international risk
governance council

IRGC GUIDELINES FOR EMERGING RISK GOVERNANCE

Guidance for the Governance
of Unfamiliar Risks

PREFACE

Some threats or risk events are predictable with precision because they are associated with known, recurring or likely patterns. Threats linked to geophysical changes are one example. Other risks, such as demographic evolution, can only be predicted with a margin of error. However, those associated with new technologies, changing patterns, complex systems or new contextual conditions are generally unanticipated and are not widely understood, and they have no convincing plan of action for mitigation. These are often called "**emerging risks**".

It is difficult for any organisation to foresee the future and to evaluate the consequences of existing trends and drivers of change. This can lead to risks going unnoticed, or being ignored or neglected. Emerging risks require a different kind of governance than established, familiar risks, as many have not yet materialised, or may simply fade without materialising.

Investing in emerging risk governance (ERG) serves to prevent future damage from new or unfamiliar threats in order to protect public interests and to enable organisations to adapt to changing conditions and possibly even recognise new opportunities therein. It also contributes to defining a new regulatory environment for emerging risk management, for instance in the finance and insurance sectors. Emerging risks always demand the involvement of top management as they must be given the requisite priority; as such, ERG should be considered an integral part of the strategic management process and allocated the necessary resources.

The project of the International Risk Governance Council (IRGC) to develop Guidelines for Emerging Risk Governance stems from previous IRGC work on *factors contributing to risk emergence* (IRGC, 2010a), obstacles to and drivers of emerging risk management (IRGC, 2011)[1] and workshop discussions with practitioners and academics[2]. The project aims to provide guidance for practitioners in business and the public sector, to help them improve their own capabilities to cope with emerging threats and surprises. Although there are differences between public- and private-sector organisations, there are also similarities, such as short-term imperatives related to either electoral constraints in governments or immediate financial returns and expectations in business, reputational issues, and general resource constraints.

IRGC intends neither to build a theory of ERG nor to focus on particular emerging risks. Rather, it seeks to **provide a road map or checklist** that organisations can adapt to their particular needs and objectives. The purpose of the guidelines, therefore, is to:

- Provide guidance for emerging risk anticipation and response
- Categorise emerging risk and place it in a response framework
- Detect and analyse relevant signs of ongoing or future dynamics that could change the risk portfolio of a given organisation
- Induce the disappearance of an emerging risk, its decommission from the watch list of emerging threats, or to prompt its move into the portfolio of routinely manageable risks.

This report and its Appendices[3] **describe the guidelines**, provide underlying scientific evidence and:

- **Give information** about other frameworks for emerging risk management
- **Present an introduction to scenario and narrative development**
- **Provide insights into concepts and methods from fields other than risk management** that can be useful to address uncertainty and emerging risk issues.

---

[1] Publications and illustrations are available from the IRGC website at www.irgc.org/risk-governance/emerging-risk.

[2] On 6 June 2014, IRGC organised a roundtable discussion on the governance of emerging risks and presented a first draft of the guidelines proposed in this paper.

[3] Published separately and available on www.irgc.org/publications/core-concepts-of-risk-governance

Abbreviations

—————

CSA   Chief scientific adviser

EC   European Commission

EFSA   European Food Safety Authority

ENISA   European Union Agency for Network and Information Security

ERG   Emerging risk governance

IEHRF   Institute for Environment, Health, Risk and Futures (UK)

IRGC   International Risk Governance Council

OECD   Organisation for Economic Co-operation and Development

UK   United Kingdom

US   United States

CONTENTS

Boxes

——

Figures

——

Table

——

SUMMARY

The IRGC Guidelines for Emerging Risk Governance describe key steps and associated methodologies for early identification and management of emerging risks.

The process proposed in this report covers an overarching, flexible and adaptable set of guidelines designed to deal with complex, evolving and uncertain environments. It can help organisations to:

- **Step 1**: Make sense of the present & explore the future
- **Step 2**: Develop scenarios based on narratives and models
- **Step 3**: Generate risk management options & formulate strategy
- **Step 4**: Implement strategy
- **Step 5**: Review risk development and decisions

At the beginning of the risk emergence process, the aim is to detect and analyse (weak) signals pertaining to ongoing and future dynamics that may change an organisation's risk portfolio, and evaluate whether risks to the organisation may materialise and with what potential impact. Emerging risk managers aim to navigate the uncertainties involved in the risk's development until more knowledge is collected and analysed. Then either the risk becomes familiar and can be steered into a portfolio of routinely manageable risks, or it is evaluated as tolerable, or it is steered into disappearance. It may be the case, for example, that the social construction and perception of an emerging risk does not coincide with its scientific assessment.

Strategies for managing emerging risks thus differ from those for managing familiar risks. IRGC proposes six management options, which can be combined for a more effective outcome:

1. Acting on the factors that contribute to risk emergence or amplification
2. Developing precautionary approaches
3. Reducing vulnerability
4. Modifying the organisation's risk appetite in line with a new risk
5. Using "conventional" risk governance instruments to manage familiar risks
6. Doing nothing

As governing emerging risks is at the intersection of various disciplines and theoretical frameworks, IRGC has integrated expertise from various fields in this project, including risk management, futures studies, innovation management, dynamic capabilities and strategic decision-making.

Particular emphasis is put on the need for an emerging risk conductor, whose role is to coordinate and lead the internal and external stakeholders involved in the assessment, management and communication of emerging issues. Equally important is that emerging risk governance be set as a strategic priority, with involvement from top management.

This report is accompanied by Appendices, published separately, in which readers can find further conceptual insights and recommendations.

1.

INTRODUCTION

1.1 Definition of emerging risks

—

IRGC defines emerging risks as new risks or familiar risks that become apparent in new or unfamiliar conditions. This definition suggests that managers need to focus on the early detection and analysis of emerging risks' triggers, including the development of familiar risks into new threats.

IRGC's initiative on emerging risks does not aim to establish conceptual or theoretical delineations. It acknowledges that definitions must be adapted to specific contexts. Scholars are working to establish a common definition, including a proposal by Roger Flage and Terje Aven (2015) to emphasise that "knowledge becomes the key concept for both emerging risk and black swan type of events" and thus that the concept of emerging risk is relative, not absolute.

Types of emerging risks

In the concept note "Emerging Risks: Sources, Drivers and Governance Issues" (IRGC, 2010b), IRGC listed various categories of risks according to their source: human, natural or causal interactions. Emerging risks can thus result from trends or events in these fields, which alone or in combination have the intrinsic potential to induce risk.

However, for the specific purpose of providing guidelines on how to manage emerging risks, IRGC focuses on risks resulting from new or future threats, or having an impact on new or future exposures and vulnerabilities. In these cases, the focus is on the *low level of knowledge* of the potential losses as well as the probability distribution of their occurrence. In any case, stakeholders with different interests or viewpoints may contest this knowledge.

IRGC suggests emerging risk categorisation according to three types:

A. **High uncertainty and a lack of knowledge about potential impacts and interactions with risk-absorbing systems**: These risks have uncertain impacts, with uncertainty resulting from new products, services or behaviours (owing to social dynamics, including advances in science and technological innovation). The dominant feature of this type of emerging risk is the lack of scientific knowledge and experience regarding the possible consequences, especially in interaction with already existing technologies and practices. Governance activities include deciding whether to authorise certain products, services, behaviours or technologies, and implementing appropriate risk management measures to avoid or mitigate potential adverse consequences. Current examples include products and processes in nanotechnology or synthetic biology.

B. **Increasing complexity, emerging interactions and systemic dependencies that can lead to non-linear impacts and surprises**: Risks with systemic impacts stem from systems with multiple interactions and adaptive behaviours. The defining feature of this type of emerging risk is the loss of safety margins or a lack of knowledge about the way familiar risks are connected to other risks in an interdependent and complex environment. In the case of technological systems, the main issue is not the risk inherent in the technologies, but its interaction with other types of risk. Examples of complex interconnected systems are numerous in the fields of energy, transportation, communications and information technology.

C. **Changes in context (for example social and behavioural trends, organisational settings, regulations, natural environments) that may alter the nature, probability and magnitude of expected impacts**: New and unexpected risks can emerge from established technologies, products or processes in evolving contexts. The main issue in this type of emerging risk is that its potential impact on familiar processes, products or technologies (in terms of both probability and magnitude) challenges seemingly well-established governance practices. Changes in context or organisational settings include ageing infrastructures, 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 this type of risk.

Differences between emerging and familiar risks

It is helpful to compare emerging risks with risks considered "familiar" (known risks evolving in familiar conditions, also sometimes called regular, routine, known or conventional risks). The concept of familiarity assumes the existence of recognisable patterns and management regimes that are relatively stable and have proven to be effective if implemented according to certain rules. By contrast, **emerging risks are characterised mainly by uncertainty regarding their potential consequences and/or probabilities of occurrence. This can be due to a lack of knowledge about causal or functional relationships between new risk sources and their environment or to the insufficient application of available knowledge to the case in question**.

The notion of familiarity emphasises that a familiar risk is familiar to a risk manager who, therefore, knows how to manage it. A risk may be familiar to certain risk managers but not to others who may thus not be aware of how to manage it.

Although this report frames emerging risks as a distinct phenomenon, in reality no sharp distinction exists between emerging and familiar risks, with

---

[4] Although low-probability, high-consequence risks are not excluded, clearly this categorisation is not specifically identified to anticipate them or the extreme case of "unknown unknowns".

[5] Some of the examples provided in this report may be "past" emerging risks. They have been chosen to provide evidence of how emerging risks were managed in the past, including certain assessment or management options, that could be relevant for emerging risks in general. Examples provide lessons from hindsight or from experience.

instead a continuum where emerging risks progressively acquire some of the features of familiar, known, risks. Through information gathering and effective management, emerging risks can become familiar risks over time.

People and organisations exposed to emerging risk must be prepared to deal with environments characterised by instability and high uncertainty of future impacts, with various sets of interactions and cascading effects. It is difficult to imagine what has never happened before; the context is often difficult to describe and frame. The future development of cyberspace, for example, with trends such as cloud computing, big data or the Internet of Things is, at least today, beyond most people's imagination.

In emerging risk management, what matters most to an organisation is its potential **exposure**. At the early stages of risk assessment, focusing on likelihood or impact can be misleading, since the underlying uncertainty makes conventional approaches to projecting loss size, relative frequencies, probability distributions or severity of consequences ineffective. To analyse potential impact, however, the necessary "filtering process" requires the assumption of some form of likelihood and relevance to the organisation. Attempts to assess emerging risks with technical or scientific instruments may prove futile as the scientific understanding of these risks can change rapidly. Therefore, **adaptability and flexibility** are crucial.

1.2 Emerging risk governance
—

Emerging risk governance begins with the process of regularly revising the organisation's portfolio of risks and opportunities. This involves scanning the environment and analysing the many signals and trends produced by early-warning systems.

An organisation's risk portfolio (or "risk profile", i.e. the description of the sets of risks that may affect it) is most often revised in three cases:

- After an accident or a "near miss"[6] (correctly analysed and treated)
- After an observed change in the organisation's environment (a new regulation, technology, entrant in the market, social or economic trend, climatic conditions, etc.)
- Through a forward-looking exercise to analyse existing and possible future trends, practices, drivers and conditions of change

In the first two cases, the organisation is reactive. When a dramatic accident or change cannot otherwise be averted, reactive approaches may be relevant (and may indeed be the only possible approach), although they have limitations (see Box 2).

This report focuses on the third case. It **promotes a proactive strategy** and suggests a process to implement it in a systematic and reflective way.

[6] The concept of "near miss" implies that a given accident sequence was stopped before adverse consequences occurred. This concept originated in the aviation industry, to analyse and draw lessons from events that could have led to accidents.

Proactive emerging risk governance

Proactive governance of emerging risks aims to **enhance anticipation and forward-looking capabilities**. Projecting managers into their possible future operating context helps highlight decision opportunities and provides them with additional lead time to prevent risks from emerging or to manage their consequences.
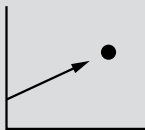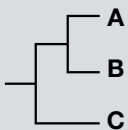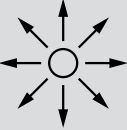
At this point, two important questions must be asked:

- As conventional risk management approaches imply a certain form of prediction (typically with anticipatory assessments to prevent the risk from materialising), what additional capabilities for "looking forward" does proactive ERG contribute?
- As looking to the future involves uncertainties (which increase with the passage of time), emerging risk management shares commonalities with uncertainty management. How can uncertainties related to the future be dealt with effectively?

Preliminary responses are provided by a typology of the various levels of uncertainty that a manager can face (see Figure 1).

Anticipatory approaches used in risk management allow decision-makers to deal with the first two levels of uncertainty. Most commonly, risk assessment addresses the combinations of events described at levels 1 and 2 that may lead to adverse consequences. Each combination has its own probability distribution, based on statistical calculations derived from past distributions or on Bayesian assessments of experts' strength of belief, and an evaluation of the adverse consequences. Risk assessment is thus the outcome of anticipatory approaches involving knowledge of system components and associated dynamics on the one hand, and the ability to imagine adverse combinations of those dynamics on the other.

Yet even if perfect knowledge of these distributions were possible and empirically validated probabilities could be assigned to each alternative at each junction (see level 2), the aggregate of all probabilities over several junctions

		Level 1	Level 2	Deep Uncertainty Level 3	Deep Uncertainty Level 4	
Determinism	**Context**	A clear enough future	Alternate futures (with probabilities)	A multiplicity of plausible futures	Unknown future	**Total Ignorance**
	System Model	A single system model	A single system model with a probabilistic parametrization	Several system models, with different structures	Unknown system model: know we don't know	
	System Outcomes	A point estimate and condifence interval for each outcome	Several sets of point estimates and confidence intervals for the outcomes, with a probability attached to each set	A known range of outcomes	Unknown outcomes: know we don't know	
	Weight on Oucomes	A single estimate of the weights	Several sets of weights, with a probability attached to each set	A known range of weights	Unknown weights: know we don't know	

would still result in low probabilities even for the most probable route through the event tree diagram. One could imagine five junctions with one resulting alternative of 0.8 probability at each intersection. The last route in this combination would have only a probability of 0.328 ($0.8 \times 0.8 \times 0.8 \times 0.8 \times 0.8$), meaning there is a 0.672 chance that the most probable outcome will not occur. This shows the limitations of this type of analysis even when the level of confidence about the probability distribution is high.

Figure 1: A typology of uncertainties (Source: Walker, Marchau & Swanson, 2010)

Anticipatory practices used in risk management are limited by the set of events that can be studied (see for example the "Cause Consequence" diagram in Figure 2). Two types of boundaries can be observed. The first boundary is temporal and occurs when only events considered plausible today and characterised by a probability distribution are studied. No or very little consideration is given to projections of how the system components may evolve or what the impact of the resulting developments may be. The second type of boundary is socially constructed. It results from the fact that practitioners incrementally define the extent to which their imagination should be limited, as well as what should and should not be taken into account in defining combinations of events. For instance, plane crashes are systematically considered as possible events in the risk assessments of nuclear power plants (US NRC, 2007), but are generally not taken into account in those of non-nuclear infrastructure.

