Concept Note

Improving the Management of Emerging Risks

Risks from new technologies, system interactions, and unforeseen or changing circumstances

Abbreviations used in the text:

ASAP	Aviation Safety Action Program
ASRS	Aviation Safety Reporting System
CCS	Carbon Capture and Storage
ECHA	European Chemicals Agency
EDF	Électricité de France OR Environmental Defense Fund
EMF	Electromagnetic Field
EPA	(US) Environmental Protection Agency
ER	Emerging Risk
EU	European Union
FAA	(US) Federal Aviation Administration
iNTeg-Risk	Early Recognition, Monitoring and Integrated Management of Emerging, New Technology related Risks
IRGC	International Risk Governance Council
NASA	(US) National Aeronautics and Space Administration
NTSB	(US) National Transportation Safety Board
PG&E	Pacific Gas and Electric
REACH	Registration, Evaluation, Authorisation and Restriction of Chemicals
RRF	Rapid Reflection Force
R&D	Research and Development
TEPCO	Tokyo Electric Power Company
UK	United Kingdom of Great Britain and Northern Ireland
US	United States of America
USFS	United States Forest Service

ISBN 978-2-9700672-9-0

Contents

Executive Summary

In this Concept Note, IRGC has focused on the management of emerging risks in technology and industry. We trust that readers in both the private and public sectors will find this Concept Note of interest, as the examples used illustrate how companies and governmental organisations share responsibility for enlightened management of emerging risks from technological and industrial change.

There are three broad categories of technology-related emerging risks that we are interested in addressing:

A. Risks with uncertain impacts, with uncertainty resulting from advancing science and technological innovation. The dominant feature of this category is a lack of knowledge and experience about consequences that could result from deploying new technology, in the form of new processes and products. The governance issues for category A risks deal with the decision to allow such technology in commerce, and the implementation of appropriate risk management measures to avoid or mitigate potential adverse consequences. Current examples include products and processes in nanotechnology or synthetic biology.

B. Risks with systemic impacts, stemming from technological systems with multiple interactions and systemic dependencies. The defining feature of category B risks is a loss of safety margins due to high levels of connectivity and interdependence. The main issue here is not the risk of the technologies (this may be known or well-estimated), but the interactions of these risks with other types of risks or activities that could lead to non-linear impacts or surprises. Examples of complex interconnected systems are numerous in energy, transportation, communication, and information technology.

C. Risks with unexpected impacts, where new risks emerge from the use of established technologies in evolving environments or contexts. The main problem here is that the potential impacts of familiar technologies (both in terms of probability and magnitude) may be altered if they are operated in a different context or organisational setting. Governance of these risks would seem well established, but may in fact be inadequate. The change in context that can lead to a risk emerging may involve ageing of infrastructure, complacency, and/or overconfidence in the ability to deal with unexpected events. The commercial aviation industry provides a useful example of the importance of effectively managing category C risks.

Following IRGC's work on risk governance deficits [IRGC, 2009a] and contributing factors to risk emergence [IRGC, 2010a], the focus in this Concept Note is on **how to overcome the major obstacles that commonly prevent organisations from improving their emerging risk management**. The eleven themes presented here are all relevant for the three categories of risk A, B and C described above, although specific approaches to risk management may differ depending on the category of risk being addressed.

Each theme derives from one obstacle and is described in such a way as to provide clarity and operational significance for managers who have the task of identifying, assessing, evaluating, prioritising and managing the early phases of development of an emerging issue. These eleven themes interact considerably,

but for conceptual clarity, we have grouped them according to the relevant dimensions of risk governance within which they fit best. These four dimensions of risk governance (from the broad, foundational level to the more specific) and the eleven themes are shown in the figure and summary table below.

Overview: the four risk governance dimensions and the eleven themes

LEVEL	THEME
Risk governance Create and maintain overarching management and organisational principles for effective emerging risk anticipation.	1. Set emerging risk management strategy as part of overall strategy and organisational decision-making 2. Clarify roles and responsibilities
Risk Culture Establish a proactive risk management culture, with systematic surveillance and the ability to retrieve and evaluate information.	3. Set explicit surveillance incentives and rewards 4. Remove perverse incentives to not engage in surveillance 5. Encourage contrarian views
Training and capacity building Capacity and resources are needed to create and maintain a culture that encourages emerging risk management.	Build capacity for: 6. Surveillance and foresight activities 7. Communicating about emerging issues and dialoguing with key stakeholders 8. Working with others to improve the understanding of, and response to, emerging risks
Adaptive planning and management Activities related to emerging risk identification, assessment, management and communication should be revisited and updated on a regular basis.	9. Anticipate and prepare for adverse outcomes 10. Evaluate and prioritise options; be prepared to revise decisions 11. Develop strategies for robustness and resilience

Introduction

The publication of this Concept Note marks the beginning of the second phase of IRGC's project on Emerging Risks. The first phase, which culminated in the publication of the IRGC Report, *The Emergence of Risks: Contributing Factors* [IRGC, 2010a], aimed to raise awareness and improve the understanding of emerging, systemic risks. This second phase aims to go further and to develop practical guidance for how organisations can better anticipate and respond to emerging risks.

This Concept Note is an effort to set forth ideas for more proactive management of emerging risks. It is intended for senior management in private sector organisations, although the ideas also apply in the public sector, and particularly, in government agencies with responsibility for establishing and enforcing risk regulation. It is not intended for a technical audience of risk analysts, although we have referenced what we believe are exemplary publications from the technical and management literature (see Appendix 1). The aim is to stimulate discussion at the conceptual and policy level on how management of emerging risks can be improved, and on how further research in a variety of disciplines might contribute to such improvement.

We use in this Concept Note the same definition as in *The Emergence of Risks: Contributing Factors*: an emerging risk is "a risk that is new, or a familiar risk that becomes apparent in new or unfamiliar conditions." And we note also that "of particular interest to IRGC are emerging risks of a systemic nature, which typically span more than one country, more than one economic sector, and may have effects across natural, technological, and social systems" [IRGC, 2010a].

In this Note, IRGC focuses on the management of emerging risks in technology and industry. Some of what is proposed below also applies to risks emerging in other sectors, for example in health, the environment or financial markets. However, we have deliberately chosen to focus on technology and industry, as this is an area that is less developed in other IRGC work. We trust that readers in both the private and public sectors will find this Concept Note of interest, as the examples in the Note illustrate how companies and governmental organisations share responsibility for enlightened management of emerging risks from technological and industrial change.

To begin with, we define three categories of technology-related emerging risks[1]: A. those associated with advancing technology and lack of knowledge on the potential impacts (uncertain impacts); B. risks associated with evolving and interacting systems (systemic impacts); and C. risks that emerge in unexpected applications because of unforeseen or changed circumstances (unexpected impacts). In all categories, managing emerging risks requires assembling and managing knowledge relevant to the risks. Especially in the third category, where risks may suddenly materialise in the form of a large accident or disaster, improvements in risk management require improvements in acquiring and disseminating risk-relevant knowledge, decision authority and the ability to change the status quo throughout an organisation, and more broadly, among all the organisations that may be bound together by a shared risk.

[1] Note that there are overlaps between these three categories.

IRGC and other organisations with an interest in improving the management of emerging or unforeseen risks also have a strong interest in risks from all three categories. In categories A and B, it might be expected that dealing with possible risk issues is already on the agenda for top management in the private and public sector organisations involved. The IRGC risk governance framework [IRGC, 2005] involving iterative dialogue supported by analysis was developed to aid in these situations, and the IRGC Report *Risk Governance Deficits, an analysis of the most common deficits in risk governance* [IRGC, 2009a] along with its companion Policy Brief [IRGC, 2010b] are intended to provide guidance on specific issues where improvement is needed. Another useful reference, particularly where dialogue and public involvement is concerned, is the 2008 US National Research Council Report [Dietz and Stern, 2008].

We then move on to identify and describe eleven themes that suggest approaches that can be used to overcome common obstacles that prevent the improvement of emerging risk management. These eleven themes range across multiple dimensions of risk governance, from the broadest level of strategy and management, which we simply term “risk governance”; to “risk culture”, which includes organisational norms, values and attitudes related to risk; to “training and capacity building”, which builds on the aforementioned two dimensions; and finally “adaptive planning and management”, which are on-going tasks and reflect an organisation’s overall risk governance policy and culture.

1. Three categories of emerging risks

A. Uncertain Impacts: Uncertainty resulting from advancing science and technological innovation

This first category, A, has as its dominant feature the lack of knowledge and experience about consequences that could result from deploying new technology, in the form of new processes and products.

As a consequence of such unknowns, the governance issues for category A risks deal with the decision to allow such technology in commerce, and, if allowed, to develop and implement appropriate risk management measures to avoid or mitigate potential adverse consequences from the new technology. There can be high uncertainty and a lack of basic knowledge about the character and the extent of impacts that will result if the technology is deployed. Current examples of interest to IRGC include products and processes in nanotechnology [IRGC, 2009b] and synthetic biology [IRGC, 2010c]. Other examples include technologies already in wide use, but having an uncertain potential for risks that may appear after a long latency period. Health impacts of electromagnetic fields (EMF) from power line and cell phone frequencies is an example ([Kheifets et al., 2010], also as a case study p. 66 in [IRGC, 2009a]). Another aspect of category A risks is that they may be site-specific, such that detailed experience may be needed to resolve scientific uncertainties for deployment of the technology in a specific location. An example studied by IRGC is the use of carbon capture and storage (CCS) technology for mitigating climate change: the capture of carbon dioxide from fossil-fuel burning power plants and placing this carbon dioxide into underground geological formations [IRGC, 2007a].

The problem of managing risk for advancing technology is a recurring theme. Historical examples include new drugs with unknown efficacy and side effects, and new chemicals that have economically useful properties but may cause toxic effects in humans or the environment. The risk governance aspect of category A emerging risks is that the decision to deploy the technology (as a product, or process) is being explicitly considered both by private organisations and by government authorities with responsibility to protect public interests, including public health and safety, and the environment. The process of taking a new drug, chemical, or device though research into clinical trials and commercial demonstration, and then seeking approval from regulatory authorities, is well established in many industries. New applications (such as nanotechnology, synthetic biology, or CCS) involve resolving scientific uncertainty, coping with societal risk perception and economic viability. These applications may also involve refining, strengthening, or reorienting governmental regulation for management of the risks.

Often the process involves initial experimentation in carefully confined laboratory facilities, then limited small-scale tests, then a careful evaluation of benefits, costs, and risks before allowing the technology (product or process) into widespread use. The usual situation is that leadership in the research and commercialisation process comes from private corporations, and regulatory agencies react to applications for approval of new products. In some cases, especially where the costs and potential consequences are large, leadership has been with government. An example of the latter is the development of light water nuclear reactors for electric power generation. The example of prescription drugs should remind us that many widely used products are

intended to be used only under qualified professional supervision, to avoid misuse and consequent high risks.

B. Systemic Impacts: Technological systems with multiple interactions and systemic dependencies

This second category, B, is characterised primarily by a loss of safety margins in the context of one or more systems. As noted in [IRGC, 2010a:22-23], this loss of safety margins, or loss of buffering capacity, occurs because "the level of connectivity in many of today's social and technical systems is greater than the past and interconnections are increasing. The pace at which many of these systems operate is becoming faster and many are operating under higher levels of stress." The result is that the systems may become more vulnerable to disruption and failure – there is interplay between the systems, the technologies involved, and a variety of risk factors, and existing risk management may therefore be inadequate.

The main issue here is not the risk of the technologies (this may be known or well-estimated), but the interactions of these risks with other types of risks or activities that could lead to non-linear impacts or surprises. Examples of complex interconnected systems are numerous in energy, transportation, communication, and information technology. For purposes of illustration, management of a utility with responsibility for transmission and distribution of electricity and/or natural gas is a good example. In many countries such utilities are private corporations operating under government regulation, and in other countries they are owned by the government. System management, and the need for long-range system planning, face essentially the same issues, whether ownership is private sector or public, although different institutional structures are used for decision-making.

