

United Nations Economic Commission for Europe

Risk Management in Regulatory Frameworks: Towards a Better Management of Risks



**United Nations
New York and Geneva, 2012**

Note

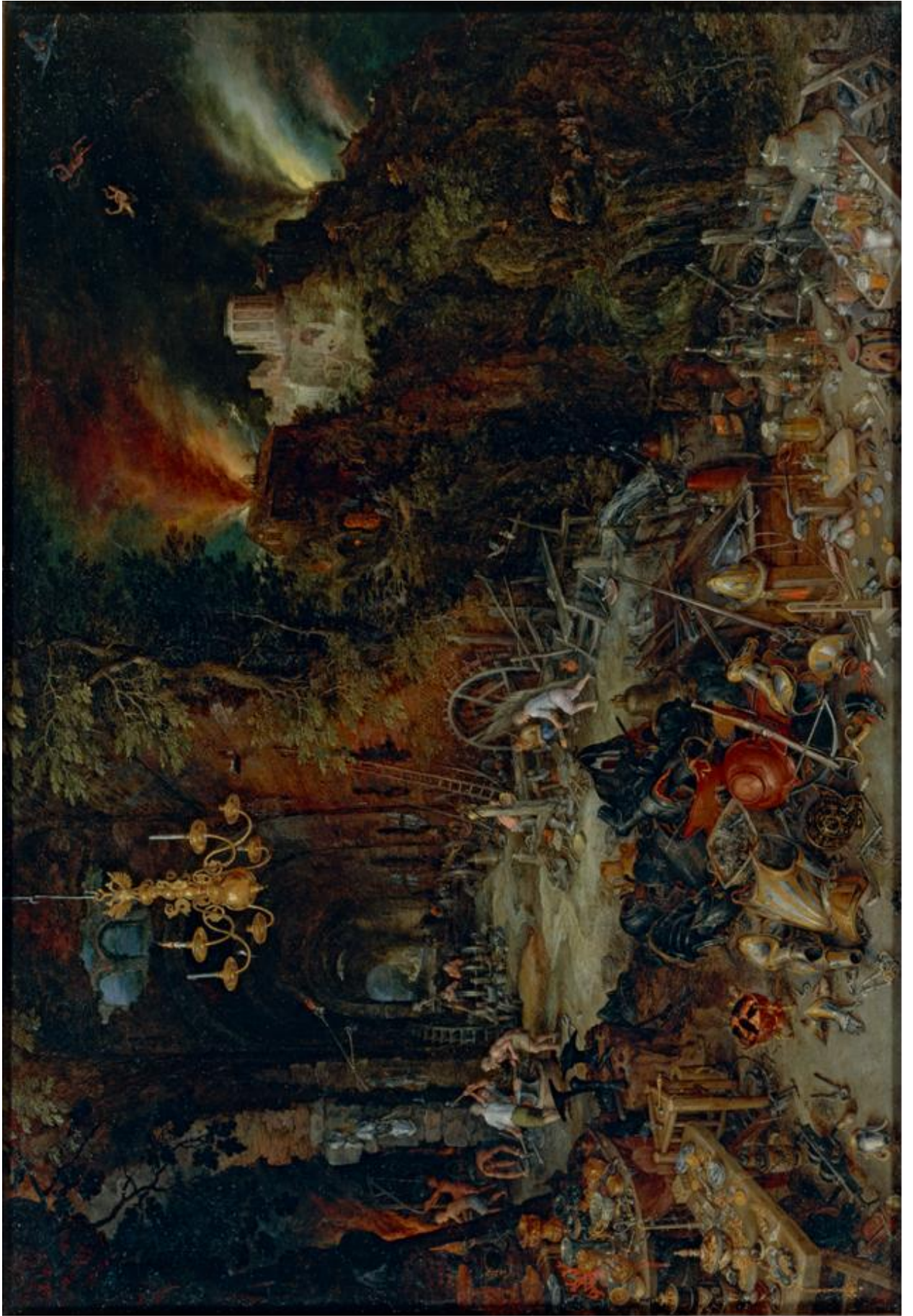
The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Acknowledgements

This publication was drafted by Lorenza Jachia and Valentin Nikonov. It is based on the work carried out under the auspices of the UNECE Working Party on Regulatory Cooperation and Standardization Policies. The authors would like to thank the members of the Group of Experts on Risk Management in Regulatory Systems as well as other experts who have participated in the Working Party's discussions on risk management since 2009. They also acknowledge with thanks the comments received from Virginia Cram-Martos, Director, Division on Trade and Sustainable Land Management at the UNECE. The publication was edited by Erica Meltzer.

The views presented in this publication are those of the authors and do not necessarily represent those of the members of the Group of Experts on Risk Management in Regulatory Systems, or of the UNECE and its member States.

Finally, the authors wish to thank the Pinacoteca Ambrosiana of Milan for granting permission to use the copyrighted image that appears on the cover page and opposite this page. The image reproduces the famous painting by Jan Bruegel, "The allegory of fire". It was chosen to illustrate the dual nature of risks: fire can destroy, fire can create. The right hand side of the painting is dominated by a wild conflagration that reduces a building to ashes, the left hand side portrays fire as the energy that men have used for millennia to create objects of everyday use. Any risk, well managed, is an opportunity.



Preface

Among the most unsettling, and paradoxical, consequences of globalization has been its effect on risks: while it has great potential to reduce the impact and likelihood of a number of risks – local and global, natural and manmade – it has also helped magnify and spread others. The increasingly complex and intertwined nature of global supply chains spanning continents and oceans has brought many benefits but also directly or indirectly contributed to a wide range of events resulting in loss of life, environmental degradation and economic hardship.

Fortunately, another outgrowth of globalization has been astounding scientific and technological progress that has produced great welfare gains for society. Such advances entail their own risks, of course, but they have also enabled humanity to better shield itself from hazards. Harnessing this potential, however, cannot be done by controlling or regulating the behaviour of an individual company, country or region. International standards, regulatory response and coordinated action at the international, regional, national and local levels are the best and perhaps the only means of treating risks that have potentially worldwide consequences. The task is urgent, given that a number of risks are acquiring global proportions.

The United Nations Economic Commission for Europe is proud to contribute through this publication to global efforts to mitigate these risks and their potentially devastating consequences – efforts in which regulation is often paramount. While much has been written about the nexus between risk management and regulation, we believe this publication is the first to address the potential role of regulatory risk management in creating an effective synergy between the two fields, by transforming risk management concepts into regulatory actions. It argues that risk management should be a central process underlying all regulatory activity; that it should involve all stakeholders and a higher level of policymaking; and that sound regulatory systems should be driven by sound risk management processes. As such, the publication is intended to assist policymakers, regulators, businesses and other decision makers in making more informed choices about mastering the risks that confront our families, our communities and our planet.

Sven Alkalaj

Executive Secretary

United Nations Economic Commission for Europe

Geneva, June 2012

Contents

Preface.....	v
Abbreviations	ix
Executive summary	xi
1 Introduction: Risk management and regulatory systems	1
2 Managing risks	3
2.1 Introduction	3
2.2 What is a risk?	5
2.3 What is good risk management?	8
2.4 The main functions of the risk management process	11
2.4.1 Establishing the context	11
2.4.2 Risk identification	12
2.4.3 Risk analysis and evaluation	15
2.4.4 Choosing and implementing risk treatment strategies.....	18
2.4.5 Contingency planning and crisis management	20
3 Risk management in regulatory systems: a reference model	23
3.1 Risks from the perspective of a regulatory system.....	23
3.2 Existing analytical frameworks of risk management in regulation and business.....	24
3.3 Key principles of risk management in regulatory systems.....	25
3.4 Setting the objectives of a regulatory system and the risk evaluation criteria	29
3.5 Management of assets (traceability provisions)	32
3.6 Risk identification in regulatory systems	35
3.7 Using the objectives of a regulatory system to evaluate risks.....	36
3.8 Available risk treatment strategies	37
3.9 Implementing risk treatment strategies	40
3.10 Crisis management in regulatory systems	41
3.11 Monitoring and review	43
3.12 Application of the model.....	44
4 Regulation as a risk mitigation tool.....	45
4.1 What is regulation?.....	46
4.2 Assessing the consistency of the regulatory portfolio.....	46
4.3 Types of regulations that can be used to mitigate risks.....	48
4.4 The structure of the regulation development process.....	49
5 How does regulation work in practice? An example.....	53

5.1	Inputs to a regulatory system	54
5.2	Different stages of rule-making	57
5.3	Production or service provision	66
5.4	Pre-market control: conformity assessment.....	69
5.5	Product market placement and consumption	76
5.6	Post-market control: market surveillance	77
5.7	Ex-post analysis	80
6	Risk management at UNECE WP.6	83
6.1	The UNECE Recommendation on risk management in regulatory frameworks	85
6.2	The UNECE recommendation on crisis management in regulatory frameworks.....	87
6.3	The Group of Experts on Risk Management in Regulatory Systems (UNECE GRM)	88
6.4	Future plans	88
7	Evaluating risk management in regulatory systems	91
7.1	Introduction and objectives.....	91
7.2	Assigning responsibility for the project.....	91
7.3	Preparing the evaluation	92
7.4	Evaluating the objectives of the regulatory system	93
7.5	Evaluating how assets are managed	94
7.6	Evaluating risk identification.....	94
7.7	Risk evaluation	95
7.8	Evaluating how risk treatment strategies are chosen	95
7.9	Evaluating how risk treatment strategies are implemented	96
7.10	Evaluating crisis preparedness.....	97
7.11	Evaluating the improvement of risk management processes.....	97
8	Conclusions	99
	ANNEX	101
	List of members of the UNECE GRM, at the time of publication	101
	References	102

Abbreviations

BIS	Bank for International Settlements
CAB	Conformity Assessment Bodies
COSO	Council of Sponsoring Organizations
CROs	Common regulatory objectives
DCMAS	Network on Metrology, Accreditation and Standardization for Developing Countries
EC	European Commission
EFSA	European Food Safety Authority
EMARS	Enhancing Market Surveillance through Best Practices in Europe
EU	European Union
GMSP	General Market Surveillance Procedure
HAZOP	Hazard and operability study
IAEA	International Atomic Energy Agency
IAF	International Accreditation Forum
IEC	International Electrotechnical Commission
IECEE	Worldwide System for Conformity Testing and Certification of Electrotechnical Equipment and Components
IECEX	International Electrotechnical Commission System for Certification to Standards Relating to Equipment for use in Explosive Atmospheres
ILAC	International Laboratory Accreditation Cooperation
IPMA	International Project Management Association
IRGC	International Risk Governance Council
ISMS	Information security management system
ISO	International Organization for Standardization
IT	Information technology
ITC	International Trade Centre
ITU	International Telecommunication Union
MARS Group	UNECE WP.6 Group of Experts on Market Surveillance
MLAs	Multilateral recognition arrangements

MRAs	Mutual recognition agreement
MSAs	Market Surveillance Authorities
NGO	Non-governmental organization
OECD	Organisation for Economic Co-operation and Development
OSHA	Occupational Health and Safety Administration
PHA	Preliminary Hazard Analysis
PMI	Project Management Institute
PROSAFE	Product Safety Enforcement Forum of Europe
RCA	Root Cause Analysis
REACH	Registration, Evaluation, Authorization and Restriction of Chemical Substances
RIA	Regulatory impact assessment
SDO	Standard development organization
SDoC	Supplier's Declaration of Conformity
SPS	Sanitary and phytosanitary measures
TBT	Technical barriers to trade
UNECE	United Nations Economic Commission for Europe
UNECE GRM	UNECE WP.6 Group of Experts on Risk Management in Regulatory Systems
UNECE WP.6	UNECE Working Party on Regulatory Cooperation and Standardization Policies
USAID	
WEF	World Economic Forum
WHO	World Health Organization
WMO	World Meteorological Organization
WP	Working Party
WTO	World Trade Organization

Executive summary

The UNECE Working Party on Regulatory Cooperation and Standardization Policies started its work in 1970 as a forum for dialogue among regulators and policymakers. Since then, it has been working on a number of topics, including technical regulations, standardization, conformity assessment, accreditation, metrology, market surveillance and risk management. It makes recommendations that promote regulatory policies to protect the health and safety of consumers and workers and preserve our natural environment, but without creating unnecessary barriers to trade and investment.