In industrial risk assessment, "bow ties" represent various possible combinations of events leading to the hazardous incident (a toxic release, explosion, etc.). Each path from one extreme of the bow tie to the other is a possible risk sequence characterised by a distribution of probabilities and an evaluation of consequences.
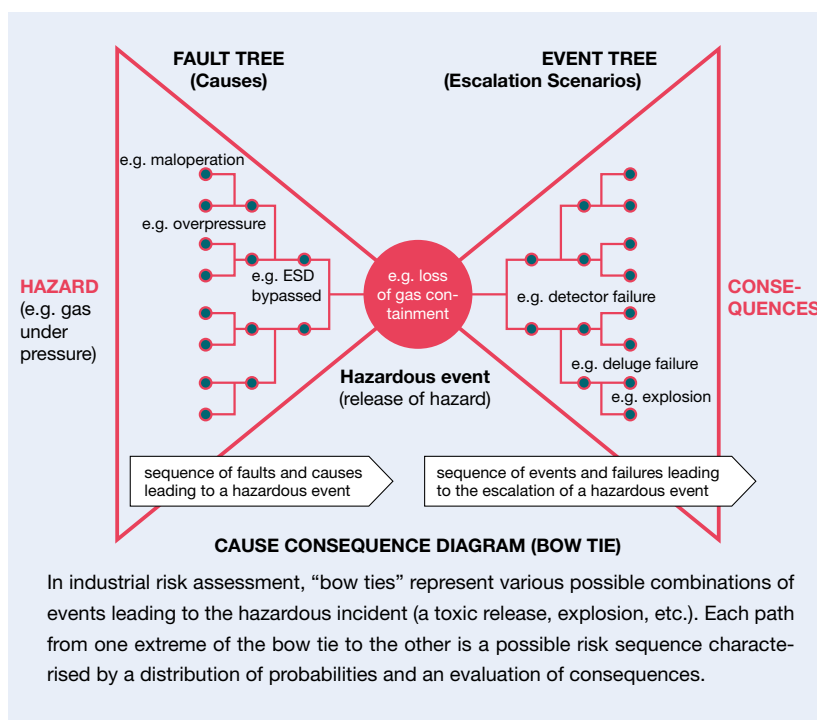
Figure 2: Anticipation in classic risk assessment: The bow-tie approach (Source: Author)

Emerging risk management, in its proactive form, must go beyond these limitations. It must help decision-makers deal with deeper levels of uncertainty (levels 3 and 4 depicted in Figure 1), where no reliable distribution of probabilities is available and only incipient trends of possible future evolutions exist, suggesting that various futures may affect the organisation[7] (see Appendix 2.2).

Scenario planning and strategic foresight

To deal with high levels of uncertainty and explore the future, it is necessary to **go beyond conventional anticipatory approaches** of forecasting that rely on past data to predict the future (Anderson, 1997). It is also necessary to go beyond the usual Bayesian approach of eliciting and calibrating expert judgments. **Emerging risks often arise from complex and interrelated systems**, the dynamics of which are potentially subject to positive feedback, non-linear evolutions and stochastic behaviour. Relying exclusively on experience or expert judgments to describe the future may thus lead to disillusions. The mutation of viruses, the development of antimicrobial resistance, financial crashes or the potential collapse of large electricity networks are examples of entire systems going through sudden and new, unanticipated and uncontrolled shifts that to a large extent remain unexplained.

The type of anticipation required for emerging risks in complex systems and uncertain environments includes combining expertise on complex dynamics and expanding one's imagination beyond the limits of experience (described as "disciplined imagination"). This involves developing scenarios of possible futures and exploiting them for decision-making even if no probability distributions are available (van Notten, 2006; Healey & Hodgkinson, 2008; Wilkinson & Kupers, 2013).

Governing emerging risks at strategic levels, in all phases of decision-making

Like other disciplines such as dynamic capabilities or innovation management (see Appendix 2.2), the governance of emerging risks needs to be performed at strategic levels of decision-making in order to cope with both underlying complexity and uncertainty, and to trigger the required deployment and implementation dynamics at all levels of an organisation.

Strategic decision-making involves a set of competences that align well with the challenges of emerging risk governance and, in general, a proactive approach to long-term thinking and acting. The most common features of strategic decision-making include a long-term view (JI, 2010), the configuration or reconfiguration of resources and competences within a changing

---

[7] The Dutch Environmental Assessment Agency proposes to emphasise the important difference between "statistical uncertainty" and "scenario uncertainty" (as well as "recognised ignorance") in order to improve the assessment of uncertainty. The evaluation of uncertainty can be further refined by paying specific attention to framing the problem and by consulting stakeholders (PBL Netherlands Environmental Assessment Agency, 2013). In line with the terminology used in the IRGC white paper on risk governance (IRGC, 2005), the sources of uncertainty are target variability, systematic and random error in modelling, indeterminacy or genuine stochastic effects, system boundaries, and ignorance or non-knowledge

environment (Johnson, Scholes, & Whittington, 2008), as well as the need to deal with issues that are ill-structured, non-routine (Mintzberg, Raisinghani, & Theoret, 1976) and complex (Elbanna, 2006).

Implementing strategic decisions about emerging risks may imply large cultural, technical and organisational shifts that will have an impact on the entire organisation. Such decisions need to be taken at the organisational levels where objectives, performance criteria and individual practices can be aligned, questioned and revised if some of them prove to be inappropriate. The ability of strategic decisions to engage substantial resources, set precedents and create decision waves at lower levels (Dean Jr. & Sharfman, 1993) defines the necessary conditions for successfully implementing the outcome of ERG processes.

ERG in organisations must thus not be a stand-alone exercise. Many of the risk management practices are generic, and addressing emerging risks must be embedded within a core corporate or organisational process.

1.3. The emerging risk "conductor"
—

Complex organisations should organise their response to emerging risks in a structured manner. Developing and deploying a systematic process for ERG to support strategic decision-making require coordinating various kinds of technical expertise, challenging existing organisational routines and balancing possibly conflicting individual stakeholder objectives within and external to the organisation. Emerging risk governance hence requires leadership: it needs a "conductor".

Just as the conductor of an orchestra shapes the overall sound and tempo of the musicians' performance, the role of the emerging risk conductor is to ensure the effective implementation of the guidelines.

The conductor and team must have the mission and resources to lead the process and to:

- **Facilitate** interactions between the participants, who may have different objectives and expertise. Special attention should be given to ensure that the needs for support and decision-makers' preferences are adequately addressed and considered before the emerging risk management options are selected.
- **Validate** technical frameworks and approaches adopted during the process, by considering their scientific soundness and appropriateness to the organisation's resources and needs.
- **Monitor** performances to demonstrate their relevance for the organisation and, if required, identify and correct weaknesses. Monitoring the performance of outcomes is challenging, so focusing on the performance and robustness of the process may be useful, rather than being fixated on outcomes.

- **Promote** behaviours and attitudes in line with the cultural challenge raised by emerging risk governance. Ensuring transparency, encouraging divergent views, avoiding simplistic visions and eliciting the consideration of extreme and highly unlikely events are examples of what is required to overcome cognitive bias (possible deviation from a standard of rationality) and organisational opposition.
- **Communicate** internally and externally to increase awareness of and concern for emerging risks, create a favourable climate for ERG, explain and clarify decisions, and answer questions.
- **Report** on the potential impact of emerging risks on various sectors and their management.
- **Periodically review** whether the adopted risk management framework and strategy options still conform with the organisation's internal and external context.

The concept of a "**risk owner**" who, in some organisations, is assigned responsibility for the effective management of a risk is different from the concept of the emerging risk conductor. The conductor is in charge of coordinating and facilitating the emerging risk governance process. The responsibility and accountability for making the organisation responsive to and literate about risk management is the task of the risk owner, if this function exists in the organisation.

The role and position of the conductor and team may vary depending on the organisation's structure (it could be the chief risk officer), or the type of organisation and regulatory framework. In some cases, the organisation has a legal mandate to address and deal with emerging risks. This, for example, is the case at the European Food Safety Authority (EFSA) or the European Union Agency for Network and Information Security (ENISA). In other instances, the organisation itself has determined that internal decision-makers need insights regarding emerging risks. Most insurance companies have emerging risk units that provide operational business units with validated information on new issues representing opportunities and risks for the insurance market. Whether ERG is performed within or outside a legal mandate, the internal process will be scrutinised for its capacity to provide effective and relevant outputs and benefits for the organisation. This can be challenging, as avoided risks are often "invisible" and avoided losses cannot be easily evaluated.

Some governments have a chief scientific adviser (CSA) who provides scientific advice to all departments. He/she makes suggestions, organises, facilitates and provides overall advice on the use of evidence-based information for policymaking and regulations. The CSA is not in charge of handling all scientific issues, but can help to mediate between science, stakeholders and politicians, especially in situations of uncertainty and ambiguity. This role is similar to the emerging risk conductor.

2.

IRGC GUIDELINES FOR EMERGING RISK GOVERNANCE

Defining an appropriate framework and a model process is of critical importance for effective risk governance, whether in the public or private sector. The guidelines proposed by IRGC provide an overarching framework to support senior managers in addressing emerging risks. They help to organise how information and evidence are collected, analysed and combined to design strategies for ERG.

The guidelines are to be further developed and adapted to each organisation, with the assistance of an emerging risk conductor. They rely on strong leadership and the willingness to challenge organisational routines and focus on mid- and long-term issues. The process is adaptable to organisational specificities.

At a broad strategic level, implementing these guidelines should result in four distinct key capabilities:

- Enhancing proactive thinking to identify future threats and opportunities
- Evaluating the organisation's willingness to bear or to avoid risk (risk appetite) for the definition of future strategies
- Prioritising investments in certain key emerging issues according to their potential impact
- Fostering internal communication and building a forward-looking culture to benefit the whole organisation

Objectives of the guidelines

The IRGC guidelines for ERG:

- **Provide guidance to organisations in anticipating and responding to emerging risks**
  Risk emergence can be a long process that can create opportunities for early and effective interventions. If, for example, an industrial process involves a new material with potential yet unproven risks, the organisation can take early management measures, such as substituting the material with a more benign one or monitoring the likely impact over an extended period, before releasing the material into the environment.

- **Provide transparent and enforceable criteria for the evaluation of the effectiveness of the ERG process, underlining, *inter alia*, the relevance and usefulness of foresight approaches and the legitimacy of decisions**
  Reflexivity, defined as the process of evaluating the relevance and quality of organisational processes, is a key issue in management. It implies answering two key questions: Do we need to do what we are doing? If yes, are we doing it right? Exploring these questions provides organisations with the capacity for continuous improvement as well as the ability to justify decisions already made. No guidelines for ERG can escape this rationality, as it may result in difficult decisions, like investing money today to avoid a hypothetical loss in the future. The more difficult the decision, the stronger the requirement for legitimacy. Demonstrating legitimacy is important for ERG to ensure that it will be taken into account when decisions are made. As reflexivity in ERG can hardly be performed through the direct evaluation of outputs that may only be revealed after a long latency period, IRGC suggests focusing on procedural evaluations through a set of evaluation criteria for each of the steps described in the guidelines.

- **Embed the emerging risk management process as a routine within the organisation, drawing from existing processes**
  Drastic events, or even catastrophes, often occur because early-warning signals were ignored. In addition to the Kodak example described in Box 2, the Pearl Harbor attack in 1941 or the Challenger Shuttle accident[8] in 1986 are relevant examples. Generally, organisations do not often try to anticipate emerging risks, even in the field of technology (Petersen, 2008). It is therefore important to tightly link foresight capabilities to strategic decision-making structures. This requires the ERG process to become a part of the organisation's routine.

IRGC stresses the relevance of establishing links in an organisation between risk managers and those in charge of strategic planning, innovation management and other management functions. These links need to be made at the conceptual level – the focus of this report – as well as at the practical level, as illustrated in case studies that IRGC is developing as a complement to this report.

---

[8] Also see Hodgkinson & Starbuck, 2008.

The IRGC guidelines for ERG (as shown in Figure 3 below) comprise five consecutive and interlinked steps. The following sections give a detailed description of each step, its objectives, key participants and expected outcomes.
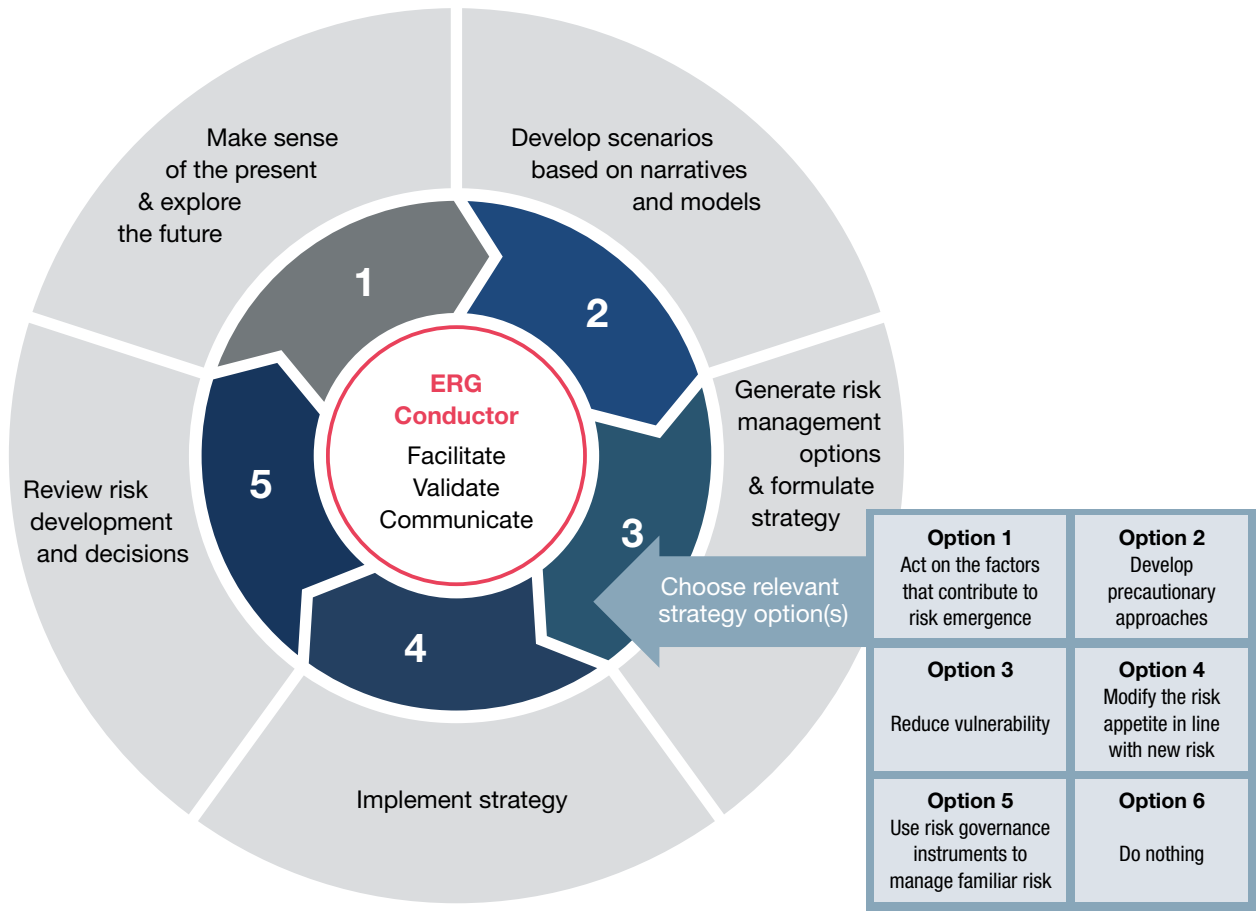
Figure 3: IRGC Emerging Risk Governance Guidelines

STEP 1

MAKE SENSE OF THE PRESENT & EXPLORE THE FUTURE

KEY OBJECTIVE: PROVIDE EARLY WARNING

Prerequisite: Establish a process to continuously screen the organisation's internal and external environment, to provide reliable and updated inputs to the ERG process.

Step 1 provides **early warning** by identifying:
- Potential threats or opportunities to relevant assets and processes.
- Contributing factors that create fertile ground for risks and opportunities to develop (emerge, amplify or attenuate).

It aims to **make sense of signals** that might shape the future.

REQUIRED ACTIONS »»»»»»»»»»»»»»»»

- **Detect** and **explore** current and possible future evolutions that may change the organisation's environment.
- **Analyse** these changes according to their ability to represent a threat and/or an opportunity in the short and medium term.
- **Filter** and **prioritise** the set of detected threats and opportunities to identify those that require further attention in Step 2, and those that can be decommissioned.
- Regularly **update** the selection of risks and opportunities when new information becomes available.

