20Project%20Report.doc