Since 2010 the Working Party has focused considerable effort on the nexus between risk management and regulation. There is a large body of literature on that nexus, most of which describes how risk management tools can be used by regulators, who have introduced many regulations in response to specific risks. This publication goes beyond that nexus, presenting a framework for designing regulatory systems with the risk management process as their driving force.

Regardless of the level on which risk management is implemented, and no matter how sophisticated, technical and theoretical its tools and methods might seem, it is fundamentally about helping decision makers choose and implement the right decisions and actions, particularly under circumstances of limited resources and uncertainty.

A regulator who is trying to set the parameters for a new regulation; a policymaker who is choosing scenarios for the future development of an economic sector; or a business that is designing its sales strategy are all examples of decisions that require applications of risk management tools.

This publication is an attempt to induce and help implement change in the structure of regulatory systems and frameworks. It presents tools and models that have been developed in response to the problems faced by various entities in implementing risk management tools within regulatory systems. It does not – nor could it – cover all such problems; instead, it focuses on those that in our view are the most important, as identified by the risk management needs assessment survey conducted by the Working Party in 2010.

Issues addressed by this publication

Risk management tools are widely implemented within businesses and in the development of regulations. However, in many cases, regulators and companies subject to regulation, as well as other regulatory stakeholders, use **different terms and refer to different models** when talking about risks and risk management.

Since standards have historically been the basis for a common language for international relations and embodied best practice across various fields, this publication begins with an overview of risk management-related standards and concepts (**Chapter 2, Managing risks**). It describes the concepts, terms and functions of the risk management process as they are presented in recent ISO standards on risk management (including ISO 31000:2009). To assist in practical implementation, the chapter offers guidance on which tools can be used when performing each function (including “what-if” analysis for risk identification, the “consequence/probability” matrix for prioritizing risks, vulnerability analysis, and the use of diversification for risk treatment).

Building a risk-based regulatory system – a rather recent trend in regulatory practice – requires a solid legal foundation that provides a consistent description of the risk management process. In many cases, **inconsistency in legislation on risk management** across various sectors and within a single legislative text leads to inefficiencies and errors and hampers risk management-based collaboration. **Chapter 3, Risk management in regulatory frameworks**, describes a holistic model of a regulatory system, function by function and with real-life examples, based on the risk management process. Drafting new legislation and reviewing existing legislation are two areas to which the model can be applied so that all essential risk management functions are consistently and clearly covered by the law.

The model – based on the UNECE Recommendation on “Risk management in regulatory frameworks” – includes the most important steps for structuring a risk-based regulatory intervention: a full and timely identification and assessment of risks, followed by a structured risk management process. In particular, the model promotes the idea that risk identification should be conducted on the basis of fully defined and shared objectives for the regulatory system and asset management processes, which are established with broad stakeholder involvement. The chapter also describes how regulators can develop and use criteria to determine acceptable levels of risk – risk that regulators deliberately choose not to mitigate – and proposes practical methods for implementing risk acceptance strategies.

Regulations are often triggered by risks. However, regulation is not the only available risk treatment option. To avoid **overreaction to risks in regulatory systems**, tools for choosing the best of four main risk treatment strategies are also described, namely: tolerating a risk, avoiding a risk, transferring a risk and mitigating a risk. In cases where the regulatory option is preferred, the chapter presents examples and best practice for implementation strategies.

Several catastrophic events have shown that regulatory stakeholders are often **unprepared for crises**. The chapter concludes by providing an overview of best practice that can be applied to make regulatory systems more resilient in the face of crises. It is based broadly on the UNECE recommendation on crisis management in regulatory frameworks and on standards covering the management of disruption-related risks.

An important tenet in risk-based regulation is the proportionality between regulations and the risks they set out to mitigate. Along with providing basic information on regulations and their types, **Chapter 4, Regulation as a risk mitigation tool**, introduces the concept of a regulatory portfolio and describes it from the perspective of an economic operator. It specifies the cases in which regulations can be independent, complementary or contradictory, offering insights on using the portfolio approach to evaluate existing regulations. The chapter introduces a reference model for a regulatory process resulting in proportionate regulatory requirements and effective pre- and post-market control. The model describes the main functions of the process (such as production and service provision, conformity assessment and market surveillance) together with their inputs and outputs. It can be used to evaluate regulatory processes within a variety of regulatory systems.

Chapter 5, How does regulation work in practice?, gives a detailed description and an example of how each function of the regulatory process can be implemented in practice. Based on an imaginary example, it offers a comprehensive overview of practical aspects of using regulation as a risk mitigation tool. The chapter also provides examples of how to implement the steps necessary for a regulation to mitigate risks.

Chapter 6, Risk management at UNECE WP.6, describes the role of the Working Party on Regulatory Cooperation and Standardization Policies and its Group of Experts on Risk Management in Regulatory Systems in helping policymakers and regulatory authorities manage risks.

Chapter 7, Evaluating risk management in regulatory systems, offers practical guidance on the steps to be taken in implementing the reference models presented in this publication. Any regulatory reform needs to start with an evaluation of existing processes. The chapter discusses how to obtain objective evidence of the level of risk management implementation within a regulatory system as well as how to develop an action plan for implementing best practice and enhancing the risk management efficiency of the system as a whole.

Who should read this publication

Given the crucial nature, broad scope and potential impact of risk management, this publication is aimed at a wide audience, including:

- **Policymakers**, who will benefit from the overview of a regulatory system with risk management as its driving force; will learn how to better apply risk management tools to policymaking; and, thanks to the overview of risk management models, will be enabled to make more informed decisions as to the fields in which risk-based regulatory systems should be developed (chapters 2 and 3).
- **Legislators**, who can use the reference models to describe risk management in legislation in a consistent manner (chapter 3).
- **Regulators**, who will learn how to establish a common risk language for use by all regulatory system stakeholders; develop a common risk management process for their regulatory system; and incorporate risk management best practice into their regulatory work (chapters 3 and 4).
- **Businesses**, which will learn how to participate more actively in regulatory processes and how to call the attention of regulatory stakeholders to risks that businesses and other economic operators cannot manage on their own (chapters 3 and 5).
- **Standardization bodies**, which will better understand their role in the risk management process through the models described in the publication, thereby ensuring that their activities address the most critical risks in regulatory systems (chapters 2 and 3).
- **Conformity assessment bodies and market surveillance authorities**, which will benefit from enhanced coordination of their activities with other regulatory stakeholders.

The publication will be especially useful if it is applied by all stakeholders working in a single regulatory system and should help solve most of the risk management-related problems outlined above.

1 Introduction: Risk management and regulatory systems

A devastating earthquake hit an already fragile Port-au-Prince in January 2010. It was the deadliest tremor in recorded history, leaving enormous losses in its wake. Yet by seismic standards it was a major, but not cataclysmic, event. The consequences were compounded by Haiti's chaotic construction, its lack of a comprehensive national building law and seismic design code, and more generally its poor planning capacity for catastrophes. In



Chile, by contrast, building codes and risk-based building rules have been regularly updated and enforced since their adoption in 1931. Innovative technologies were introduced and applied to disaster risk management and regular training sessions held in educational institutions. Better preparedness was undoubtedly among the factors that helped reduce the consequences of the earthquake that struck there in February 2010, which was 500 times more powerful than the one in Port-au-Prince (World Bank, 2011; Kaufmann and Tessada, 2010).

As this example shows, good management of risks closely mirrors social and economic progress. The history of humanity is also the history of new technologies, including specific technologies for managing risks, which have helped us address and in some cases completely master risks that would have had disastrous consequences in earlier times. Examples of how societies have organized to shield themselves from potential hazards include the invention of vaccination, the development of the insurance industry, dams, fire brigades and weather forecasts. “The revolutionary idea that defines the boundary between modern times and the past is the mastery of risk”, writes Peter Bernstein (Bernstein, 1996): “the notion that the future is more than a whim of gods and that men and women are not passive before nature”.

Good risk management does more than help avoid catastrophes and provide safety. When risks are well managed, we are prepared to take risks we might not otherwise take – risks that are ultimately critical to our success. For example, in the early days of the Internet, many of the companies that seized the opportunities it offered and took the risks it entailed trumped their more hesitant rivals. In this context, managing risks does not mean creating a risk-free world. Everyone is free to take at least some risks – and to either win more if a risky event does not occur, or bear the losses associated with such a risk if it does occur. Risk management aims to avoid unnecessary, unexpected and preventable losses.

People and organizations voluntarily – and in many cases unconsciously – implement a number of risk management strategies. But risk management at the individual level is often inadequate. This publication promotes the concept that risk management should involve policymaking at the highest level and well-structured stakeholder involvement. As risks spread faster, decision-making processes need to be more efficient. This is also because human progress

and technological change, while they do help shield people from hazards, are themselves engendering new risks.

Technological change allows for increasing specialization, and ultimately for the organization of production and consumption on a global scale. Supply chains today are complex and intertwined, spanning entire continents and beyond, and risks have a geographically wider impact than in the past. Until the early twentieth century, production was still primarily a family business. Most goods were consumed within the community that produced them. In this context, for example, the consequences of a botanical disease would generally be limited to one region. In our time, by contrast, such consequences have far wider repercussions, as was demonstrated by the E-coli outbreak of March 2011. Similarly, an economic downturn in one country is felt more widely and has broader systemic consequences for the world economy than in previous centuries. Indeed, recent years have been marked by scores of cross-frontier or even global events resulting in loss of human and animal life, economic hardship and environmental degradation.

Laws, administrative measures and technical regulations, voluntary standards and norms – everything that guides personal and corporate behaviour – are all indispensable parts of a solution to the challenges posed by this increased interdependence. By banning or restricting the use of dangerous products, for example, such measures contribute to people's safety. Taken collectively, they help make products safe, make organizations' processes stable, and protect consumers from hazards without compromising economic development or international trade. This requires sound regulatory systems that are driven by risk management processes.

The goal of this publication is to provide insights and recommendations for all stakeholders – and, again, for policymakers in particular – on designing regulatory systems that result in an efficient, effective and transparent management of risks. We hope that after reading the publication, regulators and policymakers alike will be in a better position to develop and implement projects designed to change regulatory processes so that they allow for better risk management. Even more broadly, we hope that the publication can be used to establish a process for structuring collaboration among the stakeholders involved in regulation. It is based on such collaboration that a system of guidelines for imposing new regulations and amending existing ones can be laid down. Ultimately, better risk management strategy will lead to better regulations and make the organizations involved in developing and implementing them more effective.

As risks acquire global proportions, efforts to manage risks are also being put in place at the global level, with an increasingly crucial role played by the international organizations that address global risks. The successes of the United Nations family and other development and humanitarian organizations in directly reducing risks are justly celebrated: the Organization has, for example, brought down the risk of smallpox to zero, and its rapid-reaction programmes have considerably lowered the risks to civilian populations affected by natural disasters, saving hundreds of thousands of lives. What may be less known is the Organization's role in indirect risk mitigation through the drafting of conventions, regulations and other behavioural guidelines, including vehicle safety regulations and road signs. These functions become all the more important as the world faces risks of global proportions, such as the challenges of economic stagnation, climate change and sustainable development.

This publication focuses on the important role of the United Nations as a regulator and as a policy advisor to governments. It is directed to all those – including non-governmental organizations (NGOs), businesses, and policymakers at the national, regional and international level – who want to make more informed choices about the risks that confront our communities.