EXPECTED OUTCOMES

- **List of selected threats and opportunities** that is regularly updated and that requires further analysis because of potential positive or negative, immediate or long-term, impact on the organisation.
- **Description of the context** in which these threats and opportunities may develop.
- Identification of the **necessary or sufficient conditions** for the risk or opportunity to materialise.
- **List of threats and opportunities that are irrelevant** to the organisation's objectives given information available at the time.

KEY PARTICIPANTS & RESPONSIBILITIES

Emerging risk conductor .... defines approaches and facilitates continuous interactions among experts and between experts and decision-makers.

Experts and analysts .... detect signals, perform analyses and suggest necessary characterisation.

Senior decision-makers .... validate Step 1 outputs and decide which issues will be further investigated and what resources will be allocated to the process.

KEY SUCCESS FACTORS
- Diversity of information
- Scientific soundness of data collection, analysis and prioritisation
- Data reliability and consistency
- Compatibility with existing and past or familiar threats

What to do and how
—

Challenged by a variety of sources and combinations of diverse risks and opportunities, organisations need rigorous, replicable and systematic tools for scanning and understanding their internal and external environment. At the first step of the process, the conductor will establish processes for identifying and describing possible futures in which risks and opportunities may develop.

Detection – data and information collection

At the early stages of emerging risk/opportunity development, available information is likely to be poor, highly uncertain and subject to divergent interpretations. Despite these characteristics, this type of information, described as weak signals, may serve the purpose of avoiding strategic surprises and preparing to deal with turbulent environments. Detecting and interpreting weak signals have become key objectives of the weak signals theory and, to a larger extent, of futures studies (Rossel, 2009). Environmental or horizon scanning is defined as a systemic process of strategic learning about organisations' circumstances (Spies, 1991) that aims to identify new developments that can challenge past assumptions or provide a new perspective on future threats and opportunities (Gordon & Glenn, 1994). Horizon-scanning activities can be fully exploratory or issue centred (Amanatidou, et al., 2012).

There are various ways to engage in detection practices and approaches:

- In some cases, the organisation does not have the internal capacity to develop its own detection and analysis expertise. In this case, it can **rely on predefined lists** of emerging risks and opportunities described by national and/or international entities: foresight agencies, consulting firms, professional associations, international organisations, etc.
- In other cases, the **organisation may be willing to invest resources in horizon-scanning activities and early-warning systems** to improve its own ability to identify weak signals and early warnings indicating possible shifts.

Early-warning systems can be developed in complementary ways:
- *Expert panels* may provide regular inputs on incipient or forthcoming changes. These can be collected through questionnaires, essays or moderated workshops.
- Due to the development of large databases, social media and artificial intelligence, it is becoming increasingly affordable and effective to *scan and analyse large amounts of various types of information*, ranging from scientific essays and papers to public perceptions and opinions (semantic data mining). *Keyword tracking*, *trend evolutions* or the *number of significant occurrences of an event* are examples of valuable information that automatic scanning can capture.
- Environmental scanning can also be performed by tracking the existence of contributing factors to risk emergence as described by IRGC (2010a) (see Box 3). Examples are the analysis of information asymmetries, the identification of scientific unknowns or the identification and analysis of perverse incentives in the organisation's context.

irgc

Box 3: Contributing factors to risk emergence

Factor 1: Scientific unknowns

Scientific unknowns, whether tractable or intractable, contribute to risks being unanticipated, unnoticed and over- or underestimated.

Factor 2: Loss of safety margins

The level of connectivity in many of today's social and technical systems is greater than in the past and the interconnections are increasing. The pace at which these systems operate is intensifying and many are operating under high levels of stress. This can lead to tight coupling of components within systems and to a loss of safety margins.

Factor 3: Positive feedback

Systems exhibiting positive feedback react by amplifying a change or perturbation that affects them. Positive feedback tends to be destabilising and can thus amplify the likelihood or consequences of an emerging risk.

Factor 4: Varying susceptibilities to risks

The consequences of an emerging risk may be different from one population to another. Geography, genetics, experience and wealth are just some of the possible contextual differences that create varying susceptibilities to risks.

Factor 5: Conflicts of interest, values and science

Public debates about emerging risks seldom show a clear separation between science, values and interests. This results in conflicts that create fertile ground for risks to emerge or amplify.

Factor 6: Social dynamics

Social change can lead to social harm. In other circumstances, it can attenuate potential harm. It is therefore important for risk managers to identify, analyse and understand changing social dynamics.

Factor 7: Technological advances

Risk may emerge when technological change is not accompanied by appropriate prior scientific investigation or post-release surveillance of the resulting public health, eco-nomic, ecological and societal impacts. Risks are further exacerbated when economic, policy or regulatory frameworks are insufficient. Yet technological innovation may be unduly delayed if such frameworks are overly stringent.

Factor 8: Temporal complications

A risk may emerge or be amplified if its time course makes detection difficult or if the time course does not align with the time horizons of concern to analysts, managers and policymakers.

Factor 9: Communication

Risks may be complicated or amplified by untimely, incomplete, misleading or absent communication. Effective communication that is open and frank can help to build trust. In many cases, such communication can lead to better anticipating and managing emerging risk.

Factor 10: Information asymmetries

Information asymmetries occur when some stakeholders hold back key information about a risk that is not available to others. These asymmetries may be created intentionally or accidentally. In some cases, the maintenance of asymmetries can reduce risks but, in other cases, it can be the source of risk or amplify a risk by creating mistrust and fostering non-co-operative behaviours.

Factor 11: Perverse incentives

Perverse incentives are those that induce counterproductive or undesirable behaviours, which lead to negative, unintended consequences. Such incentives may lead to the emergence of risks, either by fostering overly risk-prone behaviours or by discouraging risk prevention efforts.

Factor 12: Malicious motives and acts

Malicious motives give rise to emerging risks and therefore practitioners need to consider intentional as well as unintentional causes of risks. Malicious motives and acts are not new but, in a globalised world with highly interconnected infrastructures, their effects can have a much broader impact than in the past.

Source: IRGC, 2010a

Exploration

Organisations can decide to invest and engage in **exploratory exercises** to imagine and describe the future context in which identified opportunities and threats may arise and evolve. These exercises to sketch out possible futures require building upon a very large set of expertise and imaginative capabilities. Under the auspices of Pierre Wack (1985a; 1985b), Shell has been developing exploratory scenarios (Ramirez et al., 2011) for more than

30 years. Although this approach requires extensive resources, it provides a broad and comprehensive vision of the new threats and opportunities that may unfold in the future. In addition, it contributes to the development of an organisation's internal capacity to make sense of change and events. This capacity will also be useful at a later stage of the process (see Steps 3 and 4), for decision and strategy implementation.

The concept of "**disciplined imagination**", developed to describe the process of theory construction in organisational studies (Weick, 1989; Cornelissen, 2006), can also be applied to the exploration of future organisational contexts from which risks may emerge.

Analysis – making sense of information

The signals identified through horizon scanning (including early-warning systems) and the exploration of the future need to be further analysed and transformed into knowledge. In many cases, the possible consequences of signals are not easy to understand. In such cases, the process of assigning meaning to the outcome of scanning and exploratory exercises is usually described as sense-making (Weick, Sutcliffe, & Obstfeld, 2005).

Analysis and sense-making include the following aspects:

- Link the threat/opportunity to what is valuable for the organisation
- Describe the mechanisms and rationality underlying the emergence of a threat or drivers in changes to risk and opportunity profiles
- List the factors that may contribute to risk emergence or attenuation/ disappearance in the future
- Describe early signals of change detected in the environment, such as information in press releases, research papers or a rise in stakeholders' concerns
- Detail the pros and cons of further analysing the threat/opportunity in the next steps of the guidelines

Filtering and selecting potential threats that require attention

As the set of threats and opportunities identified can exceed the organisation's capacity for further analysis, a filtering process is required.

The filtering exercise can be performed according to the following qualitative and quantitative criteria:

- Exposure of the organisation
- Vulnerability of the organisation
- Possible impact (and severity of consequences) to the organisation's business or core values
- Estimated likelihood of a threat to materialise
- Available lead time before the threat/opportunity becomes reality
- Awareness level among competitors and civil society

The emerging risk conductor will select and describe the criteria according to the specific needs of the organisation. Filtering should occur each time additional knowledge is available, if this knowledge enables a (re)definition of priorities. Accordingly, this first filtering process can be revised or completed once scenarios and narratives have been elaborated upon in Step 2, offering a more comprehensive description of the set of threats/opportunities at hand. Filtering is not a neutral process. The choice of filters that select which information produced by horizon scanning will be used for strategic planning, decision-making (Ilmola-Sheppard, 2014) or in-depth exploration of emerging risks (Step 2) can have a large influence on the outcome.

In general, it is extremely difficult for an organisation to prioritise emerging threats or risks. It may prove to be more productive to adopt a risk-based approach to decision-making (for example prioritising investment) based on resources, capabilities and return on investment (see Step 3). The following examples show how organisations can proceed with the filtering process.

Box 4: Characterising and prioritising threats - The Dutch National Risk Assessment

National Risk Assessments are being developed in countries whose governments wish to conduct comprehensive identification, prioritisation and assessment of the major risks (resulting, for example, from natural hazards, pandemics or terrorism) that may affect the national and societal security of the country.

In the Netherlands, for instance, threat prioritisation is performed with the aid of experts according to the following impact criteria (BZK, 2009):

• **Territorial safety**, divided into "encroachment of territorial integrity of the Netherlands" and "infringement of the international position of the Netherlands"

• **Physical safety**, regarding "fatalities", "the seriously injured and chronically ill" and "physical suffering (lack of basic necessities of life)"
• **Economic safety**, evaluated according to a cost criterion.
• **Ecological safety**, describing the long-term impact on flora and fauna
• **Social and political stability**, appreciated according to three criteria, "disruption of everyday life", "violation of the democratic system" and "social and psychological impact"

A two-dimensional diagram provides a graphic representation of the threats and their criticality (likelihood and impact), permitting the selection of those deserving further analysis in the next steps. In addition, capabilities are analysed to decide which threats the government can aim to deal with.
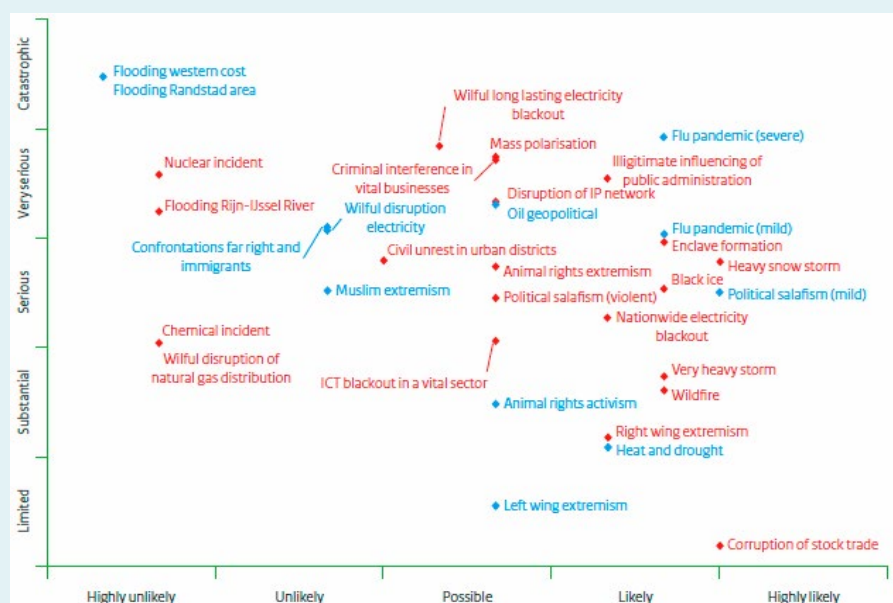
Figure 4: Example of a national risk prioritisation approach (Source: BZK, 2009)

Box 5: Using horizon scanning to prioritise threats and opportunities

The Institute for Environment, Health, Risk and Futures (IEHRF) at Cranfield University performs regular horizon-scanning exercises allowing the identification and prioritisation of emerging issues considered of importance for the entire society, including economic, environmental and social dimensions. The impact of these issues can be identified as either a threat or an opportunity or both, depending on the particular viewpoints of the observers, and is classified using risk prioritisation criteria. The issues are presented to illustrate a measure for importance, which combines levels of likelihood and expected impact, and a time horizon, which shows the current understanding of the expected timeline for the impact's occurrence. In the October 2013 "IEHRF Horizon Scan", 24 distinct threats and opportunities were identified and rated as shown in Figure 5.

The time horizon axis represents the expected time of impact and not the time required for decision-making. However, threats and opportunities categorised as possibly occurring ten years or more from now may still require an immediate decision.
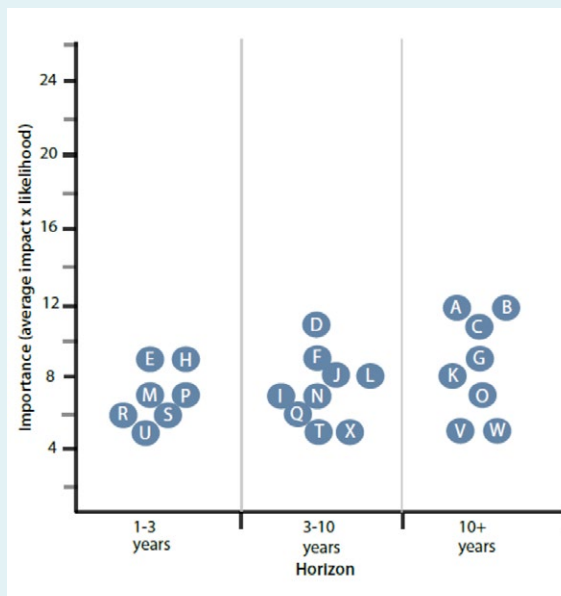
Figure 5: Example of threat and opportunity ratings
(Source: Rathe, et al., 2013)

It should be noted that scenario development can become expensive and time-consuming. Many organisations do not have the resources to undertake this costly exercise, but can find relevant material elsewhere. Additionally, scenarios can be out of date before they are published, as they take long to develop. It may be sufficient to use readily available scenarios and tailor them to the receiving audience/organisation. However, as pointed out by Healey and Hodgkinson (2008), there are occasions when this approach might not yield the benefits expected, due to a lack of engagement on the part of the recipients. Generating the scenarios from scratch, through a process of active mental simulation and engagement provides a more direct and immediate assessment of emerging risks – which is what most organisations are looking to accomplish.

An illustration is provided in Appendix 2.3: The use of signals and early warnings in technology management.

STEP 2

DEVELOP SCENARIOS BASED ON NARRATIVES & MODELS

KEY OBJECTIVE: DEVELOP SCENARIOS

Step 2 describes **scenarios** of how an emerging risk or opportunity could impact an organisation and its objectives. It:
- Offers the possibility for collaborative framing of existing and future threats and opportunities.
- Provides evidence and support for future decisions concerning the identified threats and opportunities.
- Updates the scenarios as new information and knowledge become available.

REQUIRED ACTIONS ⟩⟩⟩⟩⟩⟩⟩⟩⟩ EXPECTED OUTCOMES

- **Develop** or use various types of scenarios to explore and **evaluate** the emerging risk that could affect the organisation in the future.
- Begin to identify possible **bifurcations** and **intervention points**, to prepare the development of management options.
- Update the scenarios as necessary, taking into account the emergence of new signals and the outcome of strategic interactions with stakeholders.

- **Set of explorative scenarios**. The scenarios describe how the threats and opportunities identified in Step 1 may have an impact on the organisation. Particular attention must be given to:
  · The contributing factors (amplifying or attenuating).
  · Events or tipping points that may accelerate, reduce or generally affect the factors.
  · The consequences of each scenario for the organisation.
- **Familiarity with concepts**. During the process, participants will become increasingly familiar with new concepts (e.g. "low-probability/high-consequence events"), contributing to a common understanding of possible future developments.