Governance of complex systems in modern industrial societies is usually mandated with considerable specificity by contracts and government legislation and regulation. While there may be difficulties and perhaps ambiguities in determining how much system capacity is enough and which technological alternatives should be used for the system components, those who own, operate, or use such systems can readily identify the combination of private sector top management and regulatory authorities that are in charge for such decision-making. We view the governance aspect of category B emerging risks as follows: there is (or should be) an on-going examination of the "state of the system" and planning for its future, especially as to whether the safety margins are adequate and whether the right choices are being made for system components as the system evolves in time. The IRGC project on "Managing and reducing social vulnerabilities from coupled critical infrastructures" [IRGC, 2007b] explored how today's complex systems interact with each other, and how a disruption in one system can quickly propagate into other systems. Analysis of such issues can become formidably complex, and there are a wide range of important uncertainties to be considered. Such analysis is typically carried out by highly trained system specialists.

The interaction of systems and dependencies among systems, however, may indicate the need to supplement traditional analysis done by system specialists. The impacts and risks across the systems must be considered. Use of ethanol from corn is an example, where there is concern that adverse effects on food production may offset gains from replacing petroleum-based fuel with a renewable biomass fuel [IRGC, 2008a]. Many systemic issues may involve

natural systems where overuse of a “commons” resource – the capacity for resource removal, such as grazing by animals in a common pasture – was recognised in medieval times as having the potential to cause damage. There may also be technological and societal systems that interact with the natural system. Climate alteration is an example of an emerging risk area in which many natural, societal and technical systems are involved. Many information technology risk issues involve the interaction of multiple systems.

C. Unexpected Impacts: Established technologies in evolving environments or contexts

Category C risks are those that emerge, not from new technology or complex systems, but as surprises in established areas of technology and human activity where it was presumed that risks were being well-managed.

The main problem here is that the potential impacts of familiar technologies (both in terms of probability and magnitude) may be altered if these technologies are operated in a different context or under different organisational settings. Governance of these risks would seem to be well established, but may in fact be inadequate (or no longer adequate) for a variety of reasons. The change in context that makes for an emerging risk may involve ageing of infrastructure, complacency, and/or overconfidence in the ability to deal with unexpected events. Category C risks may emerge when regulatory institutions or corporate leadership weakens, as from budget cuts or deficiencies in leadership. For category C risks, it is usually the case that the technology, product or processes involved have been previously approved and accepted as a part of on-going commerce. While there may be concerns about long-term health, safety, environmental, economic, or social impacts, for emerging risks in category C, there may be little or no top management attention to the adequacy of risk management until a serious threat or a catastrophe occurs. Category C is intended for the neglected “old hat” risks, where the planning, risk assessment, and risk management procedures were established in the past, but surveillance and rethinking of risk management may now be inadequate, or even absent. The governance may be essentially that of on-going operational management, for technologies, products, and processes that have already been accepted into national and international commerce as acceptably safe. Across a wide spectrum of commercial activities in modern society, these operational aspects are often quite detailed and complex and society depends on them running smoothly and with disruptions happening infrequently.

The commercial aviation industry is a useful illustrative example. Every day, a very large number of commercial airliners take passengers and freight from multiple points of origin to multiple destinations all over the world, using highly sophisticated aircraft, logistical support, and communications. In most countries accidents involving loss of life of passengers and crew are now exceedingly rare. This should be viewed as a remarkable success achieved over many decades by this industry and its regulators. It is therefore an example that other sectors of commerce might usefully study, to see what they can learn to improve their management of risk [Phimister et al., 2004; Tamuz, 2004].

The fundamental focus for category C emerging risks is that of appropriate resource allocation and knowledge management, particularly, knowledge to allow foresight of situations that could lead to a disruption or accident. These situations could be an internal mishap, such as a pilot or air traffic controller

falling asleep while on duty, or an external event such as a volcano eruption putting ash high in the stratosphere, which could damage jet engines and lead to engine failure. In categories A and B it may be assumed that top managers in corporations and regulatory oversight agencies are monitoring and evaluating the risks. Many natural disasters should be regarded as falling into category C. The risk only emerges with the disaster event, although history may indicate many previous occurrences of the same type of event – hurricanes and severe storms, floods, volcano eruptions, earthquakes, tsunamis, and meteorite/asteroid impacts. Decision-makers and the public may have failed to prepare. In really severe disaster situations, preparations may be overwhelmed by the magnitude of the event. Another similar subcategory is the ageing of infrastructure, such as dams, bridges, tunnels, and buildings. Are the risks brought on by such ageing really "new or unfamiliar conditions" – and therefore appropriate to include as emerging risks? We believe the judgement must be made based on the perception of corporate and government leadership in assessing and managing such risks.

Figure 1: Three categories of emerging risk

Category	Dominant feature	Governance issue	Examples
A, Uncertain impacts: Uncertainty resulting from advancing science and technological innovation	Lack of knowledge and experience about consequences that could result from deploying new technology	Given the uncertainties about potential consequences, what risk management measures are adequate and needed for technologies, processes or products with significant benefits but unknown risks?	• Products and processes in nanotechnology or synthetic biology • Health impacts of EMF • Carbon capture and storage technologies
B, Systemic impacts: Technological systems with multiple interactions and systemic dependencies	System complexity and interconnectedness: Loss of safety margins within evolving and interacting (complex) systems	On-going examination of the state of the system and planning for its future (Are safety margins adequate? Are the right choices being made for system components as the system evolves in time?)	• Utility networks (gas and electricity) • Ecosystems • Climate change
C, Unexpected impacts: Established technologies in evolving environments or contexts	Surprises from knowable risk factors: Unforeseen or changed circumstances	Governance may seem to be well-established, but may in fact be inadequate for a variety of reasons. (Is there complacency, resulting in failure to observe and adapt to changing, potentially dangerous conditions?)	• Commercial aviation safety • Nuclear power • Ageing of infrastructures

Lessons learned from past experiences

There have been many past instances of a risk materialising with a sudden and catastrophic failure. From the perspective of professional risk analysts, such failures keep occurring and even follow a familiar pattern. Some notable examples include:

- On 23 July 2011, a high-speed train in China hit the rear of another high-speed train, which had stopped unexpectedly after being hit by lightning. More than 40 people died and several hundred were injured. The immediate cause of the collision appeared to be a signal failure, a green light instead of red to inform the operator of the second train of the first train in its path. Luo Lin, a top Chinese safety official heading the inquiry, said the accident was "completely avoidable" and blamed "serious design flaws." [BBC, 2011].

- Tokyo Electric Power Company (TEPCO) failed to anticipate that a tsunami of a certain size (as occurred on 11 March 2011) could disable backup electricity supply, and therefore, the cooling systems needed to protect the nuclear fuel in the reactor cores and storage pools [AP, 2011]. A series of equipment failures, meltdowns and releases of radioactive materials ensued, comprising the largest nuclear disaster since Chernobyl. Even the most cursory examination of the history of the north-eastern coastal area of Japan, including the Fukushima Daiichi plant complex of six nuclear reactors, would have identified that tsunamis have occurred many times in recorded history, and that these waves have often reached heights of tens of meters and devastated coastal communities. However, no one at TEPCO appears to have foreseen this possibility. TEPCO's failure to anticipate the impact of a large tsunami on its Fukushima Daiichi reactor complex has led to resignation of the Chief Executive Officer and a write-off in this current year of 15 billion dollars [Tabuchi, 2011].

- Air France flight 447 crashed into the Atlantic Ocean on 1 June 2009, with the loss of all on board. Information on the events leading to this highly unusual loss of a modern jet airliner has emerged with the recent recovery of the flight data and cockpit voice recorders. Icing conditions disrupted the Pitot airspeed sensors, and the first officers were perhaps overwhelmed by warnings of systems failures. The first officers were also faced with multiple confusing low-speed alerts that alternately were presented to them, then supressed, then reactivated. These factors affected the ability of the first officers to accomplish a relatively straightforward manual recovery from the deep stall and rapid vertical descent conditions. The airplane's more experienced captain was away from the cockpit at the critical time, a few minutes before the descent from cruising altitude into the ocean [BEA, 2011a and b]. The coupling of design and training problems is currently the subject of considerable review.

- A misreading of instruments monitoring water flows on 28 March 1979 led to the meltdown of Three Mile Island 2 reactor, the worst nuclear power plant accident that has occurred in the United States. The subsequent investigation by a Presidential Commission concluded that the deficiency was not simply a matter of operator error, it was a pervasive "mind-set" that more automation was better, rather than an understanding at all levels of management that safety depends on being prepared through training, experience, and vigilance to diagnose and manage inherently dangerous

technology [PC, 1979]. The US nuclear industry made extensive adjustments in management following the Commission's recommendations.

To this list, we could also include the blowout of the Deepwater Horizon drilling rig in the Gulf of Mexico [BOEMRE, 2011; OSC, 2011], the explosion of stored ammonium nitrate fertiliser at Toulouse in 2001 [FABIG, 2011], explosion of a petroleum vapour cloud at Buncefield, UK in 2005 after a fuel tank was overfilled [Buncefield, 2006], and many other examples.

The common thread in each of these accidents is that information that was, or should have been, available was not effectively used to avoid the accident or mitigate its severity. While the primary cause of the accident may have been a technical failure or natural disaster, the secondary cause, largely determining the magnitude of the consequences, was this lack of information stemming from an inadequate risk and safety culture. A race to save time and to cut costs may have led to inadequate surveillance, staff training or operational and maintenance practices, affecting not only the likelihood of technical failures, but also of human failures.

The importance of the human factor – for example of mind-sets, training and the ability to think outside the box – is demonstrated by the following two examples, which were very nearly catastrophic accidents in the same category as the examples above, but for the reactions of the people involved:

- US Airways flight 1549 lost power in both engines after flying into a flock of geese shortly after take-off from New York's La Guardia Airport on 15 January 2009. But Captain Chesley ("Sully") Sullenberger brought the plane down onto the Hudson River, and all passengers and crew members were rescued without a single death or injury [New York Times, 2009].

- Apollo 13 had a potentially catastrophic accident when an oxygen tank overheated and exploded 200,000 miles out, en route to the moon in April 1970. The three astronauts aboard and the NASA ground support team were able to improvise by using the lunar landing vehicle as a "life boat" and shutting down all non-essential uses of electricity, including the navigation aids. Essential course corrections were achieved manually by having the astronauts sight the earth, sun, moon, and stars out the windows of the spacecraft and bring it into proper orientation with thrusters and the rocket engine [Lovell, 1975].

Overall, these examples demonstrate that the need to develop and maintain an exemplary safety culture applies to all inherently dangerous technologies.

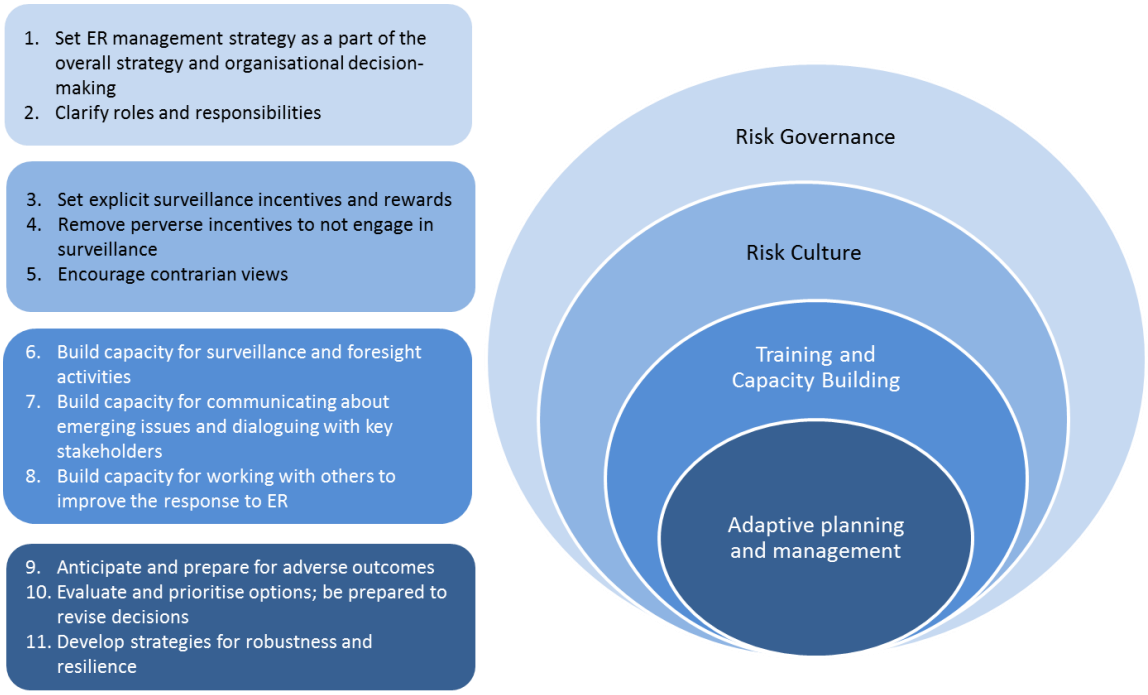
There are of course many situations in which information may be erroneous or uncertain, and what is believed by segments of the public may not correspond with the judgment of experts. Peer review and careful checking of sources are essential in any good knowledge management system. Such efforts are often time-consuming and expensive, but development and retention of accurate information relevant to risk must be central to good corporate risk management practice. Corporate managers should review the activities in their organisations, asking whether there is potential for a risk to materialise in the form of an unanticipated catastrophe. If the answer might be yes, they should then ask themselves what they can do to identify and minimise such potential. This Concept Note is intended to assist them in this process.