2 Managing risks

2.1 Introduction

Risk management is a discipline firmly rooted in organizational management, and particularly in business management. Regulations are often addressed to business operators, which need to implement them through their managerial structures. This chapter describes the various types of risk that are typically faced by business and the main tools that are used to manage them. It thus provides useful background information for the remainder of this publication, which looks at how these concepts can be applied to regulatory systems.

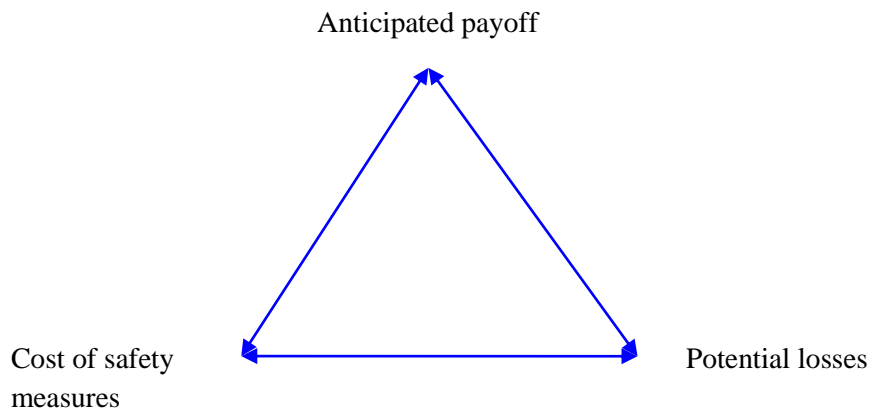
Risk management provides tools for structured thinking about the future and for dealing with the associated uncertainty. Implementing risk management in an organization, or in a regulatory authority, gives decision makers tools that enable rational choices, taken on the basis of the information available, no matter how limited it may be. To illustrate the rationale for implementing a risk management framework we will refer to the basic tenet of project management, which describes the interdependence of the following parameters: a project's budget, the quality of the end product, and the time available for its completion.

A change in any of these parameters for a given project will necessitate changes in the other two. If a project manager shortens the time required for the project's completion, for example, this will either make it more expensive or compromise its quality, or both. If a project manager cuts the project's budget, it will either take longer to complete the project, or the quality of the end product will be poorer. Finally, if the quality requirements of the end product are raised, more time or money, or both, will be required to complete the project.

We can present the general concept of risk management in a similar manner, only in this case we need to focus on the interdependence between the following parameters: the payoff from the activities associated with a risk, the cost of the safety measures, and the potential impact of the risk. The interdependence of these parameters is illustrated in the risk management triangle in Figure 2.1.



Figure 2.1 The risk management triangle



The anticipated payoff does not have to be expressed in monetary terms; we use this expression to refer to the degree to which the objectives and goals of a business or regulator are achieved. For example, the anticipated payoff for a business can be an improvement in client support services, while for a regulator, the payoff can be the benefits to human health from reducing the level of greenhouse gas emissions.

Potential losses are associated with the decision on how to achieve the objective set by the organization or regulator and how to execute the related implementation plan. For example, if the firm decides to start outsourcing its client support service in order to improve its quality, the potential loss can be the loss of control over its own processes. For the regulator, if greenhouse gases are reduced through an increased use of nuclear power as a substitute for coal power stations, the potential losses will be higher than in the higher emission scenario. As for the costs of safety measures, these will include careful processing of the contract with the firm to which the service is outsourced; for the regulator, they will include safeguards for applying a riskier technology to the industry.

For any given project or type of activity, once the objectives are fixed, risks identified and safety measures implemented, changes in any one of these parameters will generally necessitate changes in the other two. The following scenarios are possible:

- If a decision maker wants to lower the costs of safety measures, such a step will increase potential losses, i.e. losses that may be incurred in case a risk event occurs. This simultaneously lowers the anticipated payoff.
- Decisions to minimize potential losses will necessarily lead to more costly safety measures (safer technologies can be more expensive). Other things being equal, this will also decrease the payoff.
- Where there are no risks, there are no profits, and the reverse is also true. The more ambitious the objectives are, the higher the risks. Therefore, a decision to raise the anticipated payoff will lead to increased potential losses and thus more costly safety measures.

Risk management tools, then, enable rational choices to be made among the range of alternative options within the triangle. In other words, the extent to which a desired regulatory objective is achieved will be dependent on the costs of the required safety measures and on forgoing the anticipated profits from one or more areas of economic activity. A regulator could, for example, bring down the number of projected casualties from food poisoning by a desired percentage by enforcing very low tolerated limits on the potentially harmful contents of a food

product. This would, however, entail substantial safety and enforcement costs as well as a reduction in the projected profits of the food industry.

Risk management is defined in the International Standards Organization (ISO) standard ISO 31000:2009 as “coordinated activities to direct and control an organization [or any other user of the standard] with regard to risk”. Using risk management tools allows us to make the right choices so that we can achieve our future objectives.

Describing risk management is an ambitious task: this broad subject has been covered in numerous books, standards and even Nobel Prize lectures. The magnitude and nature of risks varies from one sector to another, and for this reason, many methods and tools have been developed to help people manage risks in specific sectors, some of them involving complex mathematical models. In this publication we will focus on the part of risk management that does not change, which can be thought of as the “risk management engine”. This is a prerequisite to the successful implementation of risk management and applies equally to all sectors and levels.

In the following pages, we will focus on the main elements of risk management:

- Existing definitions of the term “risk” and related terms, the interrelationships among these terms, and available risk classifications
- The context of risk management within and around the organization that implements it
- The main functions of the risk management process (with reference to existing risk management tools, where appropriate)
- Available risk treatment strategies and the situations in which each can be used.

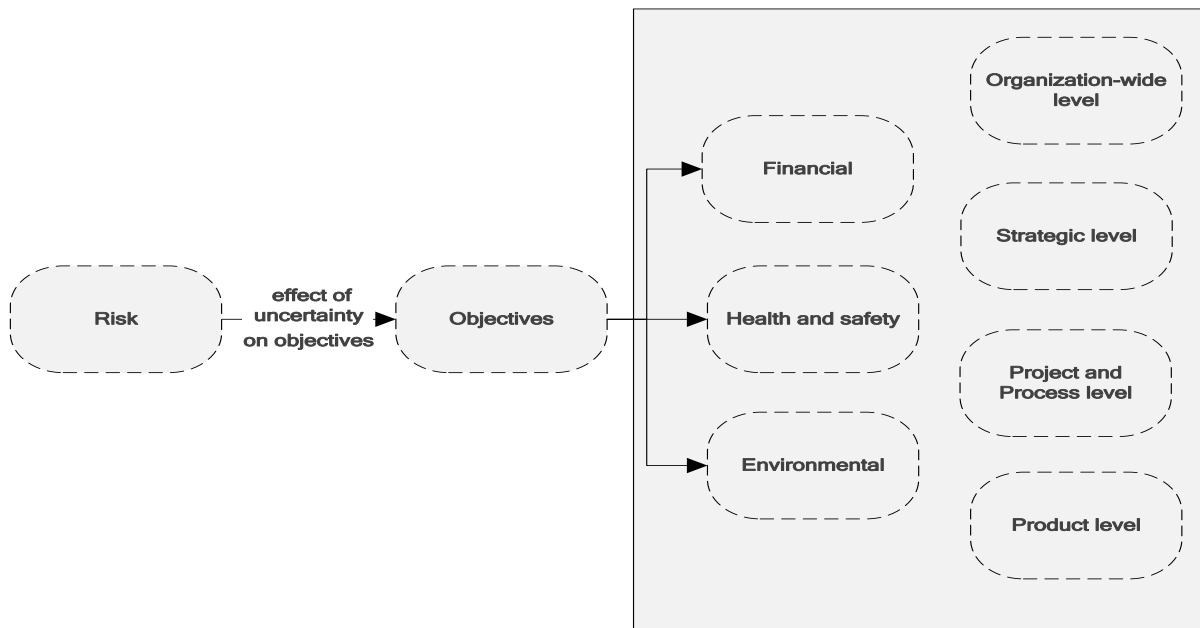
2.2 What is a risk?

A formal risk lexicon is an important building block that enables organizations to refer to and use consistent definitions and build a common understanding of terms. While a shared understanding of risk is crucial, the word “risk” has many different meanings. In fact, “a paragraph written by an expert may use the word several times, each time with a different meaning not acknowledged by the writer” (Slovic and Weber, 2002). Likewise, in everyday discourse, “risk” can refer to a hazard, a probability, a consequence, a potential adversity or threat, and even at times an opportunity.

All of these elements (probability, consequence, hazard, etc.) indeed characterize risks; ISO 31000:2009 provides a general definition of risk as an “effect of uncertainty on objectives”. It follows from this definition that managing risks is not a process that is added on top of other managerial decision-making systems. Rather, risk management is essential to all organizational activities and processes. In the context of a regulatory system, all decision-making processes should similarly be based on the consistent application of risk management tools, in order to ensure that existing and new regulations contribute to managing uncertainty and achieving well-defined societal objectives.

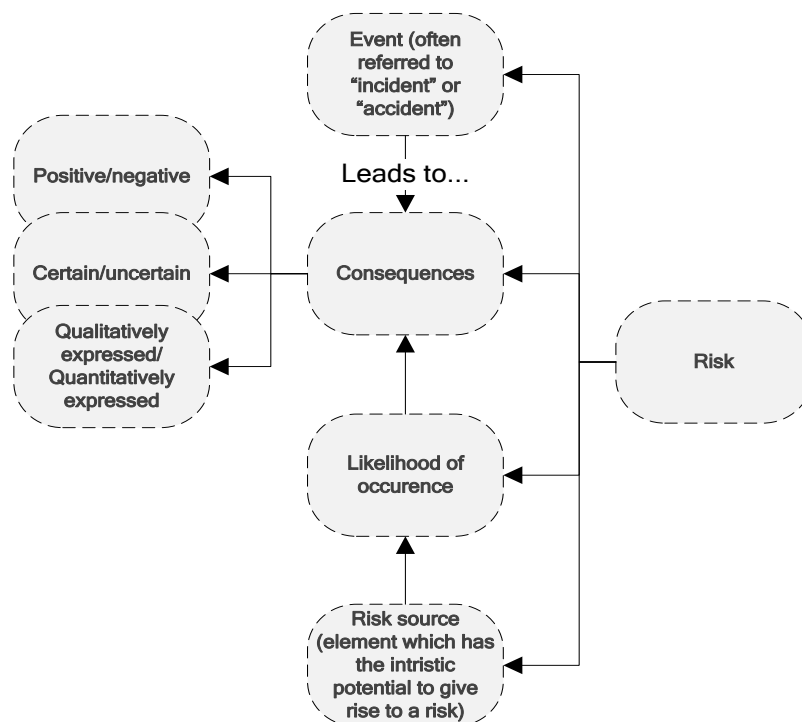
ISO 31000:2009 also states that an effect of uncertainty on objectives is “a deviation from the expected” – which can be positive and/or negative – and that “objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process)”:

Figure 2.2 Risks and objectives



The ISO 31000:2009 standard further notes that risk is often characterized “by reference to potential events and consequences, or a combination of these”, and introduces risk as “a combination of the consequences of an event ... and the associated likelihood of occurrence”. Other elements of risk are likelihood and risk sources. Risk can thus be described as a combination of the following elements, shown in figure 2.3:

Figure 2.3 Risk and its building blocks



In other words, to identify a risk one needs to envisage an event that may or may not occur (the level of uncertainty is characterized by likelihood), due to the presence of risk sources,

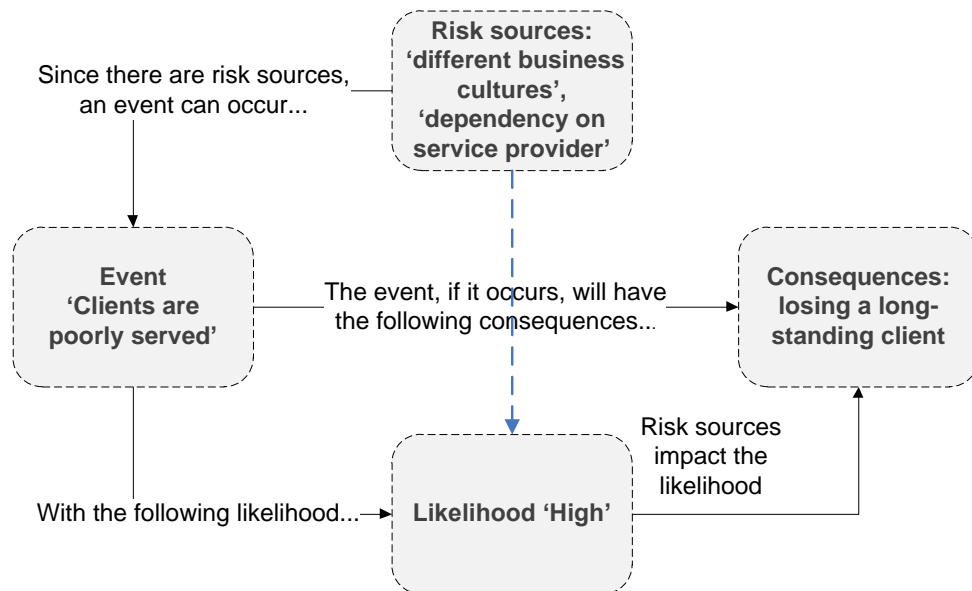
and then foresee its possible consequences. These consequences will in turn have an impact on personal or organizational objectives.