KEY PARTICIPANTS   &   RESPONSIBILITIES

Experts in futures studies & scenario-building techniques .... facilitate interactions between contributors and ensure the scientific validity of the scenario development exercise.

Emerging risk conductor .... ensures the coherence of the exercise with the threats and opportunities defined in Step 1 and the organisation's expectations.

Decision-makers .... confirm their commitment, in particular by allocating resources, providing reward and assigning responsibilities.

KEY SUCCESS FACTORS ⟩

- Relevance to the concerns and needs of the decision-makers
- Credibility, to assess the scientific soundness of the models and data used as well as the transparency of the choices made at each step of the process
- Comprehensibility and traceability, to describe the clarity of the sequence of events adopted to structure the scenarios and the ability of final users to easily understand and follow the underlying rationality
- Legitimacy, through openness of the process to various stakeholders, promoting different values and political orientations
- Creativity, to stimulate new ways of thinking and dealing with the "unusual"
- Distinctness, to assess the ability of the scenarios to jointly convey to decision-makers the diversity of possible futures

What to do and how
—

At this stage, potential threats as well as possible opportunities have been identified. Their potential impact on the organisation's future must now be further analysed. By adopting a forward-looking approach, Step 2 will rely on scenarios (based on models and narratives) to describe how threats and opportunities may become risks that need to be managed, or may develop into opportunities that need to be pursued to transform them into competitive advantages. The incentive for the risk manager here is to help his / her organisation harness risk but also to explore new opportunities.

Developing and using scenarios implies a process of looking to the future and developing possible stories about how it may unfold. Organisations can also use scenarios that have already been developed and move directly to identifying the implications – both risks and opportunities.

Scenarios represent combinations of formal models and plausible narratives (Helgeson, van der Linden, & Chabay, 2012; Wilkinson & Kupers, 2014). Depending on the topic and the state of the art of available knowledge, scenarios differ in the composition of formal modelling and storytelling. Some scenarios pursue well-known causal or functional relationships and vary primarily in their assumptions. In contrast, others develop imaginative futures based on basic knowledge, formal logic and plausibility. Almost all scenarios include methods to involve multiple actors and factors in the description of what the future could look like. Explorative scenarios ask "what if?" questions to look into alternative views of the future and create plausible stories from them. They consider long-term trends in society, the economy, policy or technology (relevant to the field in which the organisation develops), as well as factors that could trigger shifts in these trends. Visions of the future are thus built in an open process, the result of which represents the participants' points of view. For the purpose of this report, scenarios are defined as hypothetical sequences of events constructed for focusing attention on causal processes and decision points (Kahn & Wiener, 1968). Both quantitative and qualitative approaches of scenario elaboration have been considered within this work.

Scenarios are not meant to predict the future but, in the specific context of ERG, they can help to structure and organise the many uncertainties decision-makers are confronted with. Scenarios are used by organisations looking to enhance their ability to deal with the inherently uncertain and complex character of their environment (Healey & Hodgkinson, 2008). The benefits of this approach range from considering uncertainty in strategic decision-making to organisational learning and the construction of a common understanding among participants. There is, moreover, growing evidence that scenario planning is contributing effectively to the development of competitive advantages for organisations. [9]

The selection and use of scenarios depend largely on the context and the objectives. If the original aim of scenario *development* was purely norma-
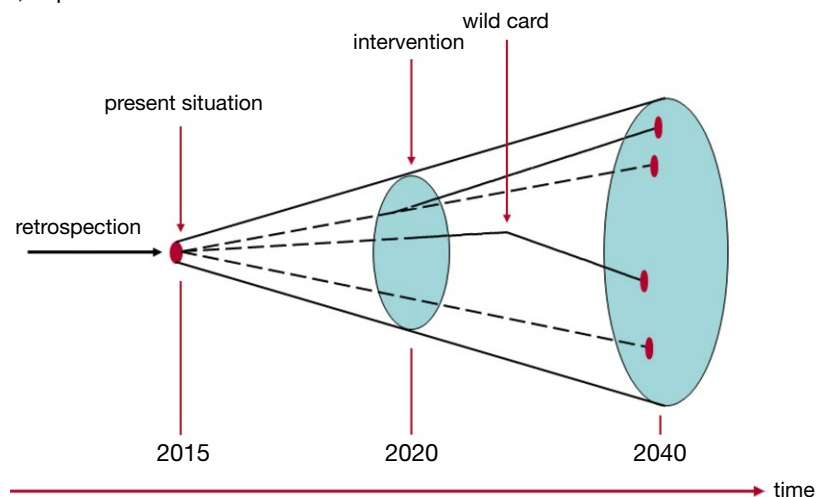
---

[9] See Mannermaa, 1986; Rohrbeck, Arnold, & Heuer, 2007.

tive at first, advances in this field have led to three types of purposes and associated practices [10]:

- *Predictive scenarios* describe and anticipate what will happen if the rules that have been governing the system's development thus far continue into the future. These types of scenarios tend to be described as *business as usual*.
- *Explorative scenarios* acknowledge the possibility that different futures could develop from current conditions. Divergent futures may result from known or unknown trends and events for which a probability distribution does not exist.
- *Normative scenarios* are usually based on backcasting. The first step in a backcasting approach is to define the desirable end-state, most often through a multi-stakeholder (participatory) process. Because of this visioning process, such scenarios are considered normative.

Explorative scenarios

Explorative scenarios are funnel-based approaches (Kosow & Gassner, 2008) that imagine various possible futures based on current knowledge and trends (Figure 6). In the case of ERG, explorative scenarios focus on the construction of plausible sequences of events where present threats and opportunities may become risks to be managed or competitive advantages to be pursued. Practitioners must also consider the possible impact of extreme variations in known distributions, as well as disruptive events and surprises often referred to as "black swans" (Taleb, 2007) The goal is to ensure that the exercise can also support the development of resilience capabilities in Step 3.

Figure 6: Funnel-shaped model of the variety of possible futures

(Source: Adapted from Schüll & Schröter, 2013)

The type of scenario development suggested here differs from the exploration of threats and opportunities conducted in Step 1, whose purpose was to imagine and describe the evolution of contexts where threats or opportunities may arise. In this second step, the objective of the exploration is to examine the impact of a set of identified threats to and opportunities for the organisation's strategy.

Explorative scenarios are widely used in organisational practices. However, practitioners should be aware of the following limits and biases when engaging in this exercise:

- Both extreme ("worst-case") scenarios and "reference" scenarios must be considered, to explore the full range of possibilities.
- If a set of scenarios is too large, it may be cognitively and organisationally difficult to use. On the other hand, a set of scenarios that is too narrow will not be representative of the variety of possible futures based on current

[10] See also van Notten, 2006; Börjeson et al., 2006; Vergragt & Quist, 2011.

knowledge. Scenarios must be clearly differentiated and include the consideration of extreme events.

- Cognitive (and emotional) biases may mislead scenario construction and exploitation (Healey & Hodgkinson, 2008, 2011). Overestimating the probability of scenarios that seem to be more plausible, not giving the same consideration to a variety of plausible futures and not considering how various affective mechanisms may influence choices are examples of such biases. It is therefore highly recommended to appoint an external facilitator who will organise and moderate interactions between participants and ensure rigour in the process.
- A superficial description of scenarios will be of limited usefulness to decision-makers. Comprehensive and thorough scenario descriptions are likely to support work in Step 3 where management options and decision opportunities have to be identified. Moreover, they will provide a better understanding of the consequences of these decisions.
- The quality of scenario descriptions should be informed by the following criteria: Make an explicit description of the proposed hypotheses, mechanisms and events that are retained as well as those that are not retained, highlight the contributing factors to risk emergence and evaluate the impact on the organisation.

Predictive and normative scenarios can be used in combination with explorative scenarios. They are useful to identify risk management options and intervention points, and thus inform decision-making exercises.

Intervention points

The development of scenarios involves the identification of drivers, but also of critical events that may trigger critical transitions and change the course of the risk development. It results that specific intervention points can be pre-identified and will be used for selecting and deploying specific management options in Step 3.

Filtering and prioritisation

As models and narratives enable risk managers to improve their understanding of how threats and opportunities will or could influence an organisation's values and assets, additional filtering and prioritisation processes – using the same criteria as described in Step 1 – can be performed. This may provide additional evidence of the impact or the absence of real impact on the organisation. In the latter case, more threats and opportunities may be decommissioned.

Methodology and example

A methodological note on scenario development is provided in Appendix 2.4. In addition to theoretical considerations, it provides three examples of scenarios exploring the possible development of the increasing trend towards obesity. It highlights some key features of scenario development and how methodological choices may influence the final output.

STEP 3

GENERATE RISK MANAGEMENT OPTIONS & FORMULATE STRATEGY

KEY OBJECTIVE: MAKE DECISIONS ABOUT THE MANAGEMENT OF AN EMERGING RISK

Step 3 **designs strategies** for the management of emerging risks that are proactive, effective, cost-efficient and adaptive in order to deal adequately with the risks and opportunities explored in Step 2.

REQUIRED ACTIONS >>>>>>>>>>>>>>>>>>>>>>>

- **Identify and evaluate possible emerging risk management options** according to the scenarios developed in Step 2 and the strategy. No option should be excluded.
- **Define intervention points (windows of opportunity) and indicators**, including the most adequate conditions for each option. Select those options that align with the organisation's strategy for dealing with the emerging risk. Consider the organisation's decision-making style, available resources and risk appetite.
- **Identify thresholds of irreversibility** after which interventions will no longer be effective, and thresholds of acceptability, below which no intervention is needed.
- **Communicate** this process and the decision that has been made in a transparent manner.
- Include **uncertainty**: being aware of what is unknown.

EXPECTED OUTCOMES

- **Management strategies** for each scenario: Step 3 is designed to provide a strategy for each of the scenarios developed in Step 2. The description of the strategy, its expected performance and the key trade-offs adopted by decision-makers must be made explicit.
- A final decision as to which emerging risk management option(s) will be implemented.

Option 1 Act on the factors that contribute to risk emergence	**Option 2** Develop precautionary approaches
Option 3 Reduce vulnerability	**Option 4** Modify the risk appetite in line with new risk
Option 5 Use risk governance instruments to manage familiar risk	**Option 6** Do nothing

KEY PARTICIPANTS   &   RESPONSIBILITIES

Decision-makers at the strategic level ..... select options and demonstrate leadership, especially when it comes to challenging comfortable or routine practices not suited to changing environments.

Emerging risk conductor .... facilitates the decision-making process and ensures that decisions are made.

KEY SUCCESS FACTORS

- Flexibility for adaptation and adjustment to new evidence when it becomes available
- Consistency with organisational values and culture as well as with procedures
- Internal openness and transparency of the process
- Clear prioritisation of actions, taking expected impacts and available resources into account
- Revision of the strategy if context and conditions change

What to do and how
—

An important component of effective ERG is making the right decision at the right time. To determine what risk management measures are appropriate and needed, ERG practitioners face the complex challenge of making decisions in a situation of uncertainty about what they need to manage and how.

The third step of the guidelines will use the output of the scanning, foresight and analysis capabilities deployed in Steps 1 and 2.

Strategy is about an organisation's direction and scope over the long term (Johnson, Scholes, & Whittington, 2008). This implies dealing with complexity and uncertainty caused by both external and internal interdependent and uncertain factors, and with ill-structured and non-routine issues (Mintzberg, Raisinghani, & Theoret, 1976). Strategy implementation will trigger "waves" of decision-making at lower levels of the organisation. Decision science [11] will be useful, especially in the face of situations that are new, complex, uncertain or ambiguous.

Risk management is possible when several options are considered and assessed, and one or several are chosen as a strategy. In this section, methodological challenges that analysts (and the conductor) as well as decision-makers may face at this stage are examined.

Generating the strategy and options for implementation

- What strategy and options could respond to the emerging risk?
- When could these options be implemented? What would be the intervention timing?

↓

Evaluating the strategic options

- What criteria will be used to assess and evaluate the options to provide the best response to the variety of possible futures?
- How will the performance of the management options be evaluated?

↓

Making robust decisions

- What decision-making approach will be chosen? How?
- What option or combination of options will be decided?
- What is the timing for implementation?

Figure 7: Step 3 of the guidelines

Generating the strategy and options for implementation

To avoid binary (yes/no) options, a set of options for each possible intervention point in every scenario is needed. In the development of dynamic systems, windows of opportunity for intervention appear, but often only for a short period. Therefore, interventions must be prepared in advance and must be ready for deployment at the right moment. IRGC suggests a typology of possible strategies representing the scope of what can be done when facing emerging risk. These six strategic options are not mutually exclusive and can be partly combined.

[11] Decision science involves the application of quantitative and behavioural methods to the problems of society to study human decision-making behaviour.

Option 1: Acting on the factors that contribute to risk emergence or amplification

Some of the factors that contribute to risk emergence are controllable (IRGC, 2010a). In those cases, an organisation can act to prevent a risk from emerging (or amplifying) or can reduce its consequences if it materialises. Scientific uncertainties or information asymmetries are examples of risk factors that can be controlled within certain limits. An organisation can exercise this control individually or with others. Acting on certain factors can only be achieved by means of a collaborative strategy involving various stakeholders (regulatory bodies, exposed organisations, insurers, etc.), either because the resources required are too costly for each organisation or simply because regulatory or societal shifts might be required. For example, mitigating the consequences of solar storms on electricity grids requires considerable investment and broad co-operation to increase redundancies and (re)install the required safety margins.

The quality of the scenario descriptions is particularly important here. It will be easier to identify and deal with the contributing factors if the drivers and mechanisms of possible development are thoroughly described and analysed during Step 2.

Box 6: REACH, a strategy to act on factors contributing to risk emergence

REACH is a European regulation that aims to manage risks in industry related to chemical substances. It is in line with the chemical industry's Responsible Care Initiative. Industries are required to demonstrate the safety of the chemical substances they use through effective risk management or to replace them with safer substances.

The European Chemicals Agency is in charge of the registration process by which the substance properties are assessed and the risk management actions in place are evaluated. A substance can be banned, restricted to priority uses or authorised.

More information: echa.europa.eu/regulations/reach

The registration process adopted by the EU acts on factors contributing to risk emergence at different levels, seeking in particular to:
- *Avoid or reduce information asymmetries*. Each substance can be registered only once. Therefore, all industries that consider its use must disclose information and knowledge on the substance's properties. By fostering stakeholder co-operation at the early stages of substance development, REACH reduces information asymmetries between industrial stakeholders.
- *Reduce scientific unknowns*. REACH decreases scientific unknowns by encouraging interaction and cross-fertilisation between industries.

Option 2: Developing precautionary approaches

Trying to avoid the risk – or at least the occurrence of any of its irreversible consequences – can represent a valuable management option in cases where the risk evaluation results in reasoned assumptions of unacceptable consequences. Strictly speaking, risk avoidance consists in circumventing or neglecting the activity that creates the risk. The activity is prohibited or proscribed. For example, insurance companies can exclude the coverage of cybersecurity attacks until they have developed methods to measure the risk.

Precautionary approaches should be chosen on a case-by-case basis, in relation to a desired level of protection against identified potential risks. The European Commission provides recommendations related to factors that

should trigger precautionary measures and guidelines for applying them (European Commission, 2000).

Precautionary approaches should focus on identifying possible courses of action where opportunities exist, but the likely consequences of risk exposure are limited and at least partially reversible. Obviously, this subtle balance cannot be maintained endlessly and it is important to identify the point at which more decisive actions are needed. This does not mean, however, that the organisation should adopt a wait-and-see strategy.

In the case of large epistemic uncertainty about an emerging risk, more research and monitoring are necessary. The available lead time [12] allowing, decision-makers must also invest in deepening their knowledge and understanding of the mechanisms described in the scenario before making a final decision. Knowledge gaps can be filled through research, monitoring and early-warning activities.