2. Eleven Themes for Improving the Management of Emerging Risks

At a working session in the spring of 2010 a small group from IRGC's Scientific and Technical Council worked on identifying the main obstacles that need to be overcome for improving the management of emerging risks. This work follows from and draws on many of the risk governance insights set forth in IRGC's previous reports on Risk Governance Deficits [IRGC, 2009a; critical review in Aven, 2011] and Emerging Risks [IRGC, 2010a]. Readers may find it useful to also refer to these reports for context. Each of the themes presented below derives from a key obstacle frequently encountered in emerging risk management. The themes are described in such a way as to provide clarity and operational significance for managers who have the task of identifying, assessing, evaluating, prioritising and managing the early phases of development of an emerging issue.

The 11 themes identified can be grouped according to 4 main dimensions. The grouping below begins with **risk governance** (a concern of strategy, top management and organisational design), then moves on to an organisation's **risk culture**, to **training and capacity building**, and finally, to **adaptive planning and management**, the latter two being on-going activities within an organisation that reflect its risk governance policy and risk culture. We envision that these themes interact considerably.

Figure 2: The eleven themes and four risk governance dimensions



2.1. Risk Governance: strategy, management and organisational matters

Risk governance relates to the identification, assessment, management and communication of risks in a broad context. In the context of emerging risks, it starts with setting a strategy, which must be endorsed at the highest level of management. The strategy will then be implemented in policies, management processes and organisational matters. It is commonly understood that risk can be of endogenous or exogenous origin. Top management, in both the public and private sector, must clarify a strategy for anticipating new risks early on, and for developing preparedness to face emerging issues that may arise from either inside or outside their organisation. If this is not achieved, it is likely that, sooner or later, the organisation will be taken by surprise and its business activity and/or reputation severely damaged.

1. Set emerging risk management strategy as a part of the overall strategy and organisational decision-making

Within a single organisation carrying out research on an emerging technology, and even more within a group of organisations responsible for management of a complex system or a set of interconnected systems, determination of policy on a specific risk issue may be a difficult and complex process. We stress here the importance of including risk aspects in the management process, and that, once policy has been established governing the risk aspects of an organisation's activities, this policy should be understood and adhered to throughout an organisation.

Safety should not to be compromised for cost saving or meeting milestones on time. Many organisations with excellent safety culture make strategic and successful balancing of safety over cost and timeliness a core principle. Again, the commercial airline industry provides a good example.

Establishing a strategy and policy must be viewed as a decision-making process that depends on alternatives (which may be limited by what is technically possible, and by legislation and regulation), on the information available (which can be expected to change over time), and on transparent decision criteria – the overall economic, environmental, and social goals, which may require clarification and which almost always involve trade-offs and attention to sharing/equity aspects.

Achieving clarity and mutual understanding among organisations may take considerable communication effort. For example, corporations would like clear rules from regulators; regulators would like information and detailed proposals from those to be regulated.

The process of making good decisions to establish strategy and policy in category C emerging risks may be more subtle and difficult, because the important issue may involve changes that are not easily recognised, and actions that are at the level of operational practices. In general, an organisation wants to encourage vigilance and avoid complacency, so that threats and risks are well understood and under good control. But how can that goal be achieved in an evolving and complex environment? The most difficult part of the problem may be in identifying these threats and risks.

Especially for large organisations with responsibility for systems, it will be appropriate to have an early-warning activity as part of foresight activities.

Strategic risk management in corporations: the example of DuPont

Emerging risk management has always been a strategy of innovative companies, which have to manage the business opportunities of developing new technologies, together with the associated risks. The approach used by Du Pont de Nemours when addressing potential health, safety and environmental risks related to nanotechnology provides an example of how management of potential threats caused by new technology was prioritised at the highest level and a clear strategy was followed.

Equally pre-occupied by safety and the pursuit of opportunity, the Board of DuPont, represented by its Chairman, decided that voluntary corporate leadership was required in order to manage the potential risks from nanotechnology. A partnership with the non-profit environmental advocacy group Environmental Defense Fund (EDF) was formed, and the two organisations thus began a collaborative effort to develop a Nano Risk Framework, aimed at setting interim standards for nanotechnology in its early stages, while regulations were still under development.

"An early and open examination of the potential risks of a new product or technology is not just good common sense – it's good business strategy" [Krupp and Holliday, 2005]

The process called for cooperation by all interested stakeholders and the final framework was the result of a two-year stakeholder dialogue project and was created by a multidisciplinary team from both organisations [Environmental Defense Fund and DuPont, 2007].

The EDF-DuPont Nano Risk Framework assembles a process for describing materials and applications, for exploring properties, hazards and exposure, and for evaluating risks. Furthermore, it gives orientation to both risk assessment and management, and provides guidance on how to implement and document decisions and to review the entire risk governance process (for more information on the EDF-DuPont Nano Risk Framework, see IRGC, 2008b, pages 39-40).

2. Clarify roles and responsibilities

In an organisation, who is responsible for identifying and dealing with emerging issues that may affect the organisation? What information is being developed to support emerging risk management decisions? What are the decision criteria? Who takes what roles in the process? For emerging risks in categories A, B, and C, the answers may differ considerably, and it is important to clarify these differences before proceeding into detail on how risk management can be improved.

An organisation's policies must enable those at lower levels in a corporation to take responsibility for identifying and fixing problems. Reducing risks can be attempted through setting up a myriad of detailed rules, but better corporate policy and practice may be to have smart, experienced people who understand

the reasoning behind the rules and can think through situations where exceptions are needed. The airline industry selects pilots who are highly intelligent, resourceful, and technically educated; they are then informed and trained to deal with as many emergency situations as can be foreseen based on careful recording of past events involving near misses as well as accidents. An implication for other industries seeking improvement in operational safety is to pay well in order to attract employees who can manage operational situations thoughtfully and effectively, and to spend more money for emergency training and back-up capability for emergencies.

There need to be good processes for communication and resolution of differences among different divisions and different levels of management within an organisation. The Chris Argyris approach described in [Argyris, 1990] emphasises dialogue and debate among those with relevant knowledge, and avoiding situations where a boss with experience acquired long ago dictates a decision, which could be based on out-dated or poor information.

A risk situation in category A usually has active management and a goal of developing, evaluating and commercialising a new technology (or product, or process), which may be perceived as having uncertain side effects that pose threats, such as to public health or the environment. Broad uncertainties usually preclude initial characterisation as probabilities: often it is not clear what the threats are, there is little information on which to base assessment, and there may be many divergent opinions. The need is to understand the "uncertainty space," and to be honest about what is not yet known, in discussion between proponents and opponents of new technologies. Managers must direct a research and experimental trials process intended to reduce important uncertainties on the positive and adverse impacts of the new technology, product, or process. These impacts must become understood to a level that will enable decision-making, both at the corporate and social levels. Often, a lengthy decision-making process is involved at the research level, leading to decisions on whether (and under what conditions) the technology, product, or process should be brought into commercial use. In this decision process, it should be made clear, both for organisations doing the research and development and for public sector organisations responsible for regulation, what the respective roles and responsibilities are, for each organisation.

For category B, any organisation involved in a system where risks may come from interdependencies should perform anticipatory risk assessment and have a foresight and evaluation team in place, so there is an early warning capability to identify and rectify system weaknesses – that is, "loss of safety margins." But often interactions among systems, and among the corporate and governmental organisations that are operating and regulating these systems, are not receiving adequate attention. Again, roles and responsibilities must be clearly defined, so that problems are identified and receive attention by the appropriate managers in the appropriate organisations.

Especially in considering category C emerging risks, we must acknowledge the difficulty in judging that an organisation is failing to be vigilant and follow best practices in managing risk and achieving adequate safety. Responsibility for noticing deficiencies and needs for change should be diffused throughout an organisation, and everyone should believe they have a potential role in making improvements. Responsibility for risk management is not only for the top of an organisation, but should occur at all levels of the work force.

To use a military inspection analogy, visiting senior officers may examine a ship or a group of soldiers to see if the brass is shined and the boots are polished, but it is much harder to determine whether the soldiers and sailors can shoot accurately, reload quickly, or function effectively as a team to carry out a complex task. Readiness and effectiveness must be assessed based on delegation of responsibility down through an organisation and careful observation of how well the parts of the organisation are functioning.

Similar lessons are applicable to businesses. First-line supervisors must set examples and train the team of workers; they must reinforce best practices and reform substandard practices. Organisations must not remain static in their practices, but must find ways to update and innovate. They must keep informed on what others (customers, suppliers, competitors) have learned and how their practices are evolving.

Clear responsibility for risk management must be assumed at the highest levels of the company and then delegated properly throughout the organisation. Discussion of improbable adverse (as well as anticipated) scenarios must be encouraged by company leadership, thereby spreading risk management functions throughout the company.

2.2. Risk Culture

Organisations need to establish a proactive emerging risk management culture, with systematic surveillance and ability to retrieve and evaluate information. Risk culture includes all norms, values and attitudes of an organisation towards identifying, assessing, managing and communicating risks and uncertainties. The risk culture itself must be communicated, both internally and to outside parties.

Perhaps the most important aspect of a proactive risk management culture is affirmation through policy that the organisation must be continually observing, reporting and learning how to do better. This is a culture that is readily linked to or derived from good laboratory practice in scientific organisations, where experimental data are carefully and systematically recorded and kept on file for subsequent use. But many organisations – sometimes including scientific laboratories – find such careful and systematic data recording to be tedious and time-consuming, so this task does not get carefully done. When management allows the practice of measuring and recording results to become lax, then opportunities to learn may become obscured and lost. The history of science is filled with examples where an unexpected result observed in the laboratory led to an important advance.

Organisations should devote resources to preparing for speculative risks and rewarding those who do the job with competence and creativity. Unless managers give priority to establishing an appropriate internal culture for dealing with emerging issues, the motivation may not materialise. Preparation may entail a wide range of activities from establishing early warning systems to designing plans for prevention, mitigation, and adaptation – including recovery plans in the event that damages occur.

3. Set explicit surveillance incentives and rewards

If the overarching need to improve management for emerging risks is to find, retain, and disseminate risk-relevant information, then an organisation wishing to improve its risk culture must begin by reviewing its incentives for carrying out these activities. It must set incentives to establish effective early warning systems, to achieve good exchange of truthful information, and to report, including on information that could be upsetting or controversial (see theme 5). It can be a very unpleasant experience to express disagreement with the boss. But the wise boss will encourage his or her people to speak up, especially when they have information indicating an emerging risk in need of immediate management attention.

In the context of research and development on emerging technologies, category A, the goal should be to make good decisions on which R&D projects should receive more resources and move forward, not success for a particular project or technology. Rewards and incentives should be for good decision-making, including decisions not to proceed further because of potential high risk. Companies and economic systems that reward commercial success, but not prudent withdrawal or remedial action in the face of high risk, may create incentives that go the wrong way, such that risks are not properly identified and then avoided or minimised.

Emerging risks in large and possibly interconnected systems (category B) may have this same incentives problem, but in a much more complex context. Again, the incentive and rewards should be for providing information to enable better decision-making, even if, in the short run, it makes for more complex analysis, longer "to-do lists," and even interruptions to operations. Most of us who have owned and operated an automobile over a long period have learned to be sensitive to changes in engine noises and vehicle handling. Such "weak signals" can indicate the need for maintenance, which if not done promptly, can require much more expensive repair. The same principle holds for most infrastructure and infrastructure systems, including transportation, energy, telecommunications, and information storage and retrieval. For complex coupled systems in a changing environment, there is a very strong need for good anticipatory risk assessment and strategic planning, with rewards for those who can achieve a better understanding of the systems and improve their safety management.