The term “event” is defined in the standard as an “occurrence or change of a particular set of circumstances”. The definition is complemented by a note explaining that “an event can be one or more occurrences, and can have several causes”. According to another note, “an event can consist of something not happening”. Since risks are most commonly associated with incidents and accidents, the standard specifies that “an event can sometimes be referred to as an ‘incident’ or ‘accident’”. Another note suggests that “an event without consequences can also be referred to as a ‘near miss’, ‘incident’, ‘near hit’ or ‘close call’”.

A risk source is defined as an element that “alone or in combination has the intrinsic potential to give rise to risk”. Likelihood – the most mysterious parameter characterizing a risk – is defined simply as the “chance of something happening”. In terms of risk management, this “something” is a risky event.

To see how these elements of risk are interrelated, let us continue the example of a firm that decides to outsource its client support service to a firm located in a country with considerably lower operational costs. The main risk is that longstanding clients will be dissatisfied and will discontinue their contracts. The interaction of the elements of the risk of such a scenario is shown in figure 2.4.

Figure 2.4 The interrelation of risk parameters



If the firm outsources its client support services to a company with a very different business culture, or if the contract was not carefully processed so that the firm has limited influence on the level of service provided, these two elements have the intrinsic potential, alone or in combination with others, to lead to an *event* – losing a long-standing client.

These two factors also have a strong impact on the *likelihood* that the event will occur: for example, if the contract was not carefully assessed, the probability that clients will be

dissatisfied will be that much higher. Similarly, if the firm outsources its services to a company in a country with which it is familiar, the chances of a poor outcome will be lower than in a situation where both sources of risk are present.

Still, even if both sources of risk are present, we cannot be certain that the event will occur: if something is known – if we know for certain that clients will be dissatisfied – then this is not a risk; it is a fact. If the event occurs, it will lead to consequences such as losing a long-standing client (direct costs) or harming the firm's reputation.

The firm can then choose to implement a risk management strategy to minimize the possible “effect of uncertainty on the organization's objectives”. Applying risk management tools will allow the decision maker to:

1. Avoid opportunity costs
2. Avoid direct costs
3. Implement safety measures that are proportionate to the risks

The firm can consider several alternative strategies:

- Outsourcing (accepting the risk)
- Outsourcing while maintaining control of business processes (mitigating the risk)
- Keeping the service in-house (avoiding the risks related to outsourcing)

Managing risks is, as we have said, a prerequisite (although not the only one) for achieving organizational or personal objectives. This, in turn, requires systematically implementing processes that are described in detail in the following pages.

Risk perception and propensity to risk

Two important psychological concepts are directly related to the notion of risk: risk perception, and propensity to risk.

Risk perception is defined in ISO Guide 73:2009, as a “stakeholder's view on a risk”. According to the Guide, risk perception reflects the stakeholder's needs, issues, knowledge, belief and values.

Propensity to risk can be defined as a decision maker's tendency to either take or avoid risks. Decision makers are often classified as risk takers, risk-averse or risk-neutral.

2.3 What is good risk management?

In the example above we have focused on only one of the risks a firm may face. Even if the decision maker manages that risk successfully, a number of other things can still go wrong, some of which could prove an even greater impediment to his or her objectives than dissatisfaction with client support services. For example, the client may already be dissatisfied with the cost of the product that the firm is delivering and may be considering alternative suppliers. This is why a comprehensive identification of all possible risks is a key element of risk management.

The following criteria should be used to assess how well risks are managed:

- Risks are identified in a timely fashion.
- Risks are properly analysed and evaluated, and the most critical risks are given the highest priority.
- A balanced risk treatment is chosen.
- Risk treatment is efficiently implemented.
- Contingency plans are developed, tested and remain relevant, and resources are available to implement them.

Meeting these criteria requires implementing systematic risk management, which calls for the following actions:

- Establishing the context, or knowing what we are “protecting” – our strategy or assets, public health, market efficiency, etc. – and knowing who our stakeholders are.
- Identifying the risks (what are the events that might occur, why might they occur, how probable are they, and what impact could they have on us) and being familiar with as many of them as possible.
- Understanding the risks that are the most important for us, which is why we analyse and evaluate them.
- Starting with the most important risks, choosing a risk treatment option (we can retain the risk, share it with another party, or mitigate or avoid it by removing its source).
- Implementing whichever decision has been taken, which is the direct result of the risk management process.
- Devising a crisis management plan for those risks that are accepted and for those that are mitigated. This results in an action plan for dealing with the risk, should it occur. It is a very important conceptual stage in the risk management process, since risk management is a tool for achieving adequate, but not absolute, safety.

ISO, COSO and other organizations develop standards that help manage different risks at various levels.

Risk management in standards

The description of the risk management process outlined above was derived from various risk management methodologies and standards, which are tools to help organizations efficiently integrate risk management into business practice.

Standards and best practice come from different spheres including banking and finance e.g. Basel III (BIS, 2010), financial reporting and accounting e.g. the Sarbanes-Oxley Act (United States, 2002), internal audit practices e.g. COSO (2004) and information technology standards (e.g. IEC/ISO 27001:2005).

Most such standards cover different types of risks or different steps in the risk management process. For example, IEC/ISO 27001:2005 provides guidance on how to manage information security risks; ISO 14001:2004, environmental risks; and ISO 9001:2008 can be used to manage operational risks*.

* For an overview of risk management-related standards see Avanesov (2009), and for more detail on implementing ISO management systems standards for corporate-wide risk management see Nikonov (2008).

In the paragraphs below, we will introduce in detail the ISO 31000:2009 standard on Risk Management. Another important standard that applies risk management processes to information security is IEC/ISO 27001:2005. It is particularly well adapted to the purposes of this book. In fact, information security presents a number of analogies with regulatory systems, since they are both complex cross-organizational and cross-disciplinary fields.

Just as regulators establish the rules of play for a specific sector or across the board, the top management of an organization develops principles with which all departments must comply. Indeed, not just the IT services but all departments are information asset owners and play a critical role in addressing information security risks. Their work is then affected by information security measures. Regulations have a similarly significant impact on all economic operators. The various departments of an organization may see risks that top management does not, just as economic operators may identify risks that regulators have missed. An organization's internal audit department performs functions similar to those of market surveillance authorities, but the scale of the two systems is different, as the "end clients" of the regulatory system are economic operators and societal stakeholders, while those of the ISMS are the organization's staff, clients and suppliers.

Risk management for information security

As described in IEC/ISO 27001:2005, an information security management system (ISMS) should function as follows.

Once an organization has established a means of coordinating its ISMS through the appropriate policy (containing specific risk acceptance criteria), it can start implementing processes for managing its informational assets. These processes result in a constantly updated informational asset inventory and answer the question, "what needs to be protected?" Once the assets have been identified, the organization performs risk identification and assessment according to an agreed methodology (in order to answer the question, "what are the threats to the assets?"). This results in a list of risks that are then ranked according to their level of criticality. Taking into account the risk acceptance criteria, the organization decides whether to accept each risk, avoid it, transfer it or mitigate it by implementing the appropriate measures. These measures may be taken from Annex A to IEC/ISO 27001:2005 and incorporated into the risk treatment plan, which is used as the basis for developing contingency plans. The ISMS has the usual set of improvement processes: all procedures within its scope are subject to regular internal audits and to corrective and preventive actions, and the characteristics of the system and of the risks are analysed during periodic management reviews.

Just as we do not see how a car engine works simply from watching a car drive by, we do not see how people decide to perform most of the actions they take when managing risks. What we "see" are the *results* of their decisions – the actions aimed at achieving specific goals. And in most cases people perform these actions in a far less structured and systematic way than that recommended by the methodologies.

Ever since the film "Titanic" hit theatres worldwide, our collective memory strongly associates risks with... icebergs. Building on this association, we can say that actions taken in response to risks are the "visible" part of a risk management iceberg, with all the other functions of the risk management process representing its "invisible" but essential foundation.

Risk management principles and guidelines (ISO 31000:2009)

Some risk management standards are generic and present a description of the overall risk management framework. ISO 31000:2009 – the most famous such standard – sets out principles and guidelines that can be applied in any organization and to any regulatory work. The idea behind the standard is to provide some form of systematic risk management in organizations of all kinds, including public organizations. The ISO 31000:2009 framework is based on the “plan-do-check-act” cycle, which helps feed risk management principles into an organization’s management systems to ensure that the latter address the risks systematically.

ISO 31000:2009 also contains a detailed description of the risk management process. It stipulates that the principles of risk management are to create and protect value, while helping to create a culture that maximizes opportunities, and that risk management should be:

- Part of the overall management of the organization, rather than a part of compliance management^{*}
- Part of all decision-making processes
- Tailored to the organization’s internal and external context, taking into account key stakeholders’ perceptions, motivations and values
- Transparent and inclusive, based on structured dialogue among stakeholders
- Dynamic and responsive to change – for example, by ensuring that regulations are updated in keeping with technological, societal and economic changes
- Subject to continual improvement

A well-known framework for enterprise risk management was developed by COSO. This framework links the risk management process to the organizational structure and shows the connection between risk management and strategic planning. The risk management process as described by COSO includes a phase for setting an organization’s objectives and also covers event identification, risk assessment, risk response, control activities, information and communication, and monitoring.

ISO 31000:2009 will likely influence the COSO framework and help align risk management standards across various professions, enabling it to be used in a wide variety of projects and areas (Knight, 2011).

In the following pages we will briefly describe the main functions of the risk management process.

2.4 The main functions of the risk management process

2.4.1 Establishing the context

Risk management is a process that consumes and produces information. As in any other process, the quality of the output depends greatly on the quality of the input. The most important inputs to a risk management process include:

1. **Objectives.** Well-defined objectives are the key input to the risk management process. Risk is, after all, an “effect of uncertainty on objectives”. If the objectives

^{*} AS/NZS 3806:2006 defines compliance as “adhering to the requirements of laws, industry and organizational standards and codes, principles of good governance and accepted community and ethical standards”.

are not well defined, it will be very difficult to identify, understand and manage the respective risks. One of the best practices called for by the Center for International Studies (CSIS) is for “risk identification and assessment [to] be done in reference to the organization’s strategy and missions” (Smith, 2011).