Box 7: Adaptive licensing in pharmaceutical regulation

Market authorisation for new drugs is a decision process constrained by the need to accelerate the deployment of potentially more effective therapies, while protecting patients from residual uncertainties about side effects. Several scandals (for example, Mediator in France (2009), Desplex in the United States (1970), human growth hormones) have demonstrated the catastrophic effects of delayed consequences that had not been considered or had been overlooked during the licensing procedure. Consequently, the yes/no authorisation process has largely proven ineffective in preventing the commercialisation of dangerous drugs or in withdrawing them quickly from the market.

In 2014, the European Medicines Agency launched a pilot project on Adaptive Licensing based on a life-cycle vision of the product. Instead of a full authorisation or a ban, a staggered authorisation process was put in place, starting from a limited process and moving to a progressively extended indication of use documentation system as more evidence and knowledge became available. At each stage of the authorisation process, the main concern lays with balancing the trade-off between expected benefits and the requirement to avoid any irreversible harm.

Option 3: Reducing vulnerability

If the organisation cannot (or finds it difficult to) identify any opportunity to act upon the sequence of events leading to a risk, or if the intervention is considered inappropriate or too costly, a reduction in the exposure, or an effort to decrease vulnerability to the risk agent can be a strategic option. Two possibilities can be considered:

- In the case of emerging but well identified risks, it is possible to reduce sensitivity to the risk by developing redundancies, improving personnel training or readjusting protection capabilities.
- In the case of unexpected events, building resilience may be an appropriate strategy. This implies considering worst-case scenarios to ensure that organisations will be able to withstand unexpected shocks, rebound to a desired equilibrium while adapting to the changed context and, in general, recover from any levels of stress while preserving operational continuity. Decentralising decisions, enabling self-organisation and social networking,

---

[12] Before the risk has an impact on the organisation in a significant way.

and promoting diversity are examples of approaches that promote resilience development (OECD, 2014). A draft framework proposed by the World Economic Forum defines resilience characteristics as: robustness (referring to the "ability to absorb and withstand disturbances and crises"), redundancy (involving "having excess capacity and back-up systems"), and resourcefulness (meaning the "ability to adapt to crises, respond flexibly and – if possible – transform a negative impact into a positive"). Other components of resilience include performance, defined as a combination of response ("ability to mobilise quickly in the face of crises") and recovery ("ability to regain a degree of normality after a crisis or event") (WEF, 2013).

Box 8: Walmart's supply chain logistics resilient to disruptions caused by Hurricane Katrina

The response to Hurricane Katrina that hit the Gulf of Mexico and the city of New Orleans in 2005 is often used as an example of organisational failure to anticipate and react to major disruptive events. However, Hurricane Katrina also revealed some successful strategies based on improving resilience to cope with unforeseen events. Walmart stores were able to provide food and water to the most impacted areas of New Orleans much faster than the US Federal Emergency Management Authority. In the three weeks following Katrina's landfall, Walmart shipped 2,500 truckloads of merchandise and made additional drivers and trucks available for community members and organisations wishing to help (Horwitz, 2009).

The following factors explain the resilience of the logistics chain put in place by Walmart:

Capacity building
- A dedicated business continuity unit, staffed by six to ten employees, was already routinely operating in 2005. In case of major events, the team was expandable to 60 people, including senior representatives from each of the company's functional areas.
- The company used its own hurricane tracker software and had contracts with private forecasters to obtain reliable and updated information in a timely manner.

Decentralisation
- Walmart's senior management gave district and store managers enough discretion to make decisions based on local information and immediate needs without requiring pre-approval. For example, a store manager who was no longer

able to contact his superiors decided to run a bulldozer through the store ruins to recover all products that had not been damaged by the water and make them available to residents. After the crisis had been abated, local decision-makers were praised by senior management for their actions.

Protocols and preparation
- Protocols to deal with major disruptive events were already in place, allowing the organisation to adapt decision-making to the evolution of the risk level. For instance, the number of personnel who were part of the command centre was gradually augmented as the risk increased. Two days before the landfall, 50 staff members had joined the team.
- As uncertainties regarding the areas that would be heavily damaged became more tractable, the decision was made to move emergency supplies, such as generators, from the current warehouse location to "designated staging areas so that the stores would be able to open quickly" (Zimmerman & Bauerlein, 2005). Those staging areas were set up outside the areas most likely to be hit the worst, to facilitate quick response with minimal danger (Horwitz, 2009).

The benefit Walmart derived from this kind of preparation obviously goes beyond what could be quantified in monetary terms.

"The only lifeline in Kenner was the Walmart stores. We didn't have looting on a mass scale because Walmart showed up with food and water so our people could survive". Philip Capitano, Mayor of New Orleans, 2005.

Option 4: Modifying the organisation's risk appetite in line with a new risk

The 2008 financial crisis revealed a significant imbalance between the risks some financial institutions were willing to take (risk appetite) and their risk-taking capacities (the maximum amount of risk an organisation can sustain, or its tolerance to risk) (Barfield, 2007).

Dealing with emerging risks requires that organisations constantly align their risk appetite to changes in their environment and the availability of new knowledge and, most importantly, to their resources and capabilities to tolerate or cope with potential risk losses. Such alignment can either be made by reducing the level of risk underwritten, according to one or several of the three options described above, or by increasing the tolerance for risk. In this fourth option, decision-makers do not act on the risk itself or its source. Instead, they choose to adapt their coping strategies to the levels of risk that are observed or anticipated. They retain the risk, accepting the potential loss, by setting aside funds to compensate for a potential future loss.

This option may appeal to decision makers in various contexts; for instance, when high value opportunities are expected or when they choose to differentiate themselves from their market competitors. In general, risk taking is a source of creative innovation, whether technological or social. Risk can yield rewards; accordingly, reducing opportunities for informed risk taking by companies, governments or the public might also depress opportunities for innovation, even in the public sector (OECD, 2010).

The 2014 UK government chief scientific adviser's annual report emphasises that innovation is key for growth, well-being, security and resilience. Hence, one of the hardest decisions for governments is to balance risk taking that accompanies innovation with risk avoidance, prevention and management. This challenge arises, for example, in governmental legislation and regulation of new or emerging technologies. The report cites the UK Human Fertilisation and Embryology Authority that regulates the application of embryology

Box 9: Risk sharing in drug licensing

The drug licensing equation is based on key aspects, including innocuousness, safety, efficacy and cost efficiency, which translate into fostering rapid access to innovative treatments for patients, avoiding negative side effects or risk transfers, and optimising resource allocation through the careful evaluation of treatment efficiency. A poor performance on any of these variables represents important risks for patients, licensing authorities and pharmaceutical companies.

Varying stakeholder groups (patients, companies, regulators) express different risk appetites, and a balance of interests must be achieved with regard to these aspects. The risk appetite might be higher for populations confronted with entirely unmet medical needs (for example those affected by a deadly virus such as Ebola) than for those disposing of treatments although they might wish them to be more efficient. For pharmaceutical companies, it may also depend on the need to develop or update their portfolio of molecules according to market evolutions.

To manage this difficult equation and allow both licensing authorities and pharmaceutical companies to increase their risk appetite to benefit from new opportunities, risk-sharing agreements may offer interesting prospects. Based on conditional approval mechanism, risk-sharing aims to redistribute risks between treatment users and suppliers. The two risk-sharing approaches are finance-based and outcome-based (OECD, 2013).

- Outcome-based schemes make pharmaceutical companies' retribution conditional on treatment performance. If the treatment does not prove effective, the supplier will be asked to refund treatment costs; otherwise, authorisation will be extended and the supplier will collect the benefits accruing.
- Finance-based schemes rely on a predefined mechanism of cost sharing between the supplier and health authorities. For instance, PFIZER offers the first cycle of treatment for its kidney cancer drug Sutent® to UK National Health Service patients.

Risk sharing may be a successful mechanism for pharmaceutical companies to balance the poor performance of some molecules under development in a wider portfolio by the better performance of more successful ones. This strategy allows regulators and companies to increase their risk appetite, thus rewarding research and innovation.

research to reproductive and regenerative medicine, a field where many promising opportunities conflict with potential, yet unknown risks (UK Government Office for Science, 2014).

Option 5: Using "conventional" risk governance instruments to manage familiar risks

When familiar risks evolve in new or changing contexts, it is reasonable to consider and adopt risk management options used for the governance of familiar (as opposed to emerging) risks. The greatest challenge when dealing with this kind of risk is organisational awareness of the contextual evolution. Using conventional risk governance mechanisms would be relevant when, for example, malaria spreads to higher latitudes and altitudes due to climate change (see Box 10) as it is a familiar risk developing in new conditions.

The IRGC risk governance framework (Figure 8) provides a holistic and comprehensive approach to familiar risks. It is suitable for risks marked by complexity, uncertainty and ambiguity, and in particular for risks labelled as *systemic* (OECD, 2003). One important aspect of the framework is the acknowledgment that there may be a gap between how people perceive risk and how experts assess it. This is often particularly relevant for risks with which people and organisations are unfamiliar.

Figure 8: IRGC risk governance framework

(Source: IRGC, 2005)
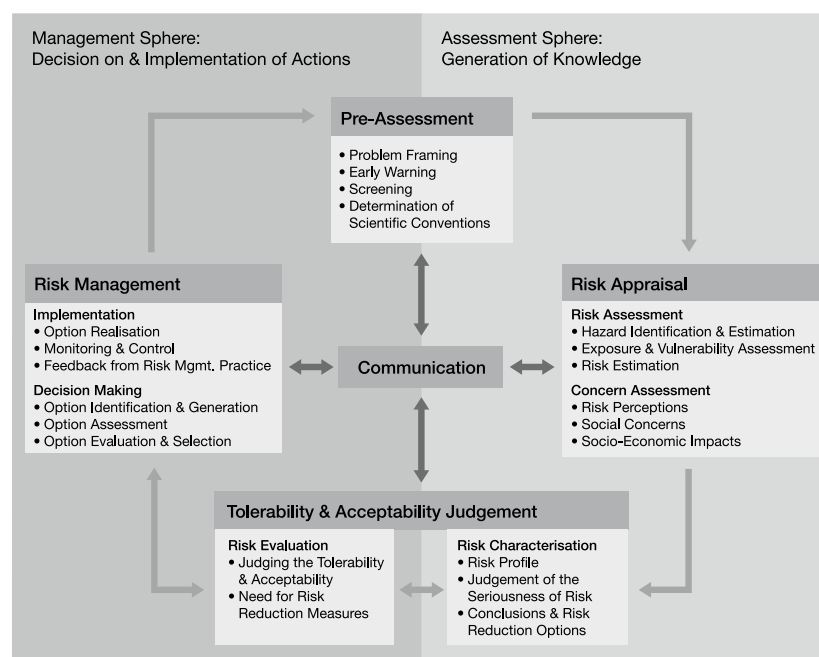
If risk assessment provides a tangible and (if possible) quantifiable outcome, it becomes possible to choose specific management options, such as risk reduction mechanisms, that reduce the probability of occurrence and severity of a risk event's impact (codes and standards, self-regulation, enforcement and compliance). Risk transfer mechanisms are also worth considering, as in compulsory or voluntary insurance schemes, or transfer to financial markets (for example via the emission of bonds).

<div style="background:#e0f0f5">

Box 10: Warmer temperatures push malaria to new altitudes

Infectious diseases in general, and malaria in particular, are sensitive to climatic conditions. Pascual, et al. (2006) have already observed that warmer years aggravate malaria epidemics in the highlands of Africa and South America. In addition to general temperature fluctuations, global warming is expected to affect various parameters that influence the spread of malaria: rainfall (IPCC, 2001), ultraviolet intensity and rising sea levels (Lipp, Huq, & Colwell, 2002). Consequently, in the coming years the disease may affect high altitude populations usually protected from malaria because of low temperatures.

Although protocols for preventing and treating malaria are well known, it will be necessary to ensure that the risk management tools developed elsewhere can be transferred to the new areas and newly exposed populations and that adequate organisational capabilities are put in place.

</div>

Option 6: Doing nothing

If, at the end of Step 2, the conductor concludes that the possible evolution of a certain potential threat (identified in Step 1) will not pose a risk to the organisation, he / she can propose to do nothing. This means that the threat is not considered plausible enough, or its impact important enough, to trigger any action at that time. This does not prevent the organisation from continuing the monitoring process, as the situation may change over time.

All the strategic options described above must be accompanied by continuous monitoring and the analysis of changes in the organisation's external and internal environments, and decisions must be revised accordingly. This is further discussed in Step 5.

Evaluating the strategic options

The evaluation of strategic options depends primarily on:

1. *The state of development of the emerging risk and the level of knowledge about it*
   When little is known about the threat but it potentially has severe negative consequences, precaution-based and resilience-focused strategies can ensure the reversibility of critical decisions and increase the system's coping capacity so it can withstand shocks or adapt to new contextual conditions. A case in point are new materials (such as nanomaterials) with potentially unknown effects. But when a well-known risk develops in new contexts, increasing the risk appetite or considering risk management instruments used for familiar risks is advisable.

2. *The set of evaluation criteria that the decision-makers will choose to adopt*
   - Effectiveness: To what extent does the selected option achieve satisfactory performance in accordance with the decision-makers' expectations?
   - Efficiency: Does the selected option provide satisfactory performance at a minimum cost?
   - Sustainability: How does the option perform in economic, ecological and social terms?
   - Sociopolitical acceptability: How does the option address issues of equity or distribution of costs and benefits among stakeholders?
   - Ethical standards: Is corporate responsibility enhanced? To what extent is the distribution of benefits and risks considered fair?

Having generated and evaluated possible options, decision-makers will select the strategy (including the combination of options) they consider most adapted to their organisation's needs and culture.

Making robust decisions

When dealing with uncertainties, decision science distinguishes between contexts where probability distributions – either derived by frequencies or Bayesian judgments or by intelligent guessing – are available and where they are not.

When probability distributions are available from past experiences or reliable models, the Maximizing Expected Utility Theory (von Neumann & Morgenstern, 1947; Savage, 1954) is the dominant paradigm. It asserts that rational decision-makers should adopt the decision that optimises the combination of probability and consequences, the latter being modelled through utility functions. This includes when subjective probabilities are obtainable and experts do not dispute these probability judgments.

When there are no reliable probability distributions for the various possible futures and when scenario outcomes are highly sensitive to changing hypotheses, the terms severe or deep uncertainty are used (Ben-Haim, 2001; Lempert et al., 2006). Optimisation does not mean much when the consequences of a course of action are uncertain. In such contexts, looking for optimisation may be futile and even dangerous as the gain expected from selecting one option for a given scenario may turn into a loss if another scenario materialises. Decision scientists have developed other methods to deal with this type of uncertainty; one relies on simple criteria reflecting decision-makers' attitudes towards risks. For instance, maximising minimum payoffs (MaxMin) or maximising maximum payoffs (MaxMax) are decision criteria respectively reflecting pessimistic and optimistic visions of the future when dealing with deep uncertainties.

However, these methods may prove to be too simplistic to deal with long-term and complex emerging issues, where objective probabilities are not available. The **concept of robustness** in decision-making, defined as the ability of decisions to display good enough – though not optimal – performances for various possible futures, may be more useful. Robustness in decision-making reflects the willingness of decision-makers to abandon the advantages of optimisation to gain a higher ability to cope with subjective probabilities (that are revised in light of new information) and generally uncertain futures (Rosenhead, Elton, & Gupta, 1972; Schoemaker, 1995; Lempert et al., 2006). Robust methods are most useful when reliable statistical data or unambiguous and convincing subjective estimates for probabilities cannot be obtained.

Developing robust and effective processes for guiding decision-making can be achieved by various means. At the core of these different operational approaches and mathematical models, lies the idea that decision-making should be less about planning and acting and more about continuously planning and adapting to situations (Rosenhead, Elton, & Gupta, 1972)[13]. In the field of climate change, the response to climate-related risks depends on improvements in scientific assessment as well as on the capability of risk managers to revise their decisions when new knowledge becomes available

---

[13] See Appendix 2.5 for an illustration of this idea and the description of practical approaches for applying robustness to strategic decision-making.