Technological systems that have been in place for a number of years (category C) may lose the people who pioneered them: people who understood risks and focused on creating an excellent safety record. Their successors may assume that safe operations, once achieved, will continue. But the people, the equipment, and the environment may change. Safety should not be slighted compared to other objectives. Emphasis on short-term cost savings and minimal compliance with government regulations may provide some immediate gains in an organisation's financial statement, but there can be long-term adverse impacts that more than offset these gains. Enlightened managers should go beyond minimal compliance with the regulations, assess the long-term implications, and be rewarded for good decision-making for the long-term, even when short-term costs for maintenance and retrofits mean that financial statements in the short-term are not as good as some might have expected.

Many areas of commerce involve inherent health or injury risk if good practices are not followed. The construction industry, and even home workshops, provide many simple and widely known examples: wear a hard hat and other protective clothing and devices (e.g., shatterproof glasses) at the job site; tools and materials that might be dropped from high levels must be tied down so they do not hit people below; etc. These examples indicate that incentives are not just compliance with rules and monetary rewards, but rather can take the form of recognition that all persons involved belong to a shared culture of doing the right thing, because if you don't, someone can get hurt as a result.

For emerging risks in our category C, at all levels in the organisation, people should recognise when something isn't right, they should work toward fixing it, and be rewarded for their efforts to identify and fix problems. A common deficiency is to simplify by ignoring weak signals and only pay attention to the strong ones. This "all or nothing" trap – assuming there is a risk, or there is no risk – should be avoided. Weak signals should be investigated, even when much of the time the investigation might show nothing there – a "false positive." But you don't want to set up incentives that will inhibit the cry of "wolf" when there might, sometime, really be a "wolf" there. It may be appropriate to allow many false positives in order to avoid an extreme false negative – an indication that all is well, when in fact a disaster is imminent.

Inadequate surveillance and information gathering: rupture of a PG&E gas pipeline

On 9 September 2010, a 30-inch natural gas pipeline ruptured in San Bruno, California, a residential suburb south of San Francisco. The resulting explosion and fire destroyed 38 homes, killed eight people, and injured 58 more, ten of them seriously. This gas pipeline was owned and operated by Pacific Gas and Electric (PG&E). The rupture occurred in a pipe installed in 1956 that did not meet PG&E company standards or industry standards of the time. PG&E had never inspected this section of pipe from the inside since its installation, and did not know that the pipe contained longitudinal (i.e., along the pipe) welds, some of which only partially connected the two sides of the pipe. PG&E had reported, incorrectly, that the pipe was seamless. One such partial longitudinal weld weakened from fatigue and ruptured after a small surge in pressure during a repair at a pumping station [NTSB, 2011]. Following the incident, PG&E took 95 minutes to stop the flow of gas and isolate the rupture site – a response time judged "excessive" by the National Transportation Safety Board (NTSB).

Federal regulators had warned gas companies of danger from pipelines installed before 1970 and constructed using the outmoded longitudinal weld technology. Previous accidents in the PG&E gas system had shown deficiencies in PG&E's record keeping, its emergency response, and unacceptable delays in shutting down its pipelines. PG&E did not recognise the high risk for defective pipe under a residential community, and regulatory rules did not force inspection. Inside-the-pipe inspection using "a pig" was not possible in this old pipe. Other inspection methods might have been used, but were not.

PG&E has suffered a great deal of adverse publicity and is the subject of multiple lawsuits from victims of the fire. The NTSB report criticises PG&E on many details and in general: "The PG&E gas transmission integrity management program was deficient and ineffective…PG&E's multiple, recurring deficiencies are evidence of a systemic problem" [NTSB, 2011]. The NTSB report also criticises the California Public Utilities Commission and the federal Pipeline and Hazardous Materials Safety Administration for lax oversight [NTSB, 2011].

On October 7, 2011 the Governor of California signed legislation requiring automatic shutoff values and other enhanced safety measures on natural gas transmission lines [CA.gov, 2011]. As of October 2011, PG&E is in the penalty consideration phase of an investigation by the California Public Utilities Commission for "whether PG&E's gas transmission pipeline recordkeeping was unsafe, whether it violated the law, and if so, whether deficient PG&E record keeping caused or contributed to the pipeline rupture in San Bruno on September 9, 2010" [CPUC, 2011]. A lack of incentives to search out and disseminate available risk information, and to go above and beyond the minimal regulatory requirements, contributed to the occurrence and severity of this accident.

4. Remove perverse incentives to not engage in surveillance

As seen above, there are some obvious advantages to an organisation's engaging regularly in surveying its environment, identifying possible emerging

risks, gathering information on those risks, and beginning to devise strategies to reduce future vulnerability.

However, senior leadership must be receptive to negative information, and not in denial. It must enable such information to be accepted and used and avoid a "don't shoot the messenger" threat to those people engaged in emerging risk surveillance.

There are many organisational and cultural settings in which managers find it locally rational to not engage in such surveillance. Suppose that the organisation's culture is such that, having identified an emerging risk, there is little or nothing it is likely to do about it. If the risk comes to pass, the fact that it had previously been identified builds a record that the organisation was aware of the risk, with the result that managers can be blamed. If they had not done the assessment, managers are less likely to be blamed – thus, in such a setting, remaining locally ignorant may be entirely rational. (The counterexample here would be the principle: *ignorantia legis non excusat* – ignorance of laws is no excuse.)

At a broader level, incorporating elements external to (and not necessarily controllable by) the organisation, e.g., the role of regulators, rating agencies and auditors, can also sometimes provide incentives not to engage in risk surveillance. Identifying how these external forces affect the organisation and its risk management activities could potentially be helpful to the process of creating new, more appropriate, incentives.

Overcoming obstacles to voluntary reporting in the civil aviation industry

As seen in theme 3, it is important to collect data about threats that have the potential to evolve into emerging risks. The two major means of collecting such data are:

1) Putting surveillance systems in place to observe and record events and trends regularly, even continuously (these systems may be automated); and

2) Through voluntary reporting systems, where stakeholders/staff etc. come forward to report unusual observations, errors, or behaviours that could contribute to risk emergence [Tamuz, 2004].

In its efforts to reduce accidents, the airline industry in the US has used both methods. The first method has been straightforward to introduce, as it has involved the installation of automated surveillance systems that record in-flight data and monitor aircraft instruments, operational commands, trajectory, and so on. While useful, due to the amount and reliability of the data collected, data from automated systems is not sufficient as it can never compare to the "richness of information" that is contained in voluntary reports – it is these reports that can give indications of the contributing factors (e.g., problematic behaviours or incentives) that lead to accidents [Tamuz, 2004].

However, as alluded to in theme 4, there may be significant obstacles to be overcome before a voluntary reporting system can yield the desired results. Even if senior leadership is willing to be receptive to negative or inconvenient information, leadership has to find a means to *convey* this to staff who are generally not inclined to report their own mistakes or contrarian views. Van der Schaaf and Kanse [2004] suggest that there are four main factors that

influence whether individuals will report an incident: fear of disciplinary action; uselessness (the impression that management will not take the problem seriously anyway); acceptance of risk (incidents are seen as just part of the job); and practical reasons (reporting is complicated or time-consuming). Studies that have focused specifically on aviation also find these factors to be relevant, citing, for example, lack of trust in management, pressure to allocate blame, embarrassment and expectation of punishment, and the military culture in aviation (similar to "acceptance of risk", as mentioned above, which incorporates the "macho" idea that "it won't happen to me") [O'Leary, 1995; Elwell, 1995; cited in Van der Schaaf and Kanse, 2004].

To overcome these obstacles to voluntary reporting, the US aviation industry has put in place two systems – one is a nation-wide reporting system managed by NASA and funded by the Federal Aviation Administration (FAA) and the other is an airline-based, public-private partnership.

The first of these, the nation-wide reporting system, is known as the Aviation Safety Reporting System (ASRS). Developed in 1976, its strategy to overcome the above obstacles to reporting is based on a promise of confidentiality (reports are de-identified with both the name of the person and of the airline removed) and the provision of limited immunity from disciplinary action by the FAA ("the FAA will not use reports…in any enforcement action except information concerning accidents or criminal offenses which are wholly excluded from the Program" [14 CFR 91.25]). The system, therefore, ultimately tries to remove perverse incentives to not report incidents; privileging learning from experience over regulatory enforcement. Indeed, it actively tries to differentiate itself from the FAA regulators as a way to overcome mistrust and fear of recrimination and punishment – although it is funded by the FAA, it operates independently and has no regulatory or enforcement powers [IOM, 2000]. The ASRS model has proven very influential and many foreign aviation regulatory bodies have followed its lead to set up their own similar voluntary reporting systems [GAIN, 2004]. However, only a sub-set of incidents reported to ASRS are included in the on-line data base. In the past this included a random sample of events, that allowed statistical assessment, but that was dropped due to resources constraints. Reinstating such a sample, or placing all reports into the on-line data base, would make ASRS a more effective tool for risk assessment and governance.

The second voluntary reporting system, the airline-based public-private partnership, is called the Aviation Safety Action Program (ASAP) and was introduced in 1996. ASAPs are operated by individual airlines (but must adhere to federal guidelines) and are based on memorandums of understanding between the company, the FAA and the labour unions [Phimister et al., 2004]. The main aim of these systems was initially to encourage reporting by pilots – especially the disclosure of their errors and, more importantly, of the factors that contributed to their errors – although they now also target other airline employees and maintenance staff. Specific guidance materials developed by the FAA are provided for each of the stakeholders, in which the non-punitive nature of the program and its aim of collecting safety-related data are clearly spelled out. Studies have found that airlines with ASAP programmes are satisfied with the system and believe that these programmes have been useful in detecting discrepancies and accident precursors [Patankar and Driscoll, 2004]. Organisations with ASAP programmes have higher levels of interpersonal trust, which can further help overcome barriers to reporting.

What sets the ASAP apart from the ASRS is the strategy that has been chosen to overcome barriers to voluntary reporting. Although the major incentive offered by both systems is the same – a certain level of protection for the individual making the report – the ASRS offers this essentially by distancing itself from the FAA, while the ASAP offers this by attempting to build-up a trusting and cooperative relationship between the FAA and the airlines, unions and staff (the FAA does not offer immunity under the ASAP, but makes it understood that unintentional violations of FAA regulations will only incur administrative reprimands rather than punitive sanctions, if they are voluntarily reported [Tamuz, 2004]).

Overall, the two systems can be seen to work in a complementary manner, with many ASAP programmes sending their reports additionally to the ASRS. However, the success of both kinds of system, ASRS and ASAP, depend on the success of publicity and communication about the systems and the incentives they offer individuals.

5. Encourage contrarian views

Establishing incentives and rewards for surveillance and foresight, and removing incentives to *not* engage in these activities, may not be enough.

There is no way to identify and consider the full spectrum of emerging risks if everyone in an organisation shares the same mind-set and vision of what is and is not important. To avoid the problem of "group think" it is also important to take additional steps to encourage contrarian views that challenge the widely-held viewpoints on expected future events within an organisation.

Some organisations do this internally by recruiting and rewarding staff with a range of different views, or even by creating separate units that have diversity of viewpoint applied to surveillance as their explicit function. But finding and encouraging well-informed and sceptical contrarian views may sometimes require the seeking of advice and guidance from outsiders, who are charged with "thinking outside the box". In either case, a group is set up whose job is to challenge conventional thinking and find weaknesses in the organisation's future planning. Note that such activities will be successful only to the extent that they are valued and rewarded for identifying and advancing ideas that do not fit comfortably with the organisation's conventional world view.

Many organisations, both military and civilian, find “red team” vs.” blue team” exercises helpful in determining where weaknesses are in military defence and corporate strategy in a competitive environment. Outside peer review is an effective way to overcome the tendency toward “group think” [Janis, 1982]. Awareness and contrarian thinking need to include external threats as well as internal events that could be precursors to accidents.