2. **Assets.** Implementing risk management also requires knowing **the assets** – the values of the organization, what it is trying to protect, and the potential sources of additional direct or opportunity costs. Key organizational assets include physical assets, technologies, internal infrastructure, capital, finance, and information systems. These assets can be ranked by criticality and grouped into various categories.
3. **Information on stakeholders and their needs.** A stakeholder is defined in ISO 31000:2009 as a “person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity”. As the behaviour and needs of an organization’s stakeholders can become the sources of many risks, it is crucial to know their needs so as to forecast their behaviour.

In order to enhance the quality of input to a risk management process, ISO 31000:2009 and other risk management standards recommend establishing the external and internal contexts that characterize the “environment in which the organization seeks to achieve its objectives”. This ensures that the process is providing relevant and sufficient data.

According to ISO 31000:2009, the main elements of the external context include the broader cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, as well as the perceptions and values of external stakeholders. The internal context includes such elements as the organization’s culture, policies, structure, roles, accountabilities and decision-making processes.

2.4.2 Risk identification

Risk identification should provide a full and timely picture of the risks faced by an organization. A document listing the risks that have been identified is called a risk register, which is developed by pinpointing the events, sources, likelihood and consequences of all the relevant risks.

Several techniques can be used to develop a risk register. The analysis of risks that have occurred previously is an important source of risk identification and can be the first step in developing an internal classification. In order to collect information on previously occurring risks, organizations draw up internal loss databases and collect information from external sources. An example follows.

In the United States, the Consumer Product Safety Commission (CPSC) maintains the National Electronic Injury Surveillance System (NEISS), a database with information on every visit to the emergency room for an injury associated with consumer products and treated in a US hospital participating in the system. The database – which is accessible and can be queried online – provides regulators with data on potentially dangerous products.

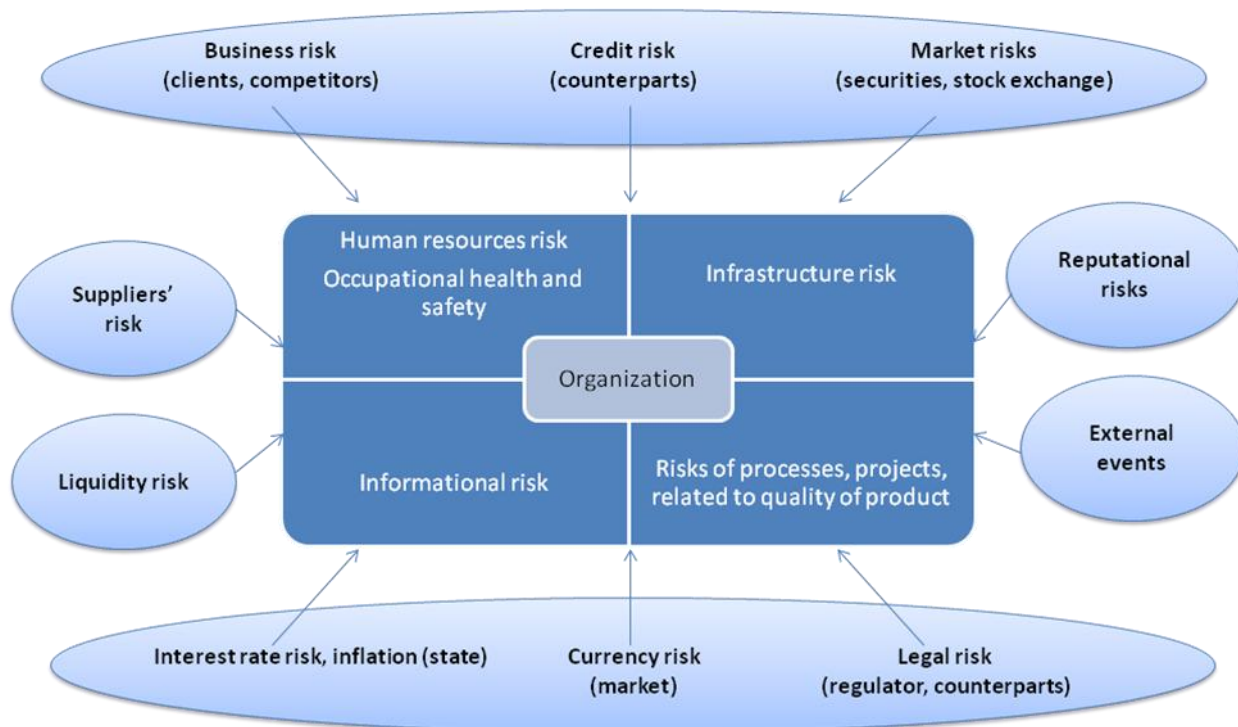
The CPSC has also developed a web-based searchable database (www.saferproducts.gov) which provides consumers and businesses with a secure platform for reporting any unsafe products of which they may be aware. The website protects users’ privacy and also gives businesses whose products have been identified as unsafe an opportunity to review the information before it becomes publicly available.

Source: www.cpsc.gov

Most risk classifications were developed in a business environment, but they can also be used in the context of a regulatory system.

The figure below illustrates some of the types of risks that can affect a business:

Figure 2.5 Various types of business risks



As shown in the figure, some of these risks are internal; they are rooted in business processes and are determined by the nature of the organization's activities. Such risks – often referred to as “operational risks” – stem from inadequate business processes, human error and system failures. Typical operational risks include occupational health and safety risks, human resources risks, information technology (IT) risks and infrastructure risks. As will be discussed in greater detail in chapter 3, from a regulator's standpoint risks can be further classified by the ability of regulatory stakeholders to manage risks on their own (as opposed to the need for coordinated actions) and by their impact on other stakeholders (as opposed to risks that affect only one entity or policy area). As the example below shows, understanding which risks affect business, and in which way they are managed, is crucial to defining a regulator's response.

Other risks have external roots: they come from markets, partners, consumers, regulatory actions, and the natural environment. Business risk comprises all the events related to changes in the demand for the organization's products and services, changes in the prices of these products, and other related factors.

Market risk can be subdivided into four categories: interest-rate risk (changes in the interest rate), currency risk (changes in currency exchange rates), commodity risk (changes in commodity prices) and security risk (changes in security prices). All of these parameters affect almost every business and can have a significant impact on the organization's ability to achieve its objectives.

All companies are exposed to market risk, although its impact varies among sectors. This is reflected in the Lloyds Bank Business Risk Report (Lloyds Bank 2011), which covers the attitudes of United Kingdom businesses to financial market risks. It states that as of April 2011, concerns about interest rate risks were the highest in the hospitality/leisure and transport sectors, although they appeared to be relatively well hedged. In contrast, concerns were the lowest in the business services and healthcare sectors, perhaps reflecting low borrowing needs and, in the case of healthcare, a relatively high level of protection against such risks.

Companies in the manufacturing, retail/wholesale and transport sectors were the most concerned about the impact of commodity prices on their business. However, the proportion of such companies with a hedging strategy in place was low relative to those that expressed greater concerns about the risk. Companies in the business services and healthcare sectors were somewhat less concerned about commodity price risks.

Source: Lloyds Bank (2011)

It is not only financial institutions that can be affected by credit risks, although such risks are very common for them. All of the events that can prevent an organization's counterparts from meeting their contractual obligations, such as when a company provides services that its clients do not pay for, can be grouped under this heading.

Most commonly, a classification of risks will also include reputational risks, liquidity risks and legal risks.

Arthur Andersen LLP, based in Chicago, was once one of the "Big Five" accounting firms providing auditing, tax and consulting services to large corporations. In 2002, the firm voluntarily surrendered its licences to practice as Certified Public Accountants in the United States after being found guilty of criminal charges relating to its handling of the auditing of Enron, a Texas-based energy corporation that had filed for bankruptcy in 2001 and later failed. Other national accounting and consulting firms bought most of the practices of Arthur Andersen. The verdict was subsequently overturned by the US Supreme Court, but the damage to its reputation has prevented it from recovering as a viable business, although it still exists on paper.

Source: Wikipedia

Risk classifications help in performing comprehensive risk identification. To develop a risk register, one can go through all the existing risk types in an effort to understand what each of them means for the organization.

On a global level, risks are identified and discussed by various international organizations and forums. For example, the Global Risks Report (WEF, 2011) identified five risks as "risks to watch", because survey respondents assessed them as having high levels of variance and low levels of confidence, while experts consider that they may have severe, unexpected or underappreciated consequences:

- Cyber-security issues, ranging from the growing prevalence of cyber-theft to the little-understood possibility of all-out cyber-warfare
- Demographic challenges adding to fiscal pressures in advanced economies and creating severe risks to social stability in emerging economies
- Resource security issues causing extreme volatility and sustained increases over the long run in energy and commodity prices, if supply is no longer able to keep up with demand
- Retrenchment from globalization as a result of populist responses to economic disparities, if emerging economies do not assume a leadership role

- Weapons of mass destruction, especially the possibility of renewed nuclear proliferation between States

Source: WEF (2011)

IEC/ISO 31010:2009 provides a detailed description of tools that can be used to perform risk identification and other steps in the process.

Risk identification can be undertaken during a brainstorming session by means of simple checklists, in which case a classification of risks can guide discussions. It can also be accomplished through a series of interviews, in which case risk classifications will help identify the most appropriate respondents and structure the questionnaires. Other useful tools for risk identification include the “Delphi technique”, a methodology for facilitated consensus-building, and “preliminary hazard analysis” (PHA). The idea of the latter is to develop a list of hazards and risks by considering such characteristics as the materials and equipment that are used or produced in a given process or industry, the operating environment, and the interfaces among system components.

Another IEC/ISO 31010:2009 tool for risk identification is HAZOP – an acronym for “hazard and operability study”. This is a structured and systematic examination of how an existing product, process, procedure or system will respond to changes in key parameters, and is based on the use of guidewords that “question how the design intention or operating conditions might not be achieved at each step in the design, process, procedure or system”. HAZOP reviews each part of a design to discover the deviations that can occur from the intended performance, their potential causes and the likely consequences.

A simpler alternative to HAZOP is structured “what-if” analysis. This involves a systematic, team-based study using standard “what-if” type phrases in combination with prompts to investigate how a system, organization or procedure will be affected by deviations from normal operations and behaviour. Discussion is facilitated by creating a question using a “what-if” phrase, such as “what if...”, “what would happen if...”, or “has anything or anyone ever...”. The intention is to stimulate the study team to explore potential scenarios and their causes, consequences and impacts.

“What-if” analysis involves the application of a more general tool called “scenario analysis”, in which descriptive models are developed of how the future might turn out. It helps to identify risks by considering possible future developments and exploring their implications. IEC/ISO 31010:2009 comments that “possible future scenarios are identified through imagination or extrapolation from the present and different risks considered assuming each of these scenarios might occur”.

Source: IEC/ISO 31010:2009

2.4.3 Risk analysis and evaluation

The objective of the risk analysis-and-evaluation phase of the risk management process is to prioritize the previously identified risks so that the most important are addressed first, which is accomplished by comparing them all with one another.

ISO 31000:2009 states that risk analysis involves “developing an understanding of the risk by determining consequences and their likelihood, and other attributes of the risk”. Risk evaluation, in turn, involves “comparing the level of risk found during the analysis process with risk criteria established when the context was considered” so that the need for treatment can be considered.

Two elements of the concept of risk can be quantified as estimates: likelihood, and consequences. Likelihood can be quantified in terms of probability, and consequences for business are often expressed as monetary or time losses, whereas for a regulator the consequences could be economic loss, ecological damage or deterioration of public health. If decision makers trust these estimates, they can calculate the expected value of a risk by multiplying probability and consequences.* Doing this for all risks permits them to be ranked. Those with the largest expected values will be the most critical to an organization.

Frequently, however, risks cannot be quantitatively assessed. In such cases, building a consequence/probability matrix is the most simple and commonly used tool for prioritizing risks. It allows for combining qualitative or semi-qualitative ratings of consequence and probability to produce an objective and consistent risk rating. According to IEC/ISO 31010:2009, it “is commonly used as a screening tool when many risks have been identified, for example to define which risks need further or more detailed analysis”.