(IPCC, 2014). Decision-making in the face of emerging risk similarly requires iterative risk management in order to foster effective adaptation. This is also important for familiar risks, but the more one expects uncertain outcomes, the more flexibility and adaptive capacity are needed to deal with variations in outcome or even surprises.

Criteria for making good decisions under conditions of uncertainty include:

- *Consistency* and procedural rationality, emphasising the importance of established, transparent and applied procedures, that are specific but can also be harmonised across organisations
- Use of all available information, considering *subjective* probability and / or reliability
- *Acceptability*, which may require participatory processes so decisions can be shared between the authority in charge and those who provided inputs during the decision making process
- A *judgment* made by the decision-maker on the extent to which his / her possible error is likely to undermine economic performance, his / her reputation and, overall, the benefits of his / her decision.

Timing of actions

Intervention points must be defined in advance, according to the possible development of the emerging risk. This can be the case when new knowledge is available or when the political agenda changes, as a result of or resulting in a change in perception and concern about the risk. When quick responses are needed, it is extremely useful to have prepared response options that address the real cause(s) of the problem and not just solutions that tackle the surface level symptoms.

A methodological note on robust decision-making is provided in Appendix 2.5.

STEP 4

IMPLEMENT STRATEGY

KEY OBJECTIVE: IMPLEMENT STRATEGY

Step 4 deals with **implementing strategy options** decided in Step 3.
Creating supportive conditions for the organisational, technical and cultural shifts required for the effective deployment of risk management options is crucial.

REQUIRED ACTIONS ›››››››››››››››››››››

- Put in place the **internal and external communication capacities** required for a common understanding of the objectives and the rationale behind them.
- **Allocate resources** to match operational capabilities with strategic orientations.
- **Clearly define roles, responsibilities and incentives** according to the strategic options adopted.
- Support strategy implementation by **ensuring adequate authority** in all phases and enabling the creation of appropriate risk cultures.

EXPECTED OUTCOMES

- Translation of the strategic objectives into individual and collective objectives at the various levels of the organisation.
- **Implementation** of the decisions made in Step 3.

KEY PARTICIPANTS & RESPONSIBILITIES

Strategic decision-makers .... endorse the responsibility of implementing the strategy; appoint a
(e.g. chief risk officer) dedicated team.

Risk owner (if any) .... effectively manages the risk and opportunity for which he / she is responsible, and is rewarded accordingly.

Other relevant stakeholders .... translate the strategic decisions into concrete actions.

Emerging risk conductor .... provides complementary knowledge or expertise regarding the risks and opportunities considered.

KEY SUCCESS FACTORS 〉

- Transparency through effective and continuous communication about the strategic objectives and decisions at all levels of the organisation
- Including relevant stakeholders for the evaluation of the strategy relevance and effectiveness, and timely reaction to resolve conflicts and trade-offs
- Continuous monitoring through the early detection of difficulties and conflicts (with bottom-up reporting)
- Continuous interactions with the emerging risk conductor to re-evaluate the relevance of the strategy in light of new signals and knowledge, if necessary

What to do and how
—

At the end of Step 3, strategies for dealing with emerging risk have been designed and decisions have been made. Although relevant strategies are sometimes difficult to conceive, they can be even more difficult to apply (Noble, 1999a; Hrebiniak, 2006). A summary of the interventions required to transform strategy into action for each of the six strategic options presented in Step 3 follows. Supportive conditions for strategy implementation are described in Appendix 2.6 and include: how the organisation's internal and external communications are organised; the allocation of resources; the roles, responsibilities and rewards in place; and the appropriate leadership and culture needed. These conditions contribute to organisational change and to the success of the chosen strategy.

Option 1: Acting on the factors that contribute to risk emergence or amplification

Option 1 involves clearly communicating, both internally and externally, the link between the contributing factors and the emerging threats and opportunities. Working early to manage the controllable factors and establishing a bottom-up feedback system will benefit the organisation and should be communicated internally, while external stakeholders should be prompted to help deal with the contributing factors. The organisation must assess the resources required to control the factors and define a clear role for itself, comparing it to that of other organisations also able to contribute to controlling certain factors. Besides setting metrics to monitor the situation, the organisation's leadership should provide momentum and vision, set priorities, and assign risk ownership, rewards and incentives. Continuous monitoring and analysis of changes in the organisation's external and internal environment will help determine if decisions need to be revised accordingly.

Option 2: Developing precautionary approaches

In adopting Option 2, the organisation must explain internally the relevant conditions and justification for developing the precautionary approach to the risks. To reinforce internal support for this option, bottom-up feedback loops should be established. Externally, exchanging information with other organisations affected by the same emerging risk will help, as will identifying partnerships (e.g. research, monitoring) that can reduce uncertainties. Translating the precautionary approach into objectives and practices at the various decision-making levels will require allocating appropriate resources; assigning or reviewing risk ownership, rewards and incentives; making any required trade-offs; and setting metrics to monitor the situation. The organisation's leadership must resolve any conflicts and ensure coherence and fairness in the process throughout the operational units. The organisation must also analyse changes in its external and internal environment in the event decisions need to be revised as a consequence.

Option 3: Reducing vulnerability

For Option 3, the organisation must work at the right decision levels internally to communicate emerging risk vulnerabilities and solicit employees for relevant inputs, particularly about any unaddressed weaknesses. Externally, it should evaluate supply-chain partners' resilience (given their links to suppliers and customers), and communicate emerging risk strategies to those potentially affected by the same risks. Demonstrating a reliable safety performance can benefit the organisation and serve as a competitive advantage. The skills required for planned actions to reduce vulnerability must be assessed, and a risk manager should be identified and budgets allocated, all the while ensuring cost effectiveness. Implementation should include metrics, as well as rewards and incentives for success. The leadership must resolve any conflicts throughout, and ensure fairness and coherence of practices across the operational units. The organisation must continuously monitor and analyse changes in its external and internal environment in the event decisions need to be revised accordingly.

**Option 4: Modifying the organisation's risk appetite
in line with a new risk**

Option 4 is driven by an evaluation of the organisation's tolerance to an emerging risk. When the decision is to increase the risk appetite (and retain the risk), the organisation needs to communicate internally about the limits of such an increase and its everyday consequences. Externally, the organisation must explain the rationale for its decision while making sure it preserves its reputation. It must also monitor other stakeholders' strategies. Resources are required for the latter, and to make provisions for additional losses. A risk owner should be identified, and incentives and rewards adapted to the risk-taking strategy. The leadership must resolve any conflicts and support the process by ensuring coherence and fairness of practices across the operational units. The organisation must continuously monitor developments and analyse changes in its external and internal environment in the event decisions need to be revised as a result.

**Option 5: Using "conventional" risk governance instruments
to manage familiar risks**

Case 1 – When an organisation has no existing risk governance framework:

The organisation must explain the need for such a framework and, subsequently, ensure its personnel knows about the one used and its implications for everyday activities. Externally, the organisation should encourage the development of dedicated regulation; regularly inform regulatory bodies, business partners and local communities about its efforts; and share experiences with organisations dealing with the same risk. Budgets for these activities need to be allocated, and the required capacities for implementing them developed.

Case 2 – When an organisation extends an existing risk management framework to a new risk:

As expanding an existing framework may be perceived as inaction or management's lack of situational awareness, internal and external communication are needed to express the organisation's cognisance of the threat or opportunity and, when necessary, to explain the rationale for its strategy. Additional resources may be needed for a risk assessment and evaluation, as well as for the management and communication strategy.

In both cases:

The organisation must assign risk ownership if the risk is established and sufficient knowledge exists to implement a conventional risk management framework. After clear responsibilities in the framework are assigned, operational tasks can be translated to employees, with associated incentives and rewards. No major changes in the organisation's leadership and culture are foreseen. However, the organisation must continuously monitor and analyse changes in its external and internal environment in the event decisions need to be revised as a consequence.

Option 6: Doing nothing

Because inaction may be perceived as management's lack of awareness or misinterpretation of an emerging risk's severity, the organisation's internal and external communication for Option 6 must show that it recognises the threat or opportunity and can explain its rationale behind the chosen strategy to do nothing. While the organisation needs to identify resources required for continuous monitoring, no adjustments to roles, responsibilities or the reward system, or major changes to the leadership or culture are required. However, it must analyse changes in its external and internal environment in the event decisions need to be revised accordingly.

Appendix 2.6 provides details and examples on the different interventions suggested to convert the six strategies into concrete actions.

STEP 5

REVIEW RISK DEVELOPMENT AND DECISIONS

KEY OBJECTIVE: REVIEW AND UPDATE THE STRATEGY

Step 5 serves to:
- **Monitor** how emerging risks and opportunities unfold.
- **Review** the relevance and performance of the decisions made.
- If needed, **update** the strategy.

It must thus:
- Demonstrate whether the organisation is dealing effectively with the opportunities and risks that emerge from changing and evolving internal or external contexts.
- Provide valuable information to Steps 1, 2 and 3 of the process.
- Provide insights on the strengths and weaknesses of the guidelines (reflexive process).

REQUIRED ACTIONS 〉〉〉〉〉〉〉〉〉〉〉〉〉〉〉〉〉〉〉〉〉〉〉〉〉

- **Deploy monitoring capabilities** for the decision options described in Step 3.
- **Create the interaction space** required for the conductor and other users of the guidelines to exchange and communicate. This will help to gain reflexivity on the strengths and weaknesses of the arrangements put in place in the earlier steps.
- **Establish bridges with risk management standards** or professional organisations, which may help confer legitimacy on how the emerging risk governance process is applied in the organisation.

EXPECTED OUTCOMES

- Risks and opportunities can either be **decommissioned**, or become **accepted** or sufficiently **well known** for familiar risk management measures to be employed.
- Risks and opportunities outside of these options must remain the subject of careful and continuous monitoring, analysis and revision.

KEY PARTICIPANTS & RESPONSIBILITIES

Senior managers........................ review decisions about the organisation's emerging risk management, i.e. the design and implementation of internal structures and processes.

Business managers.................... deploy the adopted risk management strategies.

Emerging risk conductor.......... creates interaction space for reflection and confidence.

KEY SUCCESS FACTORS 〉

- Involvement of all internal stakeholders
- Open and transparent discussions
- Regular updates of strategic decisions based on new information

What to do and how
—

No important emerging risk or opportunity must go unnoticed. The last phase of the process will thus review:

- *Timeliness*: Was the organisation able to identify all emerging risks at an early stage?
- *Avoidance of loss*: To what extent were negative impacts on the organisation's business and reputation avoided?
- *Risk mitigation* (for each emerging risk identified in Step 1): Was the risk eliminated, or was sufficient knowledge developed so that it can be managed using frameworks and instruments for familiar, established risks (for example standards and norms, regulation, and risk transfer to financial or insurance markets)?
- *Competition*: How did the organisation deal with the emerging risk in comparison to its peers or competitors?

Monitoring the consequences of decisions and reviewing them systematically is a key element in any governance process. In the case of guidelines for emerging risk governance, monitoring and reviewing the management process and its outcomes become even more crucial as the guidelines are expected to provide the organisation with proactive capabilities. By pursuing a pathway of adaptive management, the organisation learns one step at a time how to implement decisions and to monitor their intended and unintended consequences.

Box 11: Risk decision review process in familiar risk governance

As new conditions develop or new knowledge is generated, most risk management frameworks explicitly state that risk management decisions should be reviewed.

The ISO 31000 (2009) principles for risk management, for example, state: "Monitoring and review of the framework is important to ensure that risk management is effective and continues to support organisational performance. Organisations should: establish performance measures, periodically measure progress against, and deviation from the risk management plan, periodically review whether the risk management framework, policy and plan are still appropriate given the organisations' internal and external context, report on risks, progress with the risk management plan and ensure how well the risk management policy is being followed, and review the effectiveness of the risk management framework. Organisations should also engage in continual improvement of the framework. Based on the review, decisions should be made on how the risk management framework, policy and plan can be improved. These decisions should lead to improvements in the organisation's risk management, and risk management culture."

The IRGC risk governance framework also stresses the importance of systematically monitoring the effects of decisions once they are implemented: "The monitoring system should be designed to assess intended as well as unintended consequences. Often a formal policy assessment study is issued in order to explore the consequences of a given set of risk management measures on different dimensions of what people value. In addition to generating feedback for the effectiveness of the options taken to reduce the risks, the monitoring phase should also provide new information on early-warning signals for both new risks and old risks viewed from a new perspective. It is advisable to have the institutions performing the risk and concern assessments participate in monitoring and supervision so that their analytic skills and experience can be utilised in evaluating the performance of the selected management options" (IRGC, 2005, p. 43).

irgc

Insights gained from the reviewing and monitoring process benefit the organisation in multiple ways:

- Decisions that prove to be effective can provide transferable lessons, whereas decisions that perform poorly create opportunities for improvement.
- The conductor may rely on an established, routine review process and the constant monitoring of decisions.
- Reviews and monitoring can provide valuable input into Step 1 by revising the list of signals, and into Step 2 by suggesting when updating the scenarios is necessary.

The best way to achieve the objectives is to embed "routine ERG" into the organisation's processes and annual programme. The "corporate calendar" provides opportunities for the conductor to provide information on the ERG, much in the same way that corporations have annual shareholder meetings to review the year's performance and provide direction for the coming year. Just as important as an annual (or more frequent) review opportunity is the establishment of a space for internal dialogue on emerging risk. Swiss Re, for example, uses SONAR (Systematic Observation of Notions Associated with Risks), their in-house mechanism, to gather information employees believe is relevant for the identification of emerging risks (see Appendix 1.3).

In practical terms, the emerging risk conductor should organise regular reviews to determine how each of the guidelines' previous phases was conducted. These reviews serve to identify whether additional open and contextual (Step 1) or targeted (Step 2) foresight exercises are needed and to review management decisions (Step 3) and their implementation (Step 4).

Deploying monitoring capabilities

1. What needs to be monitored?

The following two aspects should be monitored in parallel:

- **Relevance of the hypotheses and the outcome of Steps 1 and 2**
  Do they need to be revised and, if so, must the strategic decisions made on their basis be adjusted as well? This initial monitoring focuses on the way threats and opportunities are effectively unfolding as opposed to what was assumed. It implies monitoring the consequences of the contributing factors, tipping points and thresholds identified in the scenarios. Clearly identifying the thresholds of, for example, acceptability or irreversibility is particularly important for emerging issues.
- **Effectiveness of the decisions made in Step 3**
  As long as the identified uncertainties and hypotheses formulated in Steps 1 and 2 remain unchanged, the monitoring should focus on the strategies' ability to perform adequately based on this information.

2. What does the monitoring involve?

Organisations need to select appropriate metrics and:

- Consider the complexity of the phenomena to be monitored so the metrics are not too simplistic.
- Ensure that the metrics are cost effective and adapted to the availability of the data.
- Favour leading indicators that provide insights on future evolutions over lagging indicators that reflect past behaviours.

3. How must the monitoring output be analysed and communicated?

The knowledge collected through monitoring must be analysed and made available to the decision-makers. It is the conductor's responsibility to ensure that Steps 1 and 2 include an updated evaluation of how risks and opportunities are actually evolving. On the other hand, the decision-makers who decided on the strategy must carefully follow the effectiveness of their approaches, preferably by combining different metrics and sources for greater reliability.

Engaging in a reflexive process

For the guidelines to be considered legitimate and effective by internal and external stakeholders, the conductor must demonstrate their validity and update the practices in view of environmental changes and new information. Both substantive and procedural validity are required.

Substantive validation is based on evaluating outcomes by comparing them with reality in terms of avoided losses (which is only possible ex post). This form of validation is not always possible as outcomes may be visible only after a long period or may not be visible at all.

Procedural validation is based on assessing the quality of the process that led to the outcomes. The scientific validity of the approaches used, regularly updated data and hypotheses, and openness and transparency are examples of the criteria used for procedural validation.