Cassandra, in the Greek myths recorded by Homer and Aeschylus, was believed to be able to predict the future, but no one believed her predictions when they were negative. An organisation truly concerned with assessing and managing risk needs to seek out Cassandra-equivalents and evaluate carefully the viewpoints that are expressed. A fresh look at a wide range of possibilities may yield important insights on threats and weaknesses in need of correction. Challenges to the conventional wisdom should not be dismissed as disloyalty or negative criticism, but as opportunities to achieve better understanding and improvement.

Thinking outside of the box: EDF and the Rapid Reflection Force

Recognising that risks can arise from complex systems, and that today's world is increasingly defined by "complex, fuzzy, inconceivable and fragmented threats and challenges" [Lagadec and Carli, 2005], some companies have begun to focus on how to develop capabilities to deal with this 21st century environment. The implementation of the Rapid Reflection Force (RRF) concept by Electricité de France (EDF) is one example of how preparedness to face emerging risks has been successfully improved by generating new viewpoints and encouraging unconventional suggestions.

The RRF is a team of people, each specially chosen for his or her ability to think outside the box, be creative, stay positive and calm in the face of the "unthinkable", and translate ideas into concrete suggestions. Its aim is essentially to provide support and advice to those at the chief executive level and to existing strategic crisis response teams in the event that they must deal with an emerging risk. The logic behind the need for an RRF is that emerging, systemic risks are likely to present a unique or novel situation and be surrounded by uncertainties [Béroux et al., 2008]. As a result, traditional preparedness measures involving conventional thinking and ready-made response strategies will not be sufficient to respond, because these traditional measures often assume a more stable and predictable environment, which may be non-existent when dealing with emerging risks and unconventional crises.

The creators of the RRF concept, Pierre Béroux, Xavier Guilhou and Patrick Lagadec describe the force's two main functions as: "to focus on the 'unthinkable' – unthinkable difficulties and unthinkable responses; and to produce specific and clear analyses and proposals for decision-makers" [Béroux et al., 2009]. Once chosen, this team should undergo continual training, via both teaching and simulation exercises, in order to remain adaptive as circumstances evolve. At the same time, the company management and other teams within the risk response platform (e.g., operations, communication) must also prepare to interact with the RRF, making sure that the roles of all players and the rules of the game are clear.

EDF first began to experiment with the RRF concept in 2006. It was decided, after conducting two exercises, one dealing with a flu pandemic, the other related to nuclear power, that the RFF had more than demonstrated its usefulness. In fact, the RFF was deemed "not only useful, but truly essential for upper echelon leaders" [Béroux et al., 2009]. Since these promising beginnings, the concept has been further refined within EDF and the RRF has been convened in several real-life situations, as well as further training exercises. For example, over the period from late 2006 to early 2007, EDF experienced a sequence of unpleasant and unexpected events: the suicide of several employees. This quickly became an important and highly visible issue, both internally and externally. It was also seen to represent a larger risk, where the essence of the problem had to do with company attitudes and the resulting organisational stress on employees. The RRF was employed to analyse the situation and recommend a course of action, which led to a process to "clear the air" within the organisation, display a willingness to listen, respect and understand employees' views as a means to enable a "global dynamic for change, improvement and healing" [Béroux et al., 2009].

2.3. Training and Capacity Building

Risk management for emerging risks should be accepted in an organisation with a good risk culture as everyone's responsibility. But having the responsibility is not the same as having skills to exercise that responsibility. To create and maintain a culture that encourages emerging risk management, capacity and resources are needed. As part of a programme of training, staff development, and personnel management, an organisation should develop the risk perception and decision-making skills of all levels of management and all individuals in its work force, not just those of people who are specialists in risk and therefore spend much of their professional time in risk analysis, data collection and management activities. Everyone in the organisation should take an interest in identifying and dealing with high-risk situations. Teamwork, knowledge for emergency response (such as first aid training) and flexibility to interrupt normal activity to do what is needed, should be encouraged at all levels of the organisation.

There is a great deal of material readily available through educational institutions, professional societies, and organisations such as IRGC to help in accomplishing an improved overview of skills needed for risk assessment and management. Better understanding of the technologies and systems that give rise to the risk enables people to judge better how to respond to unforeseen events, and especially, how to respond with knowledge and flexibility to the specifics of a given situation. A good risk culture and skills in interpreting and acting on risk information should be broadly encouraged as part of personnel development.

Here, we address three domains particularly important for dealing with emerging issues: surveillance and foresight; communication; and working with others.

6. Build capacity for surveillance and foresight activities

Training must include procedures for designing effective early warning systems, collecting and retaining early warning signs and any risk-relevant information, as well as planning and analysis in support of risk assessment and risk management activities. Advanced training in relevant scientific and engineering specialties and in probabilistic risk and safety analysis may be appropriate.

Organisations should carry out strategic planning activities, such as the development of scenarios to characterise future conditions including the emergence of new risks, plus strategic options and contingency plans for dealing with these conditions. All of this involves expenditure of resources, which may appear to some as corporate overhead that is not contributing toward profitability. But top management should consider that early warning systems and foresight activities are like an insurance policy, to foresee and avoid trouble that might be extremely expensive in penalties, damage to reputation, and profitability.

Significant investment is especially important in capabilities for data collection, data retrieval, and analysis. Investments should also be considered to obtain highly educated staff, carry out further training of staff on issues relevant to the

organisation's potential risks, and engage in large-scale assessment and practise response activities (for example, simulations of disaster response, of a type similar to "war games" or large scale manoeuvre exercises for the military).

7. Build capacity for communicating about emerging issues and dialoguing with key stakeholders

In all three categories of emerging risks, it is rarely the case that only a few people have both the responsibility and the information needed for risk management. The IRGC risk governance framework [IRGC, 2005] stresses the importance of dialogue among the key stakeholders – those who share in the responsibility for risk management, those who may have important risk-relevant information, and others who are potentially impacted and therefore have a strong interest in good risk management. Key stakeholders for private sector organisations may include suppliers, customers, neighbours to the organisation's facilities, as well as regulators and leaders in various levels of government. The importance of dialogue and the subjects for dialogue are discussed in the IRGC Emergence of Risk [IRGC, 2010a] and Risk Governance Deficits [IRGC, 2009a] documents.

Top level leadership in an organisation that is responsible for risk management, especially for the case of emerging risks, should be able and trained to review the state of communications with partner organisations and key stakeholders. For example, managers may have the opportunity to glean useful knowledge from those in other organisations that face – or have already resolved – similar challenges. At the earliest stages of risk emergence, it is particularly critical for managers to reach outside their organisation to other actors who may have valuable insight on the nature, scale and dynamics of the risk as well as the effectiveness and cost of response strategies.

Dialoguing with stakeholders being not an easy task – if it is a case of reaching out to sectors of the economy that are quite distinct or, especially, to those who may be competitors – knowledge management is instrumental for success. Establishing good communications and in-depth dialogue to support contingency planning and information sharing may be an excellent investment, especially in advance of situations where quick and effective action may be needed to deal with a sudden emergency.

8. Build capacity for working with others to improve the understanding of, and response to, emerging risks

One of the characteristic features of systemic emerging risks is that their sources and/or impacts may involve multiple organisations, sometimes in different economic sectors or even in multiple political and regional jurisdictions. Capacity for working with others is thus a key criterion for effective response and this capacity involves two elements: building up shared understanding and being able to act as a team.

Firstly, understanding is important because for emerging technologies, for complex systems, and even for well-established areas of commercial activity, the ability to make good decisions depends on understanding "how things work" and how to fix them when they do not work. For example, in a laboratory

dealing with dangerous pathogens or chemicals (or emerging nanomaterials and synthetic biology products), it may be of great importance to maintain confinement of these materials so that unintended exposures do not occur, for humans or in the natural environment. An organisation running a biosafety containment facility must consider how human error, equipment failure, natural disasters, or malevolent actions might result in a release of such materials. Doing such an assessment of risk depends on an excellent knowledge of laboratory design and laboratory practices. Successful risk mitigation depends on all staff understanding the properties of the materials and the extent of risk they may pose, as well as understanding how to act (and why) in case of an incident.

In the past, we have learned how to work with dangerous life-forms and substances, such as smallpox virus, radioactive materials and toxic chemicals. What is initially highly difficult and uncertain management evolves into routine when we understand how these life forms and materials behave, and how they can cause damage. We need to acquire this understanding, and to ensure that the knowledge is retained and used, but we must also avoid assuming that we know more than we really do. Overconfidence can be very dangerous.

Secondly, developing teamwork is an important part of building capacity to respond to an emerging risk because teamwork is needed to collect and respond to the risk-relevant information efficiently, and to implement risk management activities quickly and effectively. For example, as risks emerge, there may be a tendency for managers to react too hastily. In some cases, if efforts by one manager are not coordinated with efforts by other managers, the risk may not be controlled effectively. When a manager recognises an emerging risk as an element of a complex systemic risk or as a “commons problem”, it is critical to build capacity to cooperate with managers at other organisations that contribute to the risk or other government entities with authority to address the risk.

Developing and practising emergency procedures is highly recommended, especially in the context of on-going threats such as natural disasters and terrorist attacks. Public safety organisations, such as police and fire departments, go to considerable effort to learn from and work with others about how to deal with dangerous situations. They learn about criminal and fire behaviour, in the context of a broad range of situations they might someday confront. They work with others to develop extensive plans and procedures, and then they practise with others – a great deal.

Developing good teamwork is equally as important as having procedures based on understanding of the risks. Everyone should learn how to do their job as part of a team in coping with an emergency situation. We are all familiar with simple examples, such as lifeboat drills and instructions to those sitting in the exit row on airplanes. A large-scale example is the way the United States Forest Service (USFS) can assemble, within a matter of hours, a team of up to thousands of people from many different organisations to fight a large wild-land fire. The basis of the USFS Incident Command System is a standardised organisational structure with common terminology, job descriptions, and procedures [Rey, 2005]. It is an excellent example of a highly effective emergency response system for institutionalised teamwork that has been developed by learning through experience.

Working with others: the EU's REACH regulation

REACH, or Registration, Evaluation, Authorisation and Restriction of Chemicals, is the European Community's regulation on the safe use of industrial chemicals. The fundamental change introduced by REACH was the shifting of the burden of proof – under REACH it is the industry that must prove the safety of their chemicals, not the government. The legislation entered into force on 1 June 2007 and its aim is "to improve the protection of human health and the environment through the better and earlier identification of the intrinsic properties of chemical substances" [EC, 2011].

One important novel aspect of REACH is its concept of "one substance, one registration", which is intended to reduce duplicative animal testing and costs to industry, but which also has the positive side-effect of creating incentives for companies to cooperate and work together. Registration is the first step in the REACH process whereby any company wishing to sell or manufacture a chemical in the European Economic Area must register its product with the European Chemicals Agency, ECHA. Because only one registration may be submitted per identical substance, all the companies that produce that substance must share information with each other and submit their data in a joint registration. Thus, producers must put in place downstream communication processes for sharing information along the entire industrial supply and production chain, including manufacturers, importers, processors, distributors, and downstream users. REACH includes provisions to facilitate the sharing of information, including communication mechanisms to help importers and manufacturers reach data-sharing agreements, and systems to help registrants find other registrants with whom they can share data [ECHA website; EC, 2010]. The resulting increased cooperation and supply chain communication leads to the gathering of more targeted use and exposure information on chemicals [Christensen et al, 2011].

2.4. Adaptive Planning and Management

Organisational strategy, and the information and analysis that underlies it, can go out of date as important risk-relevant factors change. Therefore, the activities related to emerging risk identification, assessment, management and communication should be revisited and updated on a regular basis. Analysis, especially, should be revised as new information becomes available. It will often be appropriate that organisations have an on-going early warning system to identify emerging risks as soon as information appears indicating that such risks could be significant, and, therefore, that further examination and analysis is warranted. In other situations where it might be assumed that significant change has not occurred, it still may be a good idea to have an annual review of established and emerging risk issues, such as many individuals and organisations do with their insurance coverage. Have any significant changes occurred, such that past thinking and policy about the risks should be revisited? Most organisations might benefit from at least an annual review. It may be of interest to readers of this Concept Note to know that the very top level of the US military carries out an annual review of risks, incorporating methods based on the IRGC risk governance framework [Rouse, 2010].

9. Anticipate and prepare for adverse outcomes

Despite an organisation's best efforts to anticipate and guard against bad outcomes, sometimes bad things will occur. This can happen because of bad luck or because of actions by others or natural occurrences that could not be prevented. If an organisation can anticipate such potential contingencies, it may be able to take steps that will mitigate the consequences.