To apply this method, an organization should develop customized scales for potential consequences and probabilities of events and a matrix that combines the two. Probability may be graded as “very low”, “low”, “medium”, “high” or “very high”. It is important that all stakeholders understand what is meant by each of the lines in the matrix, which can be accomplished by using explanatory notes such as “low probability means ‘unlikely to occur’”.

Similarly, the whole range of consequences can be graded as having “very low”, “low”, “medium” or “high” and “very high” impact. Consequences typically include financial loss, occupational safety, client safety, environment, reputation and other parameters. A typical matrix might look as follows:

Category	Finance	Occupational safety	Reputation
Very high consequences	Losses exceeding \$1,000,000	More than 1 casualty	Broad negative news coverage in international media
High consequences	Losses from \$750,000 to \$1,000,000	Casualty	Broad negative news coverage in local media
Medium consequences	Losses from \$500,000 to \$750,000	Serious injury	Some negative articles in mass media
Low consequences	Losses from \$250,000 to \$500,000	Medium injury	Widespread rumours
Very low consequences	Losses below \$250,000	Light injury	Rumours (which have been reported less than 3 times)

One risky event may affect all these categories to differing degrees: the impact of a given risk may, for example, be “low” in finance, “medium” in occupational safety and “critical” in reputation. Developing a matrix of these criteria makes it easy to assign an overall ranking to a risk, corresponding to the highest grade assigned to any of the consequences.

* In such situations we assume that risk is a random variable with two events: 1) Risk occurs: probability P, consequences A; 2) Risk does not occur: probability 1-P, consequences 0. Expected value is P times A.

One benefit of this tool is that it prevents its users from quantifying consequences that are in fact unquantifiable, such as loss of life or health. It also helps policymakers compare risks that occur in widely different areas and develops a government-wide approach to risk management.

Once the risks have been ranked by both probability and consequences, the organization needs to assign a level of criticality to every combination of probability and consequences (such as “high probability and high impact” – a critical risk). This allows us to develop the kind of matrix illustrated in Figure 2.6.

Figure 2.6 An example of the “probability – impact” matrix for risk ranking

	Very low consequences	Low consequences	Medium consequences	High consequences	Very high consequences
Very low probability	Low risk	Low risk	Low risk	Low risk	Medium risk
Low probability	Low risk	Low risk	Low risk	Medium risk	Medium risk
Medium probability	Low risk	Low risk	Medium risk	Medium risk	Critical risk
High probability	Low risk	Medium risk	Medium risk	Critical risk	Critical risk
Very high probability	Low risk	Medium risk	Critical risk	Critical risk	Critical risk

The organization can then use the matrix to rank all the risks it has previously identified.

There are many other methods for risk evaluation, most of which can be used to analyse any risk. A few such methods are described in the following box:

Some methods for risk evaluation

“Event trees” are one of the most widely used methods in system risk analysis. The method involves performing an inductive failure analysis to determine the causes and consequences of a possible single future failure for the overall system risk or reliability. “Event tree analysis” (ETA) uses similar logic and mathematics as “fault tree analysis”, but the approach is different. The latter uses a deductive approach (from system failure to its reasons), while ETA uses the inductive approach (from basic failure to its consequences). For example, fault tree analysis would allow us to assess how our business would be affected in the event of an earthquake, whereas event tree analysis could be used to determine the possible causes of a faulty production consignment.

“Layers of protection analysis” (LOPA) is still another method – this time semi-quantitative – for estimating the risks associated with an undesirable event or scenario. It analyses whether there are sufficient measures to control or mitigate the risk.

Other quantitative methods that can be used for risk evaluation include Markov

analysis (cf. page 69 in IEC/ISO 31010), Monte Carlo simulation (page 73), FN curves (page 79), Bayesian statistics and Bayes Nets (page 76), human reliability analysis, and risk indices (page 81).

Source: IEC/ISO 31010:2009

2.4.4 Choosing and implementing risk treatment strategies

Once the risks have been prioritized, the organization can start choosing risk treatment strategies for each of them, beginning with the most critical. Risk acceptance criteria or risk appetite – the level of risk that an organization considers acceptable – is an important input to this function.

In the following pages, we will focus on four principal risk treatment strategies:

- Tolerating or accepting a risk
- Transferring or sharing a risk
- Mitigating a risk
- Avoiding a risk

As stated in ISO 31000:2009, “selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment”. Cost/benefit analysis is frequently applied to choosing a risk treatment strategy, and enables the total expected costs to be weighed against the total expected benefits in order to choose the best or most profitable option.

At least three parameters should be considered in choosing a risk management strategy: the level of risk, the benefits to be gained from the activities that involve a risk (which can be expressed in terms of objectives), and risk treatment costs.

Tolerating or accepting a risk means that an organization recognizes a risk but takes no action to lower its probability or impact. This option should be considered in the following situations:

1. Where the “stakes are high”, meaning that the expected benefits of accepting a risk are extraordinary
2. Where risk treatment costs are higher than the estimated costs associated with the occurrence of the risk (e.g., it makes little sense to spend \$100 to mitigate a risk that, should it occur, will entail losses of \$50)
3. Where something is beyond personal or organizational control, and there is nothing to be done but to accept a risk
4. Where a decision maker *wants* to accept a risk (and all the regulatory and legal requirements have been met).

Accepting a risk is by no means the same as forgetting about it. It implies that those who do so know why they are doing it; that the risk appears on the risk register; and that all accepted risks are considered when developing contingency plans.

Transferring a risk means sharing the risk with another party or parties. One strategy for this is outsourcing, in which one entity delegates to another a set of activities and the associated risks. Insurance is another commonly used risk transfer strategy.

Catastrophe financing: the use of alternative risk transfer instruments

The most common form of risk transfer, insurance, shifts exposure to insurers in exchange for a premium. However this depends on insurers being able to profitably pool and absorb a range of risks through diversification over time and space. This is becoming more difficult as disasters are increasingly regionally and temporally concentrated, thanks in part to development in hazard-prone areas. Of the most costly insured catastrophes in the past 40 years, two thirds have occurred since 2001. The World Economic Forum's Global Agenda Council on the Mitigation of Natural Disasters produced an analysis of new forms of risk transfer which involve shifting parts of catastrophe risk exposure directly to financial markets.

Alternative risk transfer (ART) instruments offer innovative financial solutions to meet the growing needs of financial coverage of catastrophic risks and permit investors to play a more direct role in that sphere. One example of such instruments is a catastrophe bond which enables a company, international organization or government to issue bonds to protect them against predefined risks. Over 160 "cat bonds" have been issued to date around the world to protect against pandemics, terrorism and natural disasters. Another promising financial innovation is weather index-based micro-insurance for subsistence farmers in countries where traditional insurance is unavailable or unaffordable. With proper regulation and transparency, such instruments can provide additional capital and offer new ways to hedge catastrophe risks, protect individuals and reduce the systemic impact of future disasters.

Source: Michel-Kerjan (2009)

Mitigating a risk means trying to minimize the consequences and/or likelihood of the risky event. This can be done by removing the risk sources, changing the likelihood of the occurrence of the event or changing its consequences.

Avoiding a risk entails renouncing or discontinuing the activity that might contribute to the occurrence of a risky event. It involves forgoing all the associated benefits, including some that cannot be foreseen. For example, banning certain production processes might hamper the development of potentially beneficial technologies. Risk avoidance is usually chosen when the expected benefits are lower than the risk mitigation costs and when the risks cannot be accepted.

There are several methods for identifying and eliminating the causes of risk events. Root cause analysis (RCA) attempts to identify the root or original causes instead of dealing with the immediately obvious symptoms. Cause-and-effect analysis seeks to pinpoint the possible causes of an undesirable event or problem. It organizes the possible contributory factors into broad categories so that all possible hypotheses can be considered. A cause-and-effect diagramme is then prepared which outlines the possible root causes or reasons for a specific event, classifies and identifies some of the interactions among the factors affecting a particular process, and analyses existing problems so that corrective action can be taken.

Diversification and hedging strategies can be used to change the consequences of a risky event. Diversification involves minimizing the level of dependence on a given parameter that can change in the future. Examples include investing simultaneously in two assets that "behave" differently, backing up information, and contracting several suppliers.

A hedging strategy entails fixing future parameters that may have an impact on an individual's or organization's objectives. Examples include forward contracts and futures and options.

31000:2009 recommends that "when selecting risk treatment options, the organization should consider the values and perceptions of stakeholders and the most appropriate ways to

communicate with them”. It also advises considering the fact that implementing new controls may create new risks. Even if they do not, a significant risk may arise due to “the failure or ineffectiveness of the risk treatment measures”.

Once an organization has identified risk treatment options for all the risks listed on the risk register, the options should be described in a risk treatment plan, which “should clearly identify the priority order in which individual risk treatments should be implemented”. The standard advises that a risk treatment plan should include:

- The reasons for the selection of treatment options, including the expected benefits to be gained
- A list of those accountable for approving the plan and of those responsible for its implementation
- Proposed actions (which might include regulations)
- Resources requirements

The risk treatment plan is the first concrete result of the risk management process, which leads to implementing proportionate safety measures and taking other decisions for mitigating risks that may affect an organization’s objectives.

2.4.5 Contingency planning and crisis management

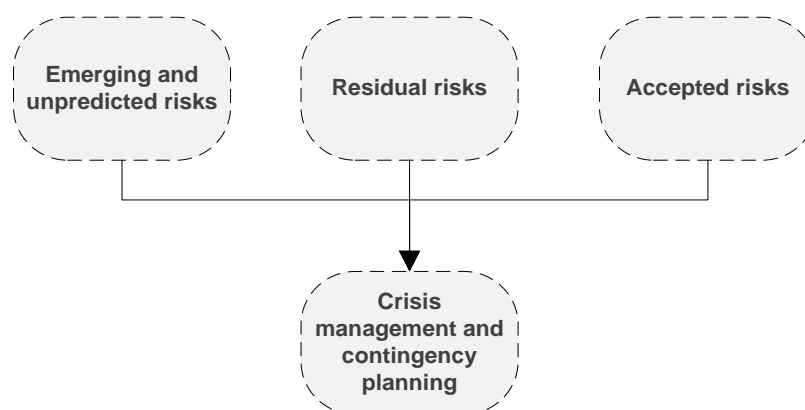
No matter which risk treatment strategies an organization has chosen and implemented, it will never succeed in eliminating risks entirely. At this stage in the process, the organization still faces three major types of risk, as depicted in the figure below:

- Events related to residual risks (risks that remain after risk treatment, as defined in the ISO Guide 73:2009)
- Risks that the organization has chosen to accept
- Risks that were not or could not have been predicted (emerging risks)

All three of these risk types lead to accidents and crises; in the case of crises, the impact depends greatly on how well they are managed. Crisis management is a crucial part of risk management, but it functions efficiently only if linked to other phases of the process, such as risk identification and risk treatment.

The objective of crisis management is to prepare for crises so that if they occur, the harm they cause is minimized. Many crises happen in the same way, leading to similar consequences, regardless of whether they are caused by different risks. Even if a risk that causes a crisis is an emerging risk (as is often the case), and therefore unknown and not spotted during the identification phase, a contingency plan developed for another risk can frequently be used.

Figure 2.7 Input to crisis management and contingency planning



Just as a safety cushion in a car does not mitigate the risk of a car accident but does help to minimize the consequences, so crisis management aims at creating “safety cushions” for organizations. This can be done in at least two ways: by creating buffers and reserves, or by planning for contingencies and developing business continuity plans.

Contingency planning and business impact analysis are among the recommendations and tools cited in the AS/NZS 5050:2010 standard on managing disruption-related risks (“disruption” is an oft-used euphemism for “crisis”).