The conductor can assess the guidelines' relevance and effectiveness through a substantive evaluation based on a number of suggested criteria for each of the previous phases. The number of criteria may be restricted depending on the organisation's culture and practices.

irgc

3.

CONDITIONS
FOR SUCCESS

Even when well designed and structured, management frameworks can fail to reach their objectives. Several factors may lie behind this failure, including a lack of motivation on the part of staff, poor communication, a reluctance to change or the unavailability of resources.

Organisations must provide a supportive environment for the process that goes beyond the careful implementation of each of the steps described earlier and the availability of technical support. Many of the components of such an environment have been discussed already. They include ensuring support from the strategic decision-making level, appointing a conductor to facilitate the process, and adapting incentives and rewards to encourage emerging risk recognition.

3.1 Insights from emerging risk management in organisations

While developing the guidelines for ERG described in this report, IRGC interviewed various organisations with experience developing and implementing dedicated systems or processes for ERG. These insights highlight additional challenges and best practices related to the role of emerging risk conductors:

- **The representation of a potential change or threat as a risk to an organisation or population may have important strategic consequences.** Often manifest as cognitive biases, organisations may show inertia and reluctance to change because of vested (economic or political) interests (Hodgkinson, 2012). Counter-incentives and inappropriate or lacking incentives may deter middle managers from recognising, reporting and addressing new risks. The health impact of asbestos, for instance, was suspected for centuries before being formally recognised as a health risk only in the 19th century in the UK. Its use was first regulated in the 1970s, amid highly controversial political, economic, legal and public considerations. In many areas of risk governance, stakeholders attempt to avoid accountability by not seeking credible information on emerging risk. For instance, certain food manufacturers in the US have opposed National Institute of Health funding for research on the adverse

effects of trans fats (a type of unsaturated fat used for frying or as an ingredient in processed foods that can lead to high cholesterol levels).

Keen political, societal and media interest in high profile issues can seriously deter decision-makers from framing certain issues as risks. Conversely, some emerging risks begin to draw attention only when they are framed as public challenges (Borraz, 2007). Risk governance does not happen in a vacuum; it is not neutral. It represents problems in ways that may privilege particular views and therefore prioritise certain decisions based on subjective criteria.

- **Innovation management and emerging risk management are interlinked, even in the public sector.**
  Innovation management is an important activity in industry to develop opportunities from new technologies. ERG can also be used to identify latent or future opportunities that may become competitive advantages for organisations. For example, in internal processes for emerging risk management developed by insurance companies, specific attention is given to business opportunities arising from new risks (see Appendices 1.3 and 2.2).

  In their role as facilitators of technological innovation, governments must consider the significant social and cultural impacts of new technologies (revealed by social science research) before deciding how, if and when to take one forward (despite the fact that it could generate new risks), or what controls to put in place. Broader deliberation with stakeholders in the public sector can be coordinated by the emerging risk conductor.

- **An ERG process needs to demonstrate that it is effective and worth the investment.**
  Like any process, ERG must provide a tangible output that is of value to the organisation. Quantitative frameworks, especially those based on or providing monetary value, for instance by assessing the relevance of risk governance strategies or policies, are of limited use in the case of emerging risk, because of high uncertainties and the lack of quantitative data. Furthermore, the benefits of emerging risk management processes may not be apparent before a long lapse of time as the time horizons considered may be over several years. Finally, the processes' outputs are only one of several aspects considered by decision-makers, making it difficult to trace back their merits and limits. Overall, engaging in ERG is expected to contribute to creating an internal risk culture appropriate for strategic planning and adaptation to change, as outlined in the introduction.

- **People in charge of identifying and assessing emerging risks must continuously communicate with decision-makers and risk owners.**
  Integrating an identified threat in the risk portfolio is the outcome of an iterative and gradual process during which, under the responsibility of the emerging risk conductor, decision-makers progressively become familiar with the potential new risk, until they identify it formally as an emerging risk with which the organisation must deal, using formal response strategies.

- **The emerging risk conductor must not be a "prophet of doom".**
  The emerging risk conductor can communicate good news in various ways. First, he/she can stress the fact that the process can also help to identify emerging opportunities that may develop as a result of new conditions or new technologies. The Kodak example and the development of digital technology in photography illustrates this well (see Box 2). Another way for the emerging risk conductor to convey a positive message is to announce when an emerging risk has been taken off the list of potential risks to the organisation (or "decommissioned"), following the successful deployment of the process. Finally, a positive message may simply consist in communicating the results of careful scientific examination. This can contribute to de-emphasising and objectivising the political or public controversies surrounding so-called "problems" backed by limited or weak scientific evidence. Social science research and monitoring can help to identify concerns and potential conflicts ahead of their actual occurrence.

In addition to these lessons from experience, organisations should also consider the following complementary crosscutting requirements: communication, tolerance to failure, understanding cognitive aspects and the need for leadership and trust.

3.2 Communication
—

As seen in Step 4, internal and external communication is central to the success of strategy implementation. At a broader level, the role of communication is to:

- Support ERG by creating the required interactions between stakeholders, within or outside the organisation.
- Foster a dialogue about the challenge of investing in emerging risk identification and response measures, despite uncertainty about the actual impact and extent of negative consequences to the organisation. The frequently adopted wait-and-see attitude and the tendency to give priority to current risks while neglecting future threats are important barriers to overcome.
- Familiarise decision-makers with the characteristics of emerging risks and with existing strategies to deal with them, for example by illustrating cases of successful emerging risk management.
- Ease the process of continuously reshaping organisational resources and objectives, especially with regard to possible internal resistance.

3.3. Tolerance for failure
—

The concept of *tolerance for failure* refers to the culture in an organisation that allows limited leeway for trial and error. This is often recognised as a feature of organisations that adopt a proactive attitude to change, "learning by doing", and for which it is important not to blame those who try to improve

how things are done, even when they do not succeed. Although tolerance for failure may be hard to apply in some public or politicised agencies or in private sector companies judged on their financial performance, the obstacles can be overcome. Providing free spaces for trial and error learning, when the errors are still manageable and can be contained in time and space is important. If the errors thus surfaced challenge the existence of the organisation or threaten its functionality, the learning process must be shifted into the virtual space where simulations can help to provide learning opportunities without risking fatal errors in the real world.

To illustrate, adopting the funnel-type process described in Step 2 allows dealing with uncertainties and complexities involved in emerging risk identification and assessment, and avoiding the risk of failing to identify an emerging risk or not stopping the exploration and assessment of an emerging risk if it is not relevant to the organisation. Funnel-type processes are designed to find the best compromise between focusing on the most relevant factors and being open to new and even unexpected developments and events. By filtering information and input, it is possible to focus on a limited number of issues, without losing one's sensitivity to complex risk interactions.

Experiences in *innovation management* in particular show that these types of processes generate "waste", i.e. ideas that turn out to be irrelevant for the organisation, before they are seen as management failures. It is very likely that comparable waste generation will be experienced in ERG, and this must be tolerated. It is the conductor's responsibility to ensure that emerging threats not relevant to an organisation are identified as early as possible to minimise resource consumption or reputational damage.

3.4. Understanding cognitive aspects
—

Emerging risk governance is not only challenging at the organisational level, it may also question cognitive patterns underlying individual decisions and behaviours. Exploring and analysing a large set of uncertain and weak signals, going beyond the behaviours of past systems to imagine their future, organising the collection of multi-disciplinary knowledge, and deciding on risks and opportunities that have not yet materialised is a very demanding and often challenging exercise. Potentially powerful cognitive biases need to be overcome. Cognitive biases, such as the tendency to systematically underestimate surprises, to assume that lessons have been learned from the past or to overestimate the ability to make judgments under unpredictable circumstances, can reinforce this propensity. In addition, problems of collective judgment, such as group biases towards cautious or risky shifts, need to be considered. Faced with a choice between a "safe" and "risky" decision, group members appear to lean towards one extreme or the other, relative to the choices each member might have made on their own (Davis & Hinsz, 1982). Both risky and cautious shifts, a phenomenon known as "group polarization", have been identified in the literature.

Careful attention should be paid to ensuring that:

- The conductor and his/her team are trained appropriately and their interventions are adequately framed to reduce biases and the attendant impact of employee morale. Hodgkinson and Healey's (2011, 2014) analysis of psychological issues related to the development of dynamic capabilities in organisations provides relevant insights.
- Participants in the process, including decision-makers at various levels of the organisation, avoid conservatism and think outside the box. Particular consideration should go into ensuring that rewards and incentives are put in place and that the behaviour of individuals implicated in the process is steered in the same direction.
- Professional support and external reviews are encouraged to provide the process with challenging outside views and complementary expertise. As already mentioned in this report, IRGC suggests relying on professional experts in futures studies to facilitate scenario development.

Biases and intuitive heuristics also relate to processing information on risk aspects, such as exposure, probability or uncertainty. Table 1 provides an overview of common biases that individuals often apply to judge risks or to draw inferences from probabilistic information (Festinger, 1957; Kahneman & Tversky, 1979; Kahneman, 2011; Renn, 2008).

Availability	Events that come to people's mind immediately (e.g. events highlighted in the mass media) are rated as more probable than events that are less in their thoughts
Anchoring effect	Probabilities are not adjusted sufficiently to the new information available, being anchored to the perceived significance of the initial information
Representativeness	Single events experienced by people or associated with properties of an event thus experienced are considered more typical than information based on the actual frequencies of those events
Avoidance of cognitive dissonance	Information that challenges perceived probabilities that are already part of a belief system will either be ignored or minimised, in an attempt to attenuate cognitive dissonance.

Table 1: Intuitive biases of risk perception

3.5. Authority and trust

Emerging risks develop in contexts often marked by uncertainty and socio-economic instability. They can represent threats to economic well-being, the provision of critical services or even moral values such as privacy. This goes hand-in-hand with growing distrust in existing institutions, be they governments or large corporations. In consequence, organisations should pay close attention to restoring, building and maintaining trust. Rather than spending resources on conventional risk management methods, such as command-and-control regulatory measures, the emerging risk conductor and leaders in ERG should establish their legitimacy and credibility by proving effective outcomes relying on skills like adaptability, flexibility and creativity.

In 2010, IRGC worked with a number of governments to identify hallmarks and drivers of effective emerging risk governance (IRGC, 2011). Success factors are listed in Box 12.

Box 12: IRGC hallmarks and drivers of effective emerging risk governance

Fostering inter-disciplinarity and multi-sectorial risk management
- Effective inclusion of stakeholders in the assessment and decision-making process
- Integration of the various risks as well as the elements that compose the risks

Establishing an appropriate risk culture
- Development of transparency in government objectives and of means to deal with uncertainty and emerging issues
- Provision of convincing methods and procedures to evaluate threats and to design options to deal with them
- Agility, innovation and creativity to ensure flexibility and adaptability
- Communication to build constructive discussions about risks

Assigning risk ownership ("home") for emerging issues
- Need to ascertain accountability
- Need to prioritise issues among the many uncertainties, potential opportunities and threats

Determining the appropriate timing to act
- Intervention points and timely action

4.

CONCLUSION

Elaborating upon previous work on the contributing factors to risk emergence and on improving the management of emerging risk, the Guidelines for Emerging Risk Governance presented in this report aim to support public and private organisations in dealing proactively with emerging risks. Designing the appropriate internal processes involves the ability to *anticipate risk* (identify, evaluate and prioritise potential threats and opportunities) and *respond to risk* (assess and respond to those threats that may develop into risks to the organisation).

Figure 9: Emerging risk governance at the intersection of various disciplines and theoretical frameworks

Emerging risks tend to develop in complex environments and display high levels of uncertainty. Applying conventional measurement logics is inadequate to address emerging risks and, therefore, frameworks for the governance of familiar risks are often not fully appropriate in these contexts. Furthermore, emerging risks and opportunities are often interrelated, making it equally important for organisations to create conditions for opportunity management as well as for risk management. This improves their capacity to adapt to changing environments as well as their competitive advantage. Ultimately, ERG aims to avoid major failures (for example "the next asbestos") and protect public well-being.

As governing emerging risks is at the intersection of various disciplines and theoretical frameworks, IRGC has integrated expertise from various fields, including risk management, futures studies, innovation management, dynamic capabilities and strategic decision-making.

IRGC will engage in further discussions on the relevance and application of the guidelines by various types of organisations, to continue to refine the process.

GLOSSARY

Complexity: The difficulty of identifying and quantifying causal links between a multitude of potential causal agents and specific observed effects (IRGC, 2005).

Complex system: A system composed of many parts that interact with and adapt to each other (OECD, 2009).

Emerging risk: A new risk, or a familiar risk in a new or unfamiliar context (re-emerging). These risks may also be rapidly changing (in nature). Although they may be perceived as potentially significant, at least by some stakeholders or decision-makers, their probabilities and consequences are not widely understood or appreciated (IRGC, 2010a).

Familiarity: Knowledge and experience with an organism, the intended application or activity and the potential receiving environment. A relatively low degree of familiarity may be compensated for by appropriate management practices. Familiarity can be increased as a result of trial or experiment. This increased familiarity can then form a basis for future risk assessment (UNEP, 1995).

Precautionary approaches: The 1992 Rio Conference on the Environment and Development adopted the Rio Declaration, whose Principle 15 states that: "In order to protect the environment, the precautionary approach shall be widely applied by States according to their capability. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation".

Risk: An uncertain negative consequence of an event or an activity with regard to something that humans value (definition originally in Kates, et al., 1985, p. 21).

Risk appetite: The amount and type of risk that an organisation is prepared to pursue, retain or take (ISO 73, 2009).

Risk assessment: The task of identifying and exploring, preferably in quantified terms, the types, intensities and likelihood of the (normally undesired) consequences related to a risk. Risk assessment comprises hazard identification and estimation, exposure and vulnerability assessment, and risk estimation (IRGC, 2005).

Risk governance: The identification, assessment, management and communication of risks in a broad context. It includes the totality of actors, rules, conventions, processes and mechanisms concerned with how relevant risk information is collected, analysed and communicated, and how and by whom management decisions are taken (IRGC, 2005).

Risk management: The creation and evaluation of options for initiating or changing human activities or (natural or artificial) structures with the objective of increasing the net benefit to human society and preventing harm to humans and what they value; and the implementation of chosen options and the monitoring of their effectiveness (IRGC, 2005).

Risk profile: In the case of a single risk, a profile capturing several dimensions, qualitative and quantitative, that describe the risk in ways useful to a risk manager who is making initial decisions about what should be done. A profile may also describe a set of risks of concern to an organisation.

Risk tolerance: An organisation's or stakeholder's readiness to bear the risk after risk treatment (process to modify the risk) in order to achieve its objectives. (Note: Risk tolerance can be influenced by legal or regulatory requirements) (ISO 73, 2009).

Systemic risks: Risks affecting the systems on which society depends. The term "systemic" was assigned to risk by the OECD in 2003 and denotes the embeddedness of any risk to human health and the environment in a larger context of social, financial and economic consequences and increased inter-dependencies both across risks and between their various backgrounds (IRGC, 2005). Systemic risks are characterised by complexity, uncertainty and ambiguity. Most often, they are also trans-boundary.

Uncertainty: A state of knowledge in which the likelihood of any effect, or the effects themselves, cannot be precisely described. (Note: This is different from ignorance about the effects or their likelihood.) (IRGC, 2005).

REFERENCES

Amanatidou, E., Butter, M., Carabias, V., Konnola, T., Leis, M., Saritas, O., van Rij, V. (2012). On Concepts and Methods in Horizon Scanning: Lessons from Initiating Policy Dialogues on Emerging Issues. *Science and Public Policy*, 39, 208-221.

Anderson, J. (1997). Technology Foresight for Competitive Advantage. *Long Range Planning*, 30(5), 665-677.

Barfield, R. (2007). *Risk Appetite: How Hungry Are You?* London: PricewaterhouseCoopers.