A good starting point to a process of assessing emerging risks is to ask what could go wrong, and collect as large a number of such scenarios as reasonably possible, including some that might initially be judged extremely unlikely. It is often useful to start with an initial event and a range of initial conditions, and then to develop the sequence of how subsequent events might lead to a disaster or serious accident, including a description of the ensuing consequences. At first this might be a “brainstorming exercise,” but with additional effort it might become a checklist compiled from the experience of many people, organisations, and history going back as far as available records permit [Shell, 2003]. The occurrence of a tsunami with a wave height of 15 metres should have been a scenario on TEPCO’s list, although the big tsunami in the area occurred over a thousand years ago (see the box on p.12). Human error, equipment malfunction, extreme weather or geological events, human malevolence, etc. – the scenario list should include what we can conceive of as causing serious adverse consequences to one’s own organisation, and perhaps to society at large.

One can’t anticipate everything – there are, indeed, some “unknown unknowns” that lie outside of human experience to date. But we have access to a very large historical record of what can go wrong, and we ought to use it. Just because it has not happened in a hundred or a thousand years doesn’t mean it won’t happen sometime soon. Earthquakes, floods, volcanic eruptions, epidemics of disease, terrorist attacks, breakdown of information systems, and the like happen regularly in other parts of the world, and we read about them. We have estimates of climate change, sea level rise, alterations in ecosystems, diminishing effectiveness of antibiotics, and a variety of other changes. What

could happen here, to us? How bad might it be? What might we do to avoid it or prepare for it?

10. Evaluate and prioritise options; be prepared to revise decisions

One can't study every conceivable scenario. All organisations have finite attention and resources. Priorities must therefore be set and a process is needed to evaluate and rank, based on the potential importance to the organisation, the responsibilities it has to its people (employees, stockholders, customers, etc.), and the legal and moral liabilities that might be associated with its activities.

Having looked for emerging threats (with an early warning system), the organisation might begin by making a list of potential risks. Then, a simple scoring of (estimated) probability multiplied by expected consequences will enable the elimination of scenarios where this product is small, either because the probability is anticipated to be extremely low or because the consequences are anticipated to be low or modest. Or, it may conclude that risk management for this scenario is outside its control and is the responsibility of another organisation. It may not make sense to set up one's own fire department, but rather to assume that fire protection will be provided by the local fire department and that fire risk will be assessed via insurance companies. But it still may make sense to think about whether there are issues involving risk of fire or explosion that the organisation should be watching. At any one time, an organisation should therefore have a set of issues that at that moment looks most critical to it, and then focus resources on learning more about these risks and on developing potential strategies for risk management, should they materialise. In setting those priorities it is also important to record the basis of the judgements – both because later this may help the organisation learn, and because it may provide an explanation in the event that an ignored risk suddenly materialises.

Once priorities are set, they should not remain frozen forever. It is important to institutionalise the process of "scanning the horizon" from time to time, and to ask, "Are we still focused on the right set of risks?" When a decision is made to reset some of the priorities, once again care should be taken to document and record the basis of the decision.

While it is often management practice in organisations to set specific goals and policies, changes in the information about emerging risks can motivate changing these goals and policies. The need for flexibility should be explained to organisation staff and outside stakeholders, and periodic appraisals should be carried out as the information changes. If a risk manager becomes locked into a particular management strategy, it may be difficult to adapt to the new information with revised strategies. Senior management must recognise and instruct lower-level management that strategies are expected to evolve as scientific knowledge accumulates. If there is resistance to change, it may be desirable to designate a team of credible specialists with responsibility for recommending modifications of strategy over time, rather than leaving responsibility for strategy revision to busy line managers.

Revising decisions to help better address uncertain risks: Progressive authorisation for pharmaceuticals

Pharmaceutical regulators face a dilemma created by, on the one hand, public demand for faster drug innovation and, on the other hand, public expectations that the drugs be risk-free. Until recently, the tendency has been towards more restrictive regulations, which minimise uncertainties about the benefits and risks of new drugs, but which also tend to constrain innovation, increasing both the costs and the time period necessary for drug approval.

Over the past few years, however, there have been a number of proposals made to substantially reform pharmaceutical regulation in the EU, Canada and the US (among others). These proposals are based on what has been called a "lifecycle" or "real-world" model of drug regulation, whereby the initial process of granting market authorisation for drugs is quicker and less restrictive, but the approval process continues well past this stage, incorporating incentives for longer-term studies. Essentially, this marks a move away from the precautionary principle and towards risk management principles for pharmaceutical regulation [Bouchard and Sawicka, 2009].

Proponents argue that these new regulatory models – known as progressive authorisation, adaptive licensing, staggered approval, or managed entry – will better balance the tension between drug access and safety, providing earlier access to innovative drugs and also allowing for *regulatory evaluation and corrections*. This latter provision will hopefully contribute to solving one of the biggest problems that many regulators have faced, which is the lack of focus on the safety and efficacy of the drug after its initial authorisation. This problem is exemplified by the case of Vioxx, a non-steroidal anti-inflammatory drug that was approved in the US and Canada in 1999, but then withdrawn from the market by the manufacturer, Merck, in 2004, because it was found to increase the risk of cardiovascular disease and stroke. If there had been more substantial, systematic post-market surveillance, this problem may have been detected much earlier [Carpenter et al., 2008; GAO, 2006].

In Canada, for example, the proposed "Progressive Licensing Framework" for drug approval (Bill C-51, an amendment to the Food and Drugs Act), if reintroduced and eventually passed, will allow for "flexible departure" or probationary approval for market authorisation of a new drug. Initial market authorisation requires that the benefits can be shown to outweigh the risks, while *maintenance* of market authorisation will be conditional on the drug continuing to demonstrate a favourable benefit-risk profile over its lifespan (post-market studies, monitoring, safety surveillance and risk management plans will be requirements) [Bouchard and Sawicka, 2009; Lexchin, 2008].

11. Develop strategies for robustness and resilience

When important emerging risks have been identified and assessed, the next stage is the development of appropriate risk management strategies. Often such strategies require both a technical component (a matter for engineers or other specialists) and institutional aspects, such as which organisational elements have what responsibilities and will bear what portion of costs.

Preparing for the improbable adverse scenarios (see theme 9) may be as simple as stockpiling some key material or building in some surge capacity, but

it inevitably involves expense in terms of both resources and institutional intention. Since developing mitigation capability is not cost-free, choosing whether and how much to invest requires at least some qualitative assessment of the probability of bad outcomes.

Many emerging risks involve large uncertainties (such as on the probability or magnitude of consequences) that may not be resolvable in the time-frame when decisions must be made. Strategies that are less sensitive to these uncertainties may be preferred despite higher costs and difficulties of implementation. Such risks are often better managed using “precaution-based” strategies and “resilience-focused” strategies. Precaution-based strategies pursue the goal of applying a precautionary approach in order to ensure the reversibility of critical decisions and of increasing a system’s coping capacity to the point where it can withstand surprises. Resilience-focused strategies are strategies directed at the risk absorbing systems. The main objective is to make these systems resilient so they can withstand or even tolerate surprises. In contrast to robustness, where potential threats are known in advance and the absorbing system needs to be prepared to face these threats, resilience is a protective strategy against unknown or highly uncertain hazards. Instruments for resilience include the strengthening of the immune system, diversification of the means for approaching identical or similar ends, reduction of the overall catastrophic potential or vulnerability even in the absence of a concrete threat, design of systems with flexible response options and the improvement of conditions for emergency management and system adaptation. Robustness and resilience are closely linked but they are not identical and require partially different types of actions and instruments.

“Robust” (i.e., best choice under current uncertainties) management strategies should be determined with the involvement of top organisation management and with an appropriate amount of analytical support. In most cases it will be appropriate to have some level of dialogue and discussion with stakeholders where there is a common interest in the risk. For example, a number of companies in the automobile and computer chip industries might wish that there had been more dialogue about what might happen in the event of a large natural disaster in Japan. When critical components come from only a few suppliers, the risk of a supply interruption occurring may be significant. Diversification of suppliers such that they are in different geographical areas and ship via different transportation routes can improve the security of a supply chain and reduce the risk of supply interruption.

LEVEL	THEME	ACTIONS
Risk governance Overarching management and organisational principles for effective emerging risk anticipation	1. Set emerging risk management strategy as a part of the overall strategy and organisational decision-making	Include risk aspects in the management process and make sure that established policies are understood and adhered to throughout the organisation
	2. Clarify roles and responsibilities	Assess readiness and effectiveness based on delegation of responsibility down through an organisation. Everyone must know their role but also believe they have a potential role in making improvements (update and innovate practices).
Risk Culture Establish a proactive risk management culture, with systematic surveillance and the ability to retrieve and evaluate information	3. Set explicit surveillance incentives and rewards	Set incentives to establish effective early warning systems, achieve good exchange of truthful information, and to report, including on controversial information.
	4. Remove perverse incentives to not engage in surveillance	Ensure that senior leadership is receptive to negative information, and not in denial. Identify how internal and external forces affect the organisation and its risk management activities in order to create new, more appropriate, incentives.
	5. Encourage contrarian views	Seek advice and guidance from outsiders, and set up a group within the organisation whose job is to challenge the conventional thinking and find weaknesses in the organisation's future planning.
Training and capacity building Capacity and resources are needed to create and maintain a culture that encourages emerging risk management	Build capacity for: 6. Surveillance and foresight activities	Top management should consider that foresight activities are like an insurance policy, to foresee and avoid trouble that might be extremely expensive in penalties, damage to reputation, and profitability.
	7. Communicating about emerging issues and dialoguing with key stakeholders	Improve the capability to exchange information and knowledge on emerging threats with key stakeholders. Establish in-depth dialogue to support decision-making.
	8. Working with others to improve the understanding of, and response to, emerging risks	Prepare collective action with other affected actors, develop understanding and teamwork, and make a conscious effort to learn from experience.
Adaptive planning and management Activities related to emerging risk identification, assessment, management and communication should be revisited and updated on a regular basis	9. Anticipate and prepare for adverse outcomes	Ask what could go wrong, how bad it might be and what could be done to prepare. Brainstorm, imagine, and use the historical record to collect scenarios, including those judged extremely unlikely.
	10. Evaluate and prioritise options; be prepared to revise decisions	Set priorities and document the decisions made, but also institutionalise horizon scanning to periodically reset priorities and refocus learning as the situation changes.
	11. Develop strategies for robustness and resilience	In order to better cope with uncertainties, develop risk management strategies that are focused on building robustness or resilience and can improve the capacity of vital systems to withstand or absorb shocks.

Conclusion

The main principle in this Concept Note on improving the management of emerging risks is that risk-relevant knowledge needs to be collected, disseminated to where it is needed, and used in timely fashion. The unfortunate converse of this principle is that failures to collect and use such information can lead to major disasters that might have been avoided by simple and straightforward actions.

Improving the management of emerging risks requires improvements in the communications to identify and characterise such risks. The risk science and safety literature and leaders in the study of human behaviour agree that in many organisations, there is not enough effective communication. For risks resulting from unexpected events, especially, complacency must be avoided and more vigilance is needed. Sufficient attention must be given to changing conditions, and to the possibility that infrequent events – which have occurred in the distant past or which are known to be possible, based on accepted theory – might occur and should be viewed as potential threats to be assessed and managed.

Managers need to be open to the possibility of adverse future events and to plan for them, using the best information they can obtain. Investments in increased vigilance, and the skills needed to identify and characterise emerging risks, could be highly beneficial in avoiding disasters.

References

[AP, 2011] The Associated Press, Fukushima Tsunami Plan a Single Page, May 27, 2011, http://www.msnbc.msn.com/id/43193695/ns/world_news-asia_pacific/t/fukushima-tsunami-safety-plan-single-page/

[Argyris, 1990] Argyris, C., Overcoming organisational Defenses, Needham Heights, Massachusetts: Allyn and Bacon. A summary of Chris Argyris work is at: http://www.infed.org/thinkers/argyris.htm. See also: Chris Argyris and Donald A. Schon, Theory in Practice, San Francisco, Jossey-Bass Inc., 1974.