The purpose of contingency planning is to improve an organization’s ability to respond quickly and optimally to events. The standard recommends that organizations “develop a small number of representative scenarios that could lead to disruption”, and then, for each of these scenarios, estimate the following parameters:

- The time required to restore the most important disrupted activities
- The effect on the organization’s objectives
- The extent to which restoration can be accomplished by current capabilities

Business impact analysis is useful for identifying and managing risks that may lead to breaks in service, as it provides detailed insights into the extent, time frames and mechanisms of disruptive consequences and their likelihoods. This should reveal processes, capabilities, infrastructure and other resources which, if disrupted, would prevent the organization from meeting its critical objectives. Such analysis produces recovery time estimates for each of the risks that can cause a disruption.

Contingency plans “can be activated after an event occurs in order to variously stabilize the situation, restore or continue critical functions and expedite restoration of normality”. They require the development of support capacity, such as reserve servers and local electricity generators. Generally, the more expensive the contingency plan, the shorter the recovery time.

Contingency plans should address three major phases of a crisis:

1. **Stabilization**, which the standard defines as “activities undertaken to limit deterioration, particularly early in a disruptive event”, including:
 - a. Acting to preserve life
 - b. Preventing the spread of further harm
 - c. Countering the source of harm
 - d. Communicating with stakeholders
 - e. Salvaging to prevent further deterioration

- f. Stopping unnecessary expenditure
- 2. **Continuing critical functions**, i.e. functions that are essential for the organization's survival and for the achievement of its critical objectives. Contingency plans should contain specific actions for each critical function or group of functions, such as:
 - a. Alternative work methods or locations
 - b. Deployment of alternative information and communications technology infrastructure
 - c. Sourcing of critical equipment or materials
- 3. **Recovery**, which is defined as "actions taken following the commencement of a disruptive event in order to return the organization to routine management". Recovery involves returning to the pre-disruption condition or to another state that takes advantage of opportunities or changed circumstances.

An example of crisis management good practice

After the 2005 terrorist attacks on the London Underground and a bus, someone set up a sign saying "London area closed". Ministers quickly released a "political value statement" announcing that London would remain open and accessible. Following the 2004 attacks on Madrid's commuter trains, the Spanish Prime Minister made a similar announcement. These announcements had a very positive impact, helping crucially to guide citizens' reactions.

Source: Netherlands (2010)

AS/NZS 5050:2010 provides a set of technical recommendations on how to develop and manage contingency plans. It specifies the purpose of the plans (such as "providing information that is required quickly but cannot be easily obtained" and "preserving good governance during a disruptive event") and their contents (including "activation and stand down criteria", "roles, accountabilities and responsibilities" and "communication and consultation requirements"). The standard can be very helpful in integrating the crisis management function into the overall risk management process.

3 Risk management in regulatory systems: a reference model

3.1 Risks from the perspective of a regulatory system

In the previous chapter we described various types of risks that typically confront businesses and some of the main tools for managing them. In this chapter, we show how these concepts can be applied to a regulatory system.

For the purposes of this publication, we define a regulatory system for any given sector as the set of processes that include: setting regulatory requirements and voluntary standards for the production of goods and the provision of services; drafting laws and regulations; and putting controls in place to check that products meet requirements and specifications.



Since the types of risk described in the previous chapter are present in all businesses (i.e., in all businesses functioning within a given regulatory system), these risks should also be considered at the level of the regulatory system as a whole. A classification of risks based on their origin, similar to the one presented in the previous chapter, can be developed for any regulatory system –food safety or aviation safety, for example.

At the same time, looking at the system as an integrated whole brings out another important dimension of risks that should serve as a basis for developing a classification of risks in a regulatory system. Risks can remain internal to an economic operator and affect its efficiency or profitability, but can also have undesirable external effects. When externalities are important, risks should be given due consideration by policymakers. Such risks typically include:

1. Risks that originate with an economic operator, whose consequences may have an impact on:
 - Consumers, communities or civil society (business-to-consumer risks)
 - Other businesses (business-to-business risks)
 - The environment (business-to-environment risks)
 - Society in general (business-to-society risks)
2. Risks that originate with a single economic operator or with the business environment, and whose mitigation requires coordination among economic operators because a single operator will not be able to mitigate (manage) on its own

3. Risks that originate with the business environment, which will have an impact on an economic operator but which an economic operator cannot control, such as environmental risks

A major type of risk in all regulatory systems is operational risk, which – as also happens in individual organizations – stem from inefficient system processes, human error and information system failures. Examples include: mistakes in regulatory impact assessment (RIA), inefficient communication among stakeholders and information system crashes.

The objectives of any regulatory system will not be achieved unless risks are well managed. As the above examples show, however, most such risks cannot be properly managed within an individual entity, be it a regulatory authority or a business. Their management instead requires collaboration among all the stakeholders in a regulatory system, including regulatory authorities, standardization and conformity assessment bodies, market surveillance authorities and economic operators. This collaboration should be based on common risk management processes that have been integrated into a regulatory system. One example of an initiative aimed at enhancing risk management collaboration is presented in the box below.

Aviation Safety Information Analysis and Sharing system

An industry/government initiative has been put in place by the United States to collect safety data across the aviation community. Named the Aviation Safety Information Analysis and Sharing (ASIAS) system, it integrates data from many sources to accomplish several objectives. First, data can help determine whether a risk that occurs with one operator is common to other operators. Then, safety professionals can develop mitigations that improve the entire system. Second, data can measure whether the safety initiatives have been implemented and are having the intended effect of improving safety. Ultimately, data analysis can uncover risks that no one has yet identified and allow the community to develop safety improvements.

Source: WEF (2010).

3.2 Existing analytical frameworks of risk management in regulation and business

The need for addressing risks through regulations has been raised frequently in connection with the economic crisis of 2008 and subsequent catastrophes, including the April 2010 oil spill in the Gulf of Mexico and the series of accidents leading to the Fukushima nuclear plant meltdowns in March 2011.

Numerous analytical frameworks have been developed to describe aspects of risk management in regulatory systems.

Regulatory impact assessments (described in more detail in paragraph 5.2 below) offer a tool for identifying the costs and benefits of a regulation, as well as the respective risks entailed in not regulating.

The OECD analytical model focuses on the concept of risk policy (OECD 2010b p. 19). It divides this into three sequential phases, all of which are linked to communication: risk assessment, which involves forecasting the probability and consequences of hazards; risk management, which is about choosing and implementing risk management strategies; and risk review, or evaluating the effectiveness of policy solutions. The “Recommendation of the Council on Regulatory Policy and Governance” (OECD, 2012) further notes that “Risk assessment, risk management and risk communication are part of a cycle of responsive regulation”. The OECD

recommendation also encourages governments to make effective use of regulation to achieve better social, environmental and economic outcomes. This echoes expectations expressed by the civil society, as expressed at events such as the 2011 International Regulatory Reform Conference organized by the International Regulatory Reform Network which stressed the need for a holistic approach*.

The International Risk Governance Council (IRGC, 2006) introduces the risk governance framework and describes its main phases: pre-assessment, risk appraisal, risk characterization, risk evaluation and risk management. The first four phases are similar to what is described as risk assessment in OECD (2010). IRGC (2006) elaborates, citing the decision to abandon development of a specific technology, or taking action to fully eliminate a given risk, as risk avoidance strategies. Risk transfer allows instead the risk to be passed on to a third party. Risk acceptance as a management option essentially means taking an informed decision to do nothing about a risk and assuming full responsibility for both the decision and its consequences. Finally, risk management through risk reduction can be accomplished by many different means.

A number of legislative texts are based – at least implicitly - on these tenets, and we will give many examples in the following chapters. Among these, the New Legislative Framework (NLF) of the European Union (European Union 2008b) notably turns some of the steps of the risk management process within a regulatory system into requirements. It calls for market surveillance authorities to perform risk identification to determine which products present a risk, evaluate those risks, and cooperate with economic operators to develop and implement the appropriate responses. If an importer, distributor or manufacturer determines that a given product presents a risk, it also has an obligation to inform the market surveillance authority.

3.3 Key principles of risk management in regulatory systems

The analytical frameworks quoted in the last paragraph were among those used to develop a reference model on which the UNECE recommendation on risk management in regulatory frameworks (UNECE, 2011b) is based. The model, which describes how risk management can be applied within a regulatory system to help achieve regulatory goals, is presented in the following pages.

Earlier, we characterized a regulatory system as a set of processes – with specific objectives, inputs and outputs – that is geared to mitigating risks. These processes include setting regulatory requirements and performing pre- and post-market controls. In this publication, we look at these processes in relation to those that are performed by economic operators to create economic value.

The concept of a regulatory system is not new. For example, the World Bank Handbook for evaluating infrastructure regulatory systems (World Bank, 2006) states that “any evaluation of regulatory effectiveness must examine the entire regulatory system – not just the characteristics and actions of the formally designated regulatory entity”. It presents “detailed, practical guidance on how to conduct quick, mid-level, and in-depth regulatory evaluations of existing national and state or province-level regulatory systems through structured case studies”.

* Using the elephant as a metaphor for a regulatory system, conference participants emphasized that “so many debates have just focused on mere parts of the elephant’s body instead of focusing on problems, questions and ideas in a holistic manner” (see www.irr-network.org/). OECD (2012) similarly calls for a commitment “at the highest political level to an explicit whole-of-government policy for regulatory quality for a “whole-of-government” approach to regulatory reform”.

The Handbook focuses on “economic regulation of commercial sector enterprises, whether publicly or privately owned”.

A key feature of any system is that the whole is worth more than the sum of its parts. Regulatory processes – such as developing regulations, assessing conformity with regulations and reviewing the existing stock of regulations – need to be designed to function as a single system. Adequate, justified and proportionate regulatory requirements will not meet the goal (of increasing safety, for example) if conformity to regulations is not assessed or is assessed poorly. Strong conformity assessment measures, in turn, will have no value if the requirements are inadequate or disproportionate.

UNECE (2009a) describes the roles of regulatory system stakeholders in addressing risks. Those roles were discussed in detail at the International Conference on Risk Assessment and Management, organized by the UNECE Working Party on Regulatory Cooperation and Standardization Policies (UNECE WP.6) in November 2009. The conference addressed the principal components of risk management within the context of the activities of policymakers, intergovernmental organizations, standardization bodies, technical regulation authorities, conformity assessment bodies and businesses. It considered actual situations in which regulatory stakeholders were responsible for the treatment of a particular type of risk and in which they performed various risk management functions within their respective regulatory systems. The conference outcome contains examples of regulators’ development of risk mitigation tools, such as standards.

The concept of a regulatory system enables us to analyse both the “what” and the “how” of regulatory activities. This type of analysis is needed to address problems associated with regulation. Such problems include situations where regulatory requirements are inadequate, do not fit the objectives of the regulatory system, contradict one another or are not enforced, or any combination thereof. A holistic approach to regulation is an important tool also because changes in one regulatory process can affect other regulatory processes. Without a model of the system as a whole, it is difficult to predict and manage the overall effects of reforms.

The coherent application of risk management to regulatory work is intended to develop a well-balanced system, as opposed to one that veers between two extremes:

- (a) Excessive or over-regulation, i.e., regulations that are too stringent with respect to the risk they set out to address, and
- (b) Insufficient regulations, which fail to address risk and unnecessarily or inordinately expose citizens and economic operators

Respecting this principle ensures that risk management is not just applied within one regulatory authority or business process but is a central process underlying all regulatory activity.

The concept of risks as triggers for regulatory intervention and as measures of its proportionality is widely recognized and applied, as described in the following box:

Applying risk management to regulatory systems: some examples

Many regulatory stakeholders already apply risk management to ensure the proportionality of safety measures to risks. In the context of the agreements of the World Trade Organization (WTO) on sanitary and phytosanitary measures (SPS) and technical barriers to trade (TBT), the proportionality principle is reflected in the provision that measures taken by members should be “no more trade-restrictive than necessary”. Under the SPS Agreement, every trade

restriction needs to be based on scientific evidence of a risk to the life or health of humans, animals or plants. Under the TBT Agreement, measures can be justified more broadly on the basis of “legitimate government objectives”. In addition, under the SPS Agreement, all measures must be based on the Codex Alimentarius, the International Plant Protection Convention (IPPC) or the World Organization for Animal Health (OIE) standards. In case of deviation from these international standards, appropriate risk assessment is required. Under the TBT Agreement, the link between scientific evidence, international standards, risk assessment and the measures applied is defined more loosely. Whether this link could and should be reinforced in the context of the TBT Agreement so as to better guarantee proportionality between risks and regulatory responses has been the subject of discussion for many years.