Ben-Haim, Y. (2001). *Info-Gap Decision Theory: Decisions Under Severe Uncertainty*. Oxford: Academic Press.

Börjeson, L., Höjer, M., Dreborg, K.-H., Ekvall, T., & Finnveden, G. (2006). Scenario Types and Techniques: Towards a User's Guide. *Futures*, 38(7), 723-739.

Borraz, O. (2007). Risk and Public Problems. *Journal of Risk Research*, 10(7), 941-957.

BZK (2009) Dutch Ministry of the Interior and Kingdom Relations. Working with Scenarios, *Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands*. Retrieved 11 February 2015, from www.preventionweb.net/files/26422_guidancemethodologynationalsafetyan.pdf.

Cornelissen, J. P. (2006). Making Sense of Theory Construction: Metaphor and Disciplined Imagination. *Organization Studies*, 27(11), 1579-1597.

Davis, J. H., & Hinsz, V. B. (1982). Current Research Problems in Group Performance Group Dynamics. In H. Brandstätter, J. H. Davis, & G. Stocker-Kreichgauer (Eds), *Group Decision Making* (pp. 1-22). London: Academic Press.

Dean Jr., J. W., & Sharfman, M. P. (1993). The Relationship Between Procedural Rationality and Political Behavior in Strategic Decision Making. *Decision Sciences*, 24(6), 1069-1083.

Elbanna, S. (2006). Strategic Decision-making: Process Perspectives. *International Journal of Management Reviews*, 8(1), 1-20.

European Commission. (2000). *Communication from the Commission on the Precautionary Principle (COM 2000)*. Brussels: EC.

Festinger, L. (1957). *A Theory of Cognitive Dissonance*. Stanford: Stanford University Press.

Flage, R., & Aven, T. (2015). *Emerging Risk and Black Swans*. University of Stavanger, Norway. (Working paper, unpublished as of 16 January 2015, available from terje.aven@uis.no).

Gordon, T. J., & Glenn, J. C. (1994). *Environmental Scanning*. AC/UNU Millennium Project.

Healey, M. P., & Hodgkinson, G. P. (2008). Troubling Futures: Scenarios and Scenario Planning for Organizational Decision Making. In G. P. Hodgkinson, & W. H. Starbuck (Eds), *The Oxford Handbook of Organizational Decision Making* (pp. 565-585). Oxford: Oxford University Press.

Helgeson, J., van der Linden, S., & Chabay, I. (2012). The Role of Knowledge, Learning and Mental Models in Public Perceptions of Climate Change Related Risks. In A. E. Wals, & P. B. Corcoran (Eds), *Learning for Sustainability in Times of Accelerating Change* (pp. 329-346). Wageningen: Wageningen Academic Publishers.

Hodgkinson, G.P. (2012). The Politics of Evidence-based Decision Making. In D. M. Rousseau (Ed), *The Oxford Handbook of Evidence-based Management* (pp. 404-419). New York: Oxford University Press.

Hodgkinson, G. P., & Healey, M. P. (2011). Psychological Foundations of Dynamic Capabilities: Reflexion and Reflection in Strategic Management. *Strategic Management Journal*, 32, 1500-1516.

Hodgkinson, G. P., & Healey, M. P. (2014). Coming in from the Cold: The Psychological Foundations of Radical Innovation revisited. *Industrial Marketing Management*, 43, 1306-1313.

Hodgkinson, G. P., & Starbuck, W. H. (2008). Organizational Decision Making: Mapping Terrains on Different Planets. In G. P. Hodgkinson, & W. H. Starbuck (Eds), *The Oxford Handbook of Organizational Decision Making* (pp. 1-29). Oxford: Oxford University Press.

Horwitz, S. (2009). Wal-Mart to the Rescue: Private Enterprise's Response to Hurricane Katrina. *The Independent Review*, 13(4), 511-528.

Hrebiniak, L. G. (2006). Obstacles to Effective Strategy Implementation. *Organizational Dynamics*, 35(1), 12-31.

Ilmola-Sheppard, L. (2014). *Increasing Flexibility by Environment Scanning of the Early Signs of Change in the Complex Environment*. Aalto: Aalto University publication series (doctoral dissertations 60/2014).

IPCC (2001). *Climate Change 2001: Impacts, Adaptations and Vulnerability*. Intergovernmental Panel on Climate Change, Working Group II. Cambridge: Cambridge University Press.

IPCC (2014). *Climate Change 2014: Impacts, Adaptation and Vulnerability*. Intergovernmental Panel on Climate Change, Working Group II. Cambridge: Cambridge University Press.

IRGC (2005). *Risk Governance: Towards an Integrative Approach*. Geneva: International Risk Governance Council.

IRGC (2010a). *The Emergence of Risks: Contributing Factors*. Geneva: International Risk Governance Council.

IRGC (2010b). *Emerging Risks: Sources, Drivers and Governance Issues*. Geneva: International Risk Governance Council.

IRGC (2011). *Improving the Management of Emerging Risks*. Geneva: International Risk Governance Council.

ISO 31000 (2009). *Risk Management - Principles and Guidelines.* Geneva: International Organization for Standardization.

ISO 73 (2009). *Risk Management. Vocabulary. Guidelines for Use in Standards*. Geneva: International Organization for Standardization.

JI, J. (2010). *Strategic Decision-Making Process Characteristics, Confucian Values and Their Effects on International Entry Mode Decisions: A Study of Chinese Private Firms*. University of Glasgow, Department of Management. Glasgow: University of Glasgow.

Johnson, G., Scholes, K., & Whittington, R. (2008). *Exploring Corporate Strategy* (8th ed.). Harlow: Prentice Hall.

Kahn, H., & Wiener, A. J. (1968). *The Year 2000: A Framework for Speculation on the Next Thirty-three Years*. New York: Collier Macmillan.

Kahneman, D. (2011). *Thinking Fast and Slow*. New York: Farrar Straus Giroux.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision Under Risk. *Econometrica*, 47(2), 263.

Kates, R.E., Hohennemser, C. & Kasperson, J. (1985). *Perilous Progress: Managing the Hazards of Technology*. Boulder: Westview Press.

Kosow, H., & Gassner, R. (2008). *Methods of Future and Scenario Analysis: Overview, Assessment and Selection Criteria*. Bonn: German Development Institute.

Lempert, R. J., Groves, D. G., Popper, S. W., & Bankes, S. C. (2006). A General, Analytic Method for Generating Robust Strategies and Narrative Scenarios. *Management Science*, 52(4), 514-528.

Lipp, E. K., Huq, A., & Colwell, R. R. (2002). Effects of Global Climate on Infectious Disease: The Cholera Model. *Clinical Microbiology Review*, 15(4), 757-770.

Mannermaa, M. (1986). Futures Research and Social Decision Making: Alternatives Futures as a Case Study. *Futures*, 18(5), 658-670.

Mintzberg, H. Raisinghani, D., & Theoret, A. (1976). The Structure of "Unstructured" Decision Processes. *Administrative Science Quarterly*, 21(2), 246-275.

Noble, C. H. (1999a). Building the Strategy Implementation Network. *Business Horizons*, 42,19-27.

Noble, C. H. (1999b). The Eclectic Roots of Strategy Implementation Research. *Journal of Business Research*, 45(2), 119-134.

OECD (2003). *Emerging Risk in the 21st Century: An Agenda for Action*. Paris: Organisation for Economic Co-operation and Development.

OECD (2009, September). Global Science Forum. *Report on Applications of Complexity Science for Public Policy: New Tools for Finding Unanticipated Consequences and Unrealized Opportunities*. Paris: Organisation for Economic Co-operation and Development.

OECD (2010). *Risk and Regulatory Policy: Improving the Governance of Risk*. Paris: Organisation for Economic Co-operation and Development.

OECD (2013). *Toward New Models for Innovative Governance of Biomedicine and Health Technologies*. Working Party on Biotechnology. Paris: Organisation for Economic Co-operation and Development.

OECD (2014). *Boosting Resilience Through Innovative Risk Governance*. Paris: Organisation for Economic Co-operation and Development.

Pascual, M., Ahumada, J. A., Chaves, L. F., Rodo, X., & Bouma, M. (2006). Malaria Resurgence in the East African Highlands: Temperature Trends Revisited. *Proceedings of the National Academy of Sciences*, 103(15), 5829–5834.

PBL Netherlands Environmental Assessment Agency. (2013). *Guidance for Uncertainty Assessment and Communication*. The Hague: PBL Dutch Environmental Assessment Agency.

Petersen, A. (2008). *Dealing with Uncertain Technological Risks*. The Hague: Netherlands Environmental Assessment Agency.

Ramirez, R., Selsky, J. W., Roodhart, L., & Manders, W. (2011). How Shell's Domains Link Innovation and Strategy. *Long Range Planning*, 44(4), 250-270.

Rathe, A. A., Lickorish, F., Prpich, G. P., Delgado, J., Shaw, H., Chatterton, J. C., Pollard, S. J. (2013, October). *IEHRF Horizon Scan*. Retrieved 29 December 2014, from Number 36: www.cranfieldfutures.com/wp-content/uploads/2013/10/IEHRF-Horizon-Scan-October-2013.pdf

Renn, O. (Ed.) (2008). *Global Risk Governance: Concept and Practice Using the IRGC Framework*. International Risk Governance Council Bookseries. Netherlands: Springer.

Rohrbeck, R., Arnold, H. M., & Heuer, J. (2007). *Strategic Foresight in Multinational Enterprises: A Case Study on the Deutsche Telekom Laboratories*. Munich: Munich Personal RePEc Archive.

Rosenhead, J., Elton, M., & Gupta, S. K. (1972). Robustness and Optimality as Criteria for Strategic Decision. *Journal of the Operational Research Society*, 23, 413-431.

Rossel, P. (2009). Weak Signals as a Flexible Framing Space for Enhanced Management and Decision making. *Technology Analysis & Strategic Management*, 21(3), 307-320.

Savage, L. J. (1954). *The Foundations of Statistics*. New York: John Wiley & Sons.

Schoemaker, P. J. (1995). Scenario Planning: A Tool for Strategic Thinking. *Sloan Management Review*, 36(2), 25-40.

Schüll, E. & Schröter, W. (2013). Integral WP 3.2 Guideline. Retrieved 2 February 2015, from forestwiki.jrc.ec.europa.eu/integral/index.php/WP_3.2_Guideline.

Spies, P. H. (1991). Formulating the Mess: Environmental Scanning. *Business Futures*, 19-24.

Taleb, N. (2007). *The Black Swan: The Impact of the Highly Improbable*. New York: Random House.

UK Government Office for Science. (2014). *Annual Report of the Government Chief Scientific Adviser 2014. Innovation: Managing Risk, Not Avoiding It*. London.

UNEP (1995). *International Technical Guidelines for Safety in Biotechnology*. Nairobi: United Nations Environment Programme.

US NRC (2007, April 24). *NRC News: NRC Proposes Adding Plane Crash Security Assessments to New Reactor Design Certification Requirements*. Retrieved 29 December 2014, from www.nrc.gov/reading-rm/doc-collections/news/2007/07-053.html

van Notten, P. (2006). Scenario Development: A Typology of Approaches. In OECD, *Think Scenarios, Rethinking Education*. Paris: OECD.

Vergragt, P. J., & Quist, J. (2011). Backcasting for Sustainability: Introduction to the Special Issue. *Technological Forecasting & Social Change*, 78, 747-755.

von Neumann, J., & Morgenstern, O. (1947). *Theory of Games and Economic Behavior* (2nd ed.). Princeton: Princeton University Press.

Wack, P. (1985a, September). Scenarios: Uncharted Waters Ahead. *Harvard Business Review*.

Wack, P. (1985b, November). Scenarios: Shooting the Rapids. *Harvard Business Review*.

Walker, W. E., Marchau, V. A. W. J. & Swanson, D. (2010). Addressing Deep Uncertainty Using Adaptive Policies: Introduction to Section 2. *Technological Forecasting & Social Change*, 77(6), 917-923.

WEF (2013). *Global Risks 2013: Eighth Edition*. Geneva: World Economic Forum.

Weick, K. E. (1989). Theory Construction as Disciplined Imagination. *Academy of Management Review*, 14(4), 516-531.

Weick, K. E., Sutcliffe, K., & Obstfeld, D. (2005). Organizing and the Process of Sensemaking. *Organization Science*, 16(4), 409–421.

Wilkinson, A., & Kupers, R. (2013, May). Living in the Futures. *Harvard Business Review*.

Wilkinson, A., & Kupers, R. (2014). T*he Essence of Scenarios: Learning from the Shell Experience*. Amsterdam: Amsterdam University Press.

Zimmerman, A., & Bauerlein, V. (2005, September 12). At Wal-Mart, Emergency Plan Has Big Payoff. *The Wall Street Journal*.

irgc

ACKNOWLEDGEMENTS

About IRGC

The International Risk Governance Council (IRGC) is an independent non-profit foundation with an aim to help improve the understanding and management of risks and opportunities by providing insight into systemic risks that have an impact on human health and safety, on the environment, on the economy and on society at large.

Established in 2003 at the initiative of the Swiss government, IRGC is based at École Polytechnique Fédérale (EPFL) in Lausanne, Switzerland, with network partners in Europe, the US and Asia.

As a science-based think tank and neutral collaborative platform with multidisciplinary expertise, IRGC's mission includes developing concepts of risk governance, anticipating major risk issues, and providing risk governance policy advice for key decision-makers. It also aims to build bridges between science and policy in today's challenging governance environment.

Members of the IRGC Foundation Board

Philippe Gillet (Chairman), Vice-President and Provost, École Polytechnique Fédérale de Lausanne (EPFL), Switzerland; **Charles Kleiber** (Vice-chairman), Former State Secretary for Education and Research, Switzerland; **John Drzik**, President, Global Risk and Specialties, Marsh, Inc.; Chairman, Marsh & McLennan Companies Global Risk Center; **Christian Mumenthaler**, CEO, Reinsurance and Member of the Executive Committee, Swiss Re, Switzerland; **Daniele Tonella**, CEO, AXA Technology Services, France; **Margareta Wahlström**, Assistant Secretary-General, Special Representative of the Secretary-General for Disaster Reduction (UNISDR), Switzerland; **Wang Weizhong**, former Vice-minister, Ministry of Science and Technology, People's Republic of China

Members of the IRGC Scientific and Technical Council

Prof. M. Granger Morgan (Chairman), University and Lord Chair Professor, Department of Engineering and Public Policy, Carnegie Mellon University, USA; **Dr. V.S. Arunachalam**, Founder Chairman, Center for Study of Science, Technology and Policy (CSTEP), India; **Prof. Wändi Bruine de Bruin**, Professor of Behavioural Decision Making, Leeds University Business School, UK; **Prof. Luis Abdón Cifuentes**, Associate Professor of Industrial Engineering, Pontifica Universidad Católica, Chile; **Dr. Gérard Escher**, Senior Advisor to the President, École Polytechnique Fédérale de Lausanne (EPFL), Switzerland; **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. Janet Hering**, Director, Swiss Federal Institute of Aquatic Science and Technology (EAWAG), Switzerland; **Prof. Kenneth Oye**, Associate Professor of Political Science and Engineering Systems, Massachusetts Institute of Technology (MIT), USA; **Prof. Arthur Petersen**, Professor of Science, Technology and Public Policy, University College London (UCL), UK; Prof. Ortwin Renn, Dean of the Economic and Social Science Department, University of Stuttgart, Germany; **Prof. Jonathan B. Wiener**, William R. and Thomas L. Perkins Professor of Law, Duke Law School, USA; **Prof. Xue Lan**, Professor and Dean, School of Public Policy and Management, Tsinghua University, People's Republic of China

irgc

International Risk Governance Council

c/o Ecole polytechnique fédérale de Lausanne EPFL
CM 1 517
Case Postale 99
1015 Lausanne
Switzerland

Tel +41 (0)21 693 82 90
Fax +41 (0)21 693 82 95

info@irgc.org
www.irgc.org