[Aven, 2011] Aven, T., On risk governance deficits, *Safety Science*, 49 (6): 912-919

[BBC, 2011] BBC News, China train crash: Design flaws to blame – safety chief, 12 August 2011, http://www.bbc.co.uk/news/world-asia-pacific-14504877

[BEA, 2011a] Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile (BEA), Interim report f-cp090601ae on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France, flight AF 447 Rio de Janeiro – Paris, July 2009, http://www.bea.aero/docspa/2009/f-cp090601e1.en/pdf/f-cp090601e1.en.pdf

[BEA, 2011b] Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile (BEA), Accident to the Airbus A330-203 flight AF 447 on 1st June 2009, Update on Investigation, 27 May, 2011, http://www.bea.aero/fr/enquetes/vol.af.447/point.enquete.af447.27mai2011.en.pdf

[Béroux et al., 2009] Béroux, P., Guilhou, X. and Lagadec, P., Rapid Reflection Forces put to the reality test, *Crisis Response*, 4 (2): 38-40

[Béroux et al., 2008] Béroux, P., Guilhou, X. and Lagadec, P., Implementing Rapid Reaction Forces, *Crisis Response*, 3 (2):36-7

[BOEMRE, 2011] The Bureau of Ocean Energy Management, Regulation and Enforcement, Report regarding the causes of the April 20, 2010 Macondo well blowout, 14 September 2011, http://www.boemre.gov/pdfs/maps/DWHFINAL.pdf

[Bouchard and Sawicka, 2009] Bouchard, R.A. and Sawicka, M., The mud and the blood and the beer: Canada's progressive licensing framework for drug approval, *McGill Journal of Law and Health*, 3, 49-84, http://mjlh.mcgill.ca/pdfs/vol3-1/BouchardSawicka_1.pdf

[Buncefield, 2006] Buncefield Major Incident Investigation Board, Buncefield Major Incident Investigation: Initial Report to the Health and Safety Commission and the Environment Agency of the investigation into the explosions and fires at the Buncefield oil storage and transfer depot, Hemel Hempstead, on 11 December 2005, HSE, July 2006, http://www.endsreport.com/docs/20060713d.pdf

[CA.gov, 2011] Office of the Governor of the State of California, Edmund G. Brown Jr., 'Governor Brown signs legislation to protect Californians from pipeline explosions', http://gov.ca.gov/news.php?id=17263

[Carpenter et al., 2008] Carpenter, D., Zucker, E.J. and Avorn, J., Drug-review deadlines and safety problems, *The New England Journal of Medicine*, 358 (13), 1354-1361, http://www.nejm.org/doi/pdf/10.1056/NEJMsa0706341

[Christensen et al., 2011] Christensen, F.M., Eisenreich, S.J., Rasmussen, K., Riego Sintes, J., Sokull-Kluettgen, B., Van de Plassche, E.J., European Experience in Chemicals Management: Integrating Science into Policy, *Environmental Science and Technology*, 45(1): 80-89

[14 CFR 91.25] Code of Federal Regulations, Title 14 - Aeronautics and Space, Chapter 1: Federal Aviation Administration, Department of Transportation, Part 91: General operating and flight rules, 91.25 Aviation Safety Reporting Program: Prohibition against use of reports for enforcement purposes, http://law.justia.com/cfr/title14/14-2.0.1.3.10.1.4.13.html

[CPUC, 2011] California Public Utilities Commission (CPUC), Announcement, CPUC Begins Penalty Consideration Regarding PG&E Gas Pipeline Recordkeeping – Feb. 24, 2011, http://www.cpuc.ca.gov/PUC/events/110224_sanbruno.htm

[Dietz and Stern, 2008] Dietz, T. and Stern, P.C., (eds), Public Participation in Environmental Assessment and Decision Making, Washington, D.C., National Academies Press, http://www.nap.edu/catalog.php?record_id=12434

[EC, 2011] European Commission, DG Environment, Chemicals, REACH, Introduction,

http://ec.europa.eu/environment/chemicals/reach/reach_intro.htm

[EC, 2010] European Commission, DG Enterprise and Industry, REACH White Paper - background communication, http://ec.europa.eu/enterprise/sectors/chemicals/documents/reach/archives/white-paper/background/communication/index_en.htm

[ECHA website] European Chemicals Agency, REACH Processes, http://guidance.echa.europa.eu/reach_processes_en.htm

[Elwell, 1995] Elwell, R.S., Self-report means under-report, In: McDonald, N., Johnston, N. and Fuller, R. (eds), Applications of Psychology to the Aviation System, Aldershot, UK, Ashgate Publishing, 129-136

[Environmental Defense Fund and DuPont, 2007] Environmental Defense Fund and DuPont, Nano Risk Framework, http://nanoriskframework.com/page.cfm?tagID=1081

[FABIG, 2011] Fire and blast information group (FABIG), AZF Toulouse, http://www.fabig.com/Accidents/AZF+Toulouse.htm

[GAIN, 2004] Global Aviation Information Network, A Roadmap to Just Culture: Enhancing the Safety Environment, http://flightsafety.org/files/just_culture.pdf

[GAO, 2006] United States Government Accountability Office, Drug safety: improvement needed in FDA's postmarket decision-making and oversight process, Washington DC, GAO, http://www.gao.gov/new.items/d06402.pdf

[Guldenmund, 2010] Guldenmund, F., (Mis)understanding Safety Culture and Its Relationship to Safety Management, *Risk Analysis,* 30 (10), 1466-1480

[IOM, 2000] Institute of Medicine (IOM), Kohn, L.T., Corrigan, J.M. and Donaldson, M.S. (eds), To Err is Human: Building a Safer Health System, Washington, DC, National Academies Press.

[IRGC, 2010a] IRGC, The Emergence of Risk: Contributing Factors, Geneva, IRGC, http://irgc.org/IMG/pdf/irgc_ER_final_07jan_web.pdf

[IRGC, 2010b] IRGC, Risk Governance Deficits: Analysis, illustrations, and recommendations (Policy Brief), Geneva, IRGC, http://irgc.org/IMG/pdf/IRGC_RiskGovernanceDeficits_PolicyBrief2010.pdf

[IRGC 2010c] IRGC, Guidelines for the Appropriate Risk Governance of Synthetic Biology (Policy Brief), Geneva, IRGC, http://www.irgc.org/IMG/pdf/irgc_SB_final_07jan_web.pdf

[IRGC, 2009a] IRGC, Risk Governance Deficits: An analysis and illustration of the most common deficits in risk governance (Report), Geneva, IRGC, http://irgc.org/IMG/pdf/IRGC_rgd_web_final.pdf

[IRGC, 2009b] IRGC, Appropriate Risk Governance Strategies for Nanotechnology Applications in Food and Cosmetics (Policy Brief), Geneva, IRGC, http://www.irgc.org/IMG/pdf/irgc_nanotechnologies_food_and_cosmetics_policy_brief.pdf

[IRGC, 2008a] IRGC, Risk Governance Guidelines for Bioenergy Policies (Policy Brief), Geneva, IRGC, http://www.irgc.org/IMG/pdf/IRGC_PB_Bioenergy_WEB-2.pdf

[IRGC, 2008b] IRGC, Risk Governance of Nanotechnology Applications in Food and Cosmetics (Report), Geneva, IRGC, http://www.irgc.org/IMG/pdf/IRGC_Report_FINAL_For_Web.pdf

[IRGC, 2007a] IRGC, Regulation of Carbon Capture and Storage (Policy Brief), Geneva, IRGC, http://www.irgc.org/IMG/pdf/Policy_Brief_CCS.pdf

[IRGC, 2007b] Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures (Policy Brief), Geneva, IRGC, http://www.irgc.org/IMG/pdf/IRGCinfra_site06.11.07-2.pdf

[IRGC, 2005] IRGC, White Paper No.1, Risk Governance: Towards an Integrative Framework, Geneva, IRGC, http://irgc.org/IMG/pdf/IRGC_WP_No_1_Risk_Governance__reprinted_version_.pdf

[Janis, 1982] Janis, I.L., Groupthink: Psychological Studies of Policy Decisions and Fiascoes, Cengage Learning, 2nd edition

[Kheifets et al., 2010] Kheifets, L. et al., Risk Governance for Mobile Phones, Power Lines, and Other EFM Technologies, *Risk Analysis* 30(10): 1481-1494

[Krupp and Holliday, 2005] Krupp, F. and Holliday, C., Let's Get Nanotech Right, *The Wall Street Journal*, 14 June 2005, http://www.edf.org/sites/default/files/5177_OpEd_WSJ050614.pdf

[Lagadec and Carli, 2005] Lagadec, P. and Carli, P., Crossing the Rubicon, *Crisis Response*,1 (3): 39-41, http://www.patricklagadec.net/fr/pdf/Crisis_Response_Journal_Carli.pdf

[Lexchin, 2008] Lexchin, J. Progressive licensing of drugs: music or noise? *Healthcare Policy*, 3 (4), 11-15, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2645165/pdf/policy-03-011.pdf

[Lovell, 1975] Lovell, J., Houston We've Had a Problem, Chapter 13 in Cortright, E.M., (ed), Apollo Expeditions to the Moon, Washington D.C., Scientific and Technical Information Office, National Aeronautics and Space Administration

[New York Times, 2009] New York Times, Topics, US Airways Flight 1549, http://topics.nytimes.com/top/reference/timestopics/subjects/a/airplane_accidents_and_incidents/us_airways_flight_1549/index.html

[NTSB, 2011] National Transportation Safety Board, Accident report NTSB/PAR-11/01 PB2011-916501, Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire, San Bruno, California, September 9, 2010, http://www.ntsb.gov/doclib/reports/2011/PAR1101.pdf

[O'Leary, 1995] O'Leary, M.J., Too bad we have to have confidential reporting programmes: Some observations on safety culture, In: McDonald, N., Johnston, N. and Fuller, R. (eds), Applications of Psychology to the Aviation System, Aldershot, UK, Ashgate Publishing, 123.128.

[OSC, 2011] Oil Spill Commission, National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, Final report, January 11, http://www.oilspillcommission.gov/final-report

[Patanker and Driscoll, 2004] Patanker, M.S. and Driscoll, D., Factors affecting the success or failure of aviation safety action programs in aviation maintenance organisations, published in the Proceedings of the First Safety Across High-Consequence Industries Conference, March 9-10, 2004, St. Louis Missouri, 97-102.

[PC, 1979] President's Commission, Report of the President's Commission on the Accident at Three Mile Island, John G. Kemeny, Chair, October 30, 1979, http://www.pddoc.com/tmi2/kemeny/index.html

[Phimister et al., 2004] Phimister, J.R., Bier, V.M. and Kunreuther, H.C. (eds) Accident Precursor Analysis and Management, Washington, D.C., National Academy Press, http://www.nap.edu/catalog.php?record_id=11061

[Rey, 2005] Mark Rey, Testimony of the Undersecretary, US Department of Agriculture, October 26, 2005, http://www.fs.fed.us/congress/109/house/oversight/rey/102605.html

[Rouse, 2010] Rouse, J.F., The Chairman of the Joint Chiefs of Staff Risk Assessment System, Presentation at the Annual Meeting of the Society for Risk Analysis, Salt Lake City, Utah, December 17, 2010

[Shell, 2003] Shell, Exploring the Future, Scenarios: An Explorer's Guide, Global Business environment, Shell International, www.shell.com/scenarios

[Tabuchi, 2011] Tabuchi, H., Head of Nuclear Utility Steps Down After Nuclear Crisis, *The New York Times*, May 21, 2011, http://www.nytimes.com/2011/05/21/business/global/21iht-tepco21.html?pagewanted=all

[Tamuz, 2004] Tamuz, M., Understanding Accident Precursors, In: [Phimister et al., 2004], 63-78

[Van der Schaaf and Kaanse, 2004] Van der Schaaf, T. and Kanse, L., Checking for Biases in Incident Reporting, In: [Phimister et al., 2004], 119-126.

Note: all web addressed last accessed 7 October 2011.

Appendices

Appendix 1: Exemplary References on Safety Culture and Knowledge Management

For those readers who wish to learn more about the scholarly basis for the ideas set forth in this Concept Note, three references are highly recommended. The National Academy of Engineering convened a workshop in July 2003 that led to a 2004 report [Phimister et al., 2004], which includes a number of papers presented at the workshop. The organisers and speakers at this meeting included experts in engineering safety, risk sciences, and senior executives responsible for risk management in industries including health, energy, and transportation. A main focus is on information management for precursor events that can lead to accidents.

The 2010 paper by Frank W. Guldenmund in *Risk Analysis* [Guldenmund, 2010] summarises a great deal of literature on safety culture in relation to safety management. The 109 references in this paper cover a great deal that has been written about safety culture from the perspective of the behavioural sciences, such as psychology, sociology, and anthropology, on what is meant by "safety culture" and how good safety culture can be achieved. One particularly important passage from near the end of this paper is reproduced below:

> *…organizations that are able to learn continuously and effectively from deviations in their processes, are supposedly, improving their safety performance in the long run. Also, these organizations are eager to pick up and analyze still "weak signals" that have not materialized into something serious yet. Importantly, significant information that should be able to flow uninhibited throughout the organization, so that anybody who has to be informed about something, actually also is. What is more, qualities like trust and responsibility are also demonstrated with the empowerment provided to the workforce to solve safety issues online.*
>
> [From Guldenmund, 2010: 1477]

Chris Argyris [Argyris, 1990] has had a long career as a professor of education and organisational behaviour at the Harvard Business School. His extensive research with top management in many large organisations over many decades has led to important insights on why corporate management is often inadequate in obtaining and using the information needed for good decision-making. The research results and recommendations for improved practices from the work of Professor Argyris and his colleagues and successors are highly consistent with those emerging from the engineering risk, risk science, and behavioural science communities. In the words cited from Guldenmund above, organisations need to learn continuously and effectively, from "deviations" in their processes – indications that improvement is needed. Even "weak signals" must be captured, retained, and analysed. Learning must flow out to all levels in the organisation. Trust, responsibility, and working out differences in judgement through effective dialogue must enable decisions that are based on the best available information and on values for the organisation as a whole, and not the interests of individuals or subgroups within the organisation. Achieving such practices in large bureaucratic organisations may be quite difficult, even under excellent leadership. A key aspect for success is a focus on process improvement, whereby "weak signals" are recognised and processes are then improved. This is inherently a bottom-up process of making small changes, although it may be facilitated by top-down policies to improve openness, communication across organisational boundaries, and commitment to long-term values as opposed to short-term expediency. Often, the "weak signals" indicate that old theories and practices have become outmoded and

need to be changed. Many organisations find that recognising the signals and accomplishing the needed change are quite difficult, because the natural behavioural tendency, especially in more senior and experienced people, is to stick with the old ways.

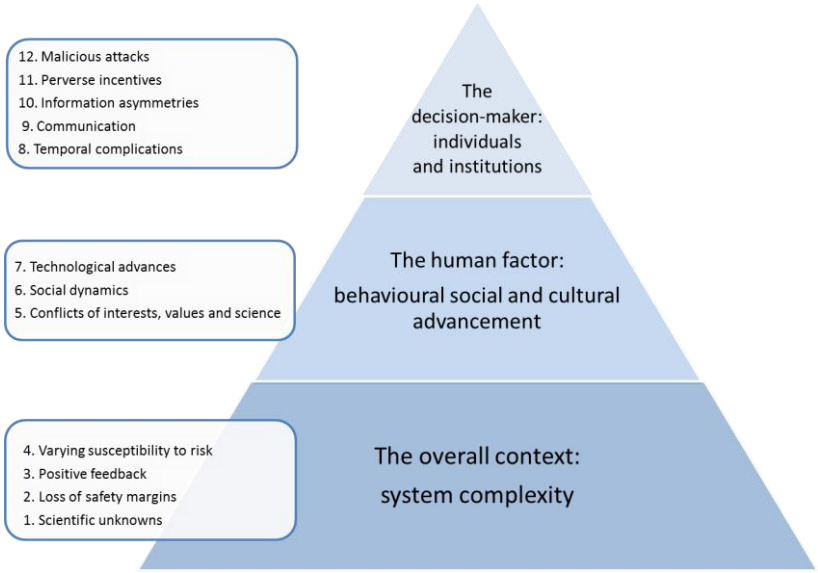
Appendix 2: Context of this work on emerging risks

The publication of this Concept Note marks the beginning of the second phase of IRGC's project on Emerging Risks. The first phase of this project examined the origins of emerging risks and produced a report identifying and describing the contributing factors to risk emergence, so that risk professionals, by understanding and recognising these factors, may be better able to avoid or mitigate emerging risks in future [IRGC, 2010a]. The eleven themes in this Note draw on insights from this first phase of the project.

Contributing factors to risk emergence

These twelve factors all have the capacity to contribute to creating "fertile ground" from which new risks may emerge. The presence, absence, or direction of influence of these factors thus amplify or attenuate the likelihood and/or severity of an emerging risk. These factors are generic in the sense that they are prevalent across many domains of nature, science and technology, society and the economy.

One possible way to conceptualise the list of factors is to view them as operating at three different levels: factors 1-4 are more structural in nature and have to do with the properties of the complex systems often implicated in systemic risk emergence, or elements (e.g., geography, genetics) that interact with these properties. Factors 5-7 operate more at the level of human society and deal with aspects that derive from human nature, behaviour and actions with a focus on social and cultural relations and advancement. Moving from the broader societal level to the level of individual actors, factors 8-12 deal with the impact that personal or institutional decisions can have on risk emergence. Nevertheless, we note that the twelve contributing factors below are highly interdependent and may be ordered or prioritised in many different ways. See [IRGC, 2010a] for more details.



IRGC is by no means the only organisation working on the important topic of emerging risks. In particular, we would like to draw to the reader's attention the European iNTeg-Risk project, which specifically addresses the topic of this Concept Note: emerging risks related to new technologies.

The iNTeg-Risk project

The iNTeg-Risk project 2009-2013, funded by the 7th Framework programme of the European Union, addresses the "early recognition, monitoring and integrated management of emerging, new technology related, risks".

It defines as *emerging* any risk that is *new* and/or is *increasing.*

By *new* it is meant that:

- The risk has not previously been encountered and may be caused by new processes, new technologies, new workplace contexts, or social or organisational change; or
- A long-standing issue is newly considered as a risk due to change in social or public perception; or
- New scientific knowledge allowing a long-standing issue to be identified as a risk.

The risk is *increasing* if:

- The number of hazards that can lead to the risk is growing; or
- The likelihood of exposure to the risk is increasing (exposure level and/or the extent of human values exposed); or
- The potential adverse consequences of the risk are becoming greater (severity of consequences and/or the extent of human values affected).

Practically speaking, any risk that is "emerging" in this sense will require a new or updated management approach

Under this definition, iNTeg-Risk proposes examples of issues that are potentially emerging risks:

- CO_2 capture and storage: the technology is rather new although already existing in e.g., the oil and gas industry. But the extent to which it is intended to be used is much larger and additional safety requirements may be needed
- Deep underground hubs: is there a depth limit beyond which an underground infrastructure is intrinsically safe? How can this be assessed? What is the role of stakeholders' perceptions?
- Monitoring pipelines with drones: is the risk reduction on third party accidents worth taking the risk of a drone crash? Is it acceptable to stakeholders?
- How can the risk created by a new nanopowder manufacturing plant be assessed? How can the risk of nanopowders be compared with the usual risk caused by car brake dust?

The leaders of the iNTeg-Risk project (Aleksandar Jovanovic, Olivier Salvi and Ortwin Renn) have all been involved in the IRGC emerging risk project.

See http://www.integrisk.eu-vri.eu/ for further details.

Acknowledgements

Work on this publication was led by D. Warner North (President, NorthWorks Inc., and Consulting Professor, Department of Management Science and Engineering, Stanford University, USA).

IRGC appreciates the contributions from those who attended the IRGC workshop in Rüschlikon, Switzerland in December, 2010, particularly the suggested reformulation of the themes by Reto Schneider and Martin Weymann of Swiss Re, and the contribution of Stephen Barrager, who co-authored with Warner North a background paper for the Rüschlikon workshop setting forth ideas from the writings of Chris Argyris. Comments on earlier drafts from Ortwin Renn, Lutz Cleeman, John Graham, Paul Stern, Richard Gowland and Brian Smith are also appreciated.

Project work on emerging risks would not have been possible without the generous support of IRGC's donors, including the Swiss Secretariat for Education and Research, Swiss Reinsurance Company and Oliver Wyman Inc.

About IRGC

The International Risk Governance Council (IRGC) is an independent organisation based in Switzerland whose purpose is to help improve the understanding and governance of emerging, systemic global risks. It does this by identifying and drawing on scientific knowledge and the understanding of experts in the public and private sectors to develop fact-based recommendations on risk governance for policymakers.

IRGC believes that improvements in risk governance are essential if we are to develop policies that minimise risks and maximise public trust and effectiveness in the processes and structures of risk-related decision-making. A particular concern of IRGC is that important societal opportunities resulting from new technologies are not lost through inadequate risk governance.

Members of the Foundation Board

Charles Kleiber (Chairman), Former State Secretary for Education and Research, Swiss Federal Department of Home Affairs, Switzerland; **John Drzik** (Vice-Chairman), President and CEO, Oliver Wyman, USA; **Walter Fust**, Former Head of Swiss Development Cooperation, Switzerland; **José Mariano Gago**, Former Minister for Science, Technology and Higher Education, Laboratory for Particle Physics (LIP), Portugal; **Philippe Gillet**, Vice-President and Provost, Federal Institute of Technology (EPFL) Lausanne, Switzerland; **C. Boyden Gray**, Gray & Schmitz LLP, USA; **Liu Yanhua**, Counsellor, Counsellors' Office of the State Council, People's Republic of China; **Michel Maila**, President, MIGEM Consulting Inc., Canada; **Christian Mumenthaler**, Chief Executive Officer, Reinsurance, Swiss Reinsurance Company, Switzerland; **Michael Oborne**, Former Director, International Futures Programme, OECD, France; **Margareta Wahlström**, Assistant Secretary-General, Special Representative of the Secretary-General for Disaster Risk Reduction (UNISDR), Switzerland. The **OECD** has observer status.

Members of the Scientific and Technical Council

Prof. M. Granger Morgan (Chairman), Head, Department of Engineering and Public Policy, Carnegie Mellon University, USA; **Dr V. S. Arunachalam**, Chairman and Founder, Center for Study of Science, Technology and Policy, India; **Prof. Fabiana Arzuaga**, Professor of Regulation of Biotechnology and Patent Law, Faculty of Law, University of Buenos Aires, Argentina; **Dr Lutz Cleemann**, Senior Adviser, Sustainable Business Institute, Germany; **Dr Anna Gergely**, Director, EHS Regulatory, Steptoe & Johnson, Belgium; **Dr John D. Graham**, Dean, Indiana University School of Public and Environmental Affairs, USA; **Prof. Manuel Heitor**, Professor, Instituto Superior Técnico, Technical University of Lisbon, Portugal; **Prof. Carlo C. Jaeger**, Head, Social Systems Department, Potsdam Institute for Climate Impact Research (PIK), Germany; **Prof. Wolfgang Kröger** (IRGC Founding Rector), Managing Director, Risk Center, Swiss Federal Institute of Technology (ETH) Zurich, Switzerland; **Prof. Jeffrey McNeely**, A.D. White Professor at large, Cornell University and Senior Scientific Advisor, IUCN - The International Union for Conservation of Nature, Switzerland; **Dr D. Warner North**, President, NorthWorks Inc., and Consulting Professor, Department of Management Science and Engineering, Stanford University, USA; **Prof. Norio Okada**, Director, Disaster Prevention Research Institute, Kyoto University, Japan; **Prof. Kenneth Oye**, Associate Professor, Political Science and Engineering Systems, Massachusetts Institute of Technology (MIT), USA; **Prof. Ortwin Renn**, Professor for Environmental Sociology, University of Stuttgart, Germany; **Prof. Úrsula Oswald Spring**, Research Professor, Regional Centre of Multidisciplinary Research, National University of Mexico, Mexico; **Prof. Joyce Tait**, Innogen Scientific Advisor, ESRC Centre for Social and Economic Research on Innovation in Genomics, UK; **Dr Timothy Walker**, Chair, Accounting and Actuarial Discipline Board, Financial Reporting Council, UK; **Prof. Xue Lan**, Dean, School of Public Policy and Management, Tsinghua University, People's Republic of China.

International Risk Governance Council

Chemin de Balexert 9
1219 Châtelaine
Geneva – Switzerland

www.irgc.org

Tel.: +41 22 795 17 30
Fax.: +41 22 795 17 39

ISBN 978-2-9700672-9-0