Although the application of risk management tools to regulatory systems is relatively recent, it is already at the heart of many of the regulatory systems of the European Union (EU). European legislation in the fields of food safety, environment, technical regulation and others requires regulatory stakeholders to perform risk management functions. The Food Safety Regulatory System of the European Union, for example, based on Regulation 178/2002 (European Union, 2002), provides a very comprehensive description of risk management functions as they should be performed within the system. It also serves as a basis for harmonizing the national legislation of member States. That is why in this publication we use the food safety regulation as an example of how different risk management functions can be carried out within a regulatory system. A detailed analysis of exactly how this is done in this specific regulation, followed by important general conclusions, can be found in a recent paper on “Applying risk management concepts to the design of legislation” (Jachia and Nikonov, 2011a).

All of the functions of the risk management process presented below should be consistently described in legislation establishing a regulatory system. The legislation should also specify who is responsible for performing each task in the process.

The reference model for a risk-based regulatory system (see figure 3.1 below) lays out in detail the risk management roles of all the key actors in the regulatory process and shows how risk management functions can be incorporated in overall regulatory functions.

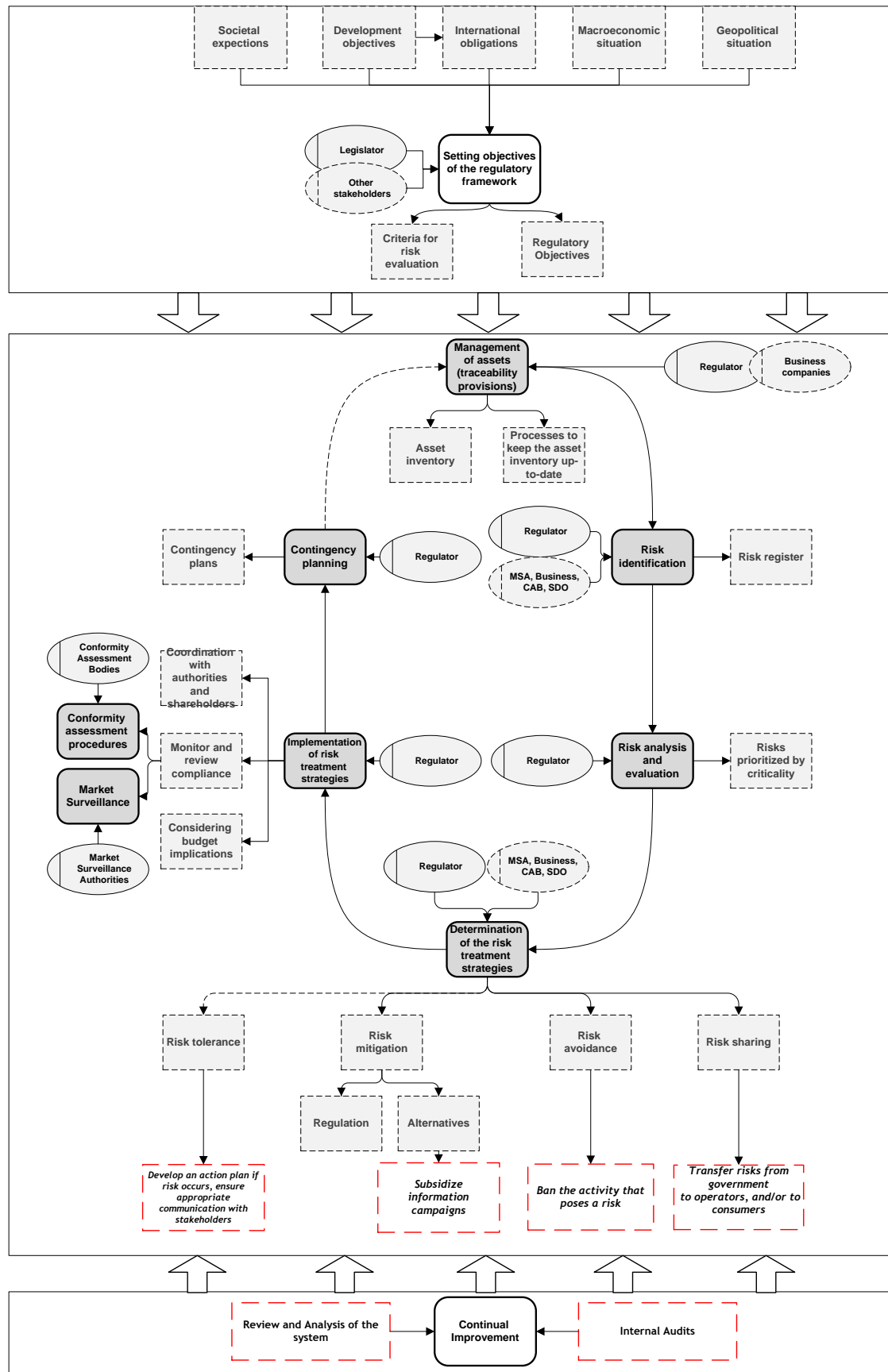
Implementing the model involves developing a timely and comprehensive management of risks. This should be a “stand-alone” process, which may – but need not necessarily – result in the development or review of a regulation.

The model shows how the following risk management functions are performed within a regulatory system:

- Setting the objectives of the regulatory system
- Management of assets (traceability provisions)
- Risk identification
- Risk analysis and evaluation: understanding the most important risks
- Choosing risk treatment strategies
- Implementing risk treatment strategies
- Contingency planning and crisis management (including developing a plan to deal with disruption-related risk)
- Monitoring, reviewing and improving the risk management process

Each of these functions is described in the following diagram and in the paragraphs below.

Figure 3.1 A risk-based regulatory system: a reference model



3.4 Setting the objectives of a regulatory system and the risk evaluation criteria

It is generally accepted that the objective of economic regulation is to prevent market failures. This objective can be defined within the broader context of a country's development and societal objectives. A good characterization of the objectives of a regulatory system can be found in President Barack Obama's Executive Order 13563, on "Improving Regulation and Regulatory Review" (United States, 2011). It describes the objectives of the national regulatory system as those of protecting "public health, welfare, safety, and ... environment while promoting economic growth, innovation, competitiveness, and job creation".

Similarly, the European Commission's Communication on Smart Regulation (European Commission, 2010) states that "markets ... serve a purpose which is to deliver sustainable prosperity for all, and they will not always do this on their own". It argues that "we must limit burdens for [businesses] to what is strictly necessary, and allow them to work and compete effectively". The objectives of sector-specific regulations are more precise. For example, Regulation EC/178/2002, which lays the foundations for the EU's food and feed system, states that the system should aim at a "high level of protection of human life and health" but also at providing "[equal] conditions for competition" (European Communities, 2002).

Based on these two texts, the objectives of a regulatory system can be formulated as follows:

1. To promote growth, innovation, competitiveness and job creation without creating unnecessary risks to welfare, safety, public health and environment, and
2. To protect public health, welfare, safety and environment without stifling growth, innovation, competitiveness and job creation

Although worded differently, these objectives are the same as those that underlie ISO 31000:2009 i.e., risk management strategies should protect value and at the same time maximize opportunities.

The EU food safety system (1)

The objectives of the system for providing food safety in the European Union, as set forth in the law (European Communities, 2002), include the following:

- not placing food on the market if it is unsafe ("food shall be deemed to be unsafe if it is considered to be: (a) injurious to health; (b) unfit for human consumption")
- providing a high level of protection of human life and health
- protecting the interests of consumers
- providing for the free movement of safe and wholesome food
- equal conditions for competition
- confidence in the decision-making processes underpinning food law, its scientific basis and the structures and independence of the institutions that protect health and other interests

Regulatory systems are complex cross-industry systems that bring together a broad range of stakeholders with their own motivations, values and perceptions. One of the challenges faced by regulators setting the objectives of a regulatory system has been referred to in IRGC (2006) as the “subjective perception of risks”, which is often accompanied by a “failure to adequately identify and involve relevant stakeholders”.

Assuming that there are always different perceptions of risks, a prerequisite for an effective risk governance framework is transparent and reliable mechanisms for consultations with stakeholders, especially at the early stages of regulatory activity. In the context of RIAs, policymakers are explicitly required to conduct extensive and wide-ranging public consultations. Consultations should include not only business and civil society, but also the different ministries and other public authorities involved.

In the United Kingdom, for example, a Code of Practice on Consultation was adopted in 2008, laying out seven consultation criteria detailing: the timing and duration of consultation exercises, the clarity and accessibility of consultation documents, the minimization of the burden and the need to provide feedback to consultees, and the need for a continual improvement of the consultation mechanisms (United Kingdom, 2008).

Regulatory objectives are also an important criterion in the ex-post evaluation of legislative texts and can be used in particular to evaluate redundancies in regulatory requirements.

Another important dimension of the objectives of a regulatory system is that they are closely correlated with a society’s tolerance for risks, and with the particular risk sensitivities that a country aims at protecting (such as risks that affect the disabled, the elderly and the young). This dimension is used by regulatory authorities in setting the criteria against which a risk is evaluated. There are many options for defining such criteria, and the responsibility for choosing among them should be clearly assigned.

Using an example from the shipbuilding industry – that will be developed in Chapter 5 - the objectives of the regulatory system would include:

- Protecting passenger safety:
 - minimizing accidents
 - minimizing the consequences of accidents
- Minimizing the environmental impact
- Avoiding escalating costs for businesses

These objectives could be used as categories for the consequences of a risk. Hence, for evaluating risks, a regulator should identify their impact on passenger safety (in terms of the number of accidents and their consequences), their environmental impact, and associated business costs.

When setting the objectives of a regulatory system, absolute safety should not be considered as a regulatory goal. Aiming at zero risks would lead to controls so widespread as to be ineffective. It would also not be desirable, because abandoning a new technology, for example, might incur even greater risks if that technology could result in advances in science or medicine that could have helped save lives. Bernstein (1996) provides the following explanation of the zero-risk concept:

“The scientist who developed the Saturn 5 rocket that launched the first Apollo mission to the moon put it this way: ‘You want a valve that doesn’t leak and you try everything possible to develop one. But the real world provides you with a leaky valve. You have to determine how much leaking you can tolerate.’”

Perhaps the most difficult task for a regulator is to develop appropriate criteria to decide which risks are acceptable, or tolerable. Taking into account the level of risk tolerance of the regulatory system’s stakeholders, regulatory authorities should establish, implement and maintain a process for determining, analysing, reviewing and monitoring a socially acceptable level of risk. Systematization of this process helps create a well-balanced regulatory system, as defined above.

IGRC (2009) identifies a number of risk governance deficits related to risk acceptance. These deficits can be grouped into two clusters. The first involves the definition of an acceptable level of risk, and the second concerns the necessary organizational infrastructure. One way to address these challenges is to design threshold numbers, although OECD (2009) states that “very few RIA guidelines, documents or government risk publications provide clear statements about the threshold between acceptable and unacceptable risks”. WHO (2001) suggests some approaches to defining acceptable risk, based on an arbitrary level of defined probability; on a level that is already tolerated; or on a level that public health professionals say is acceptable.

Another widely used concept in this context is the “precautionary principle”, a key tenet of European and other legal systems (see, for example, Commission of the European Communities, 2000), also enshrined in Principle 15 of the Rio Declaration (United Nations Conference on Environment and Development, 1992). According to that principle, if “an action or policy has a suspected risk of causing harm to the public or to the environment, in the absence of scientific consensus that the action or policy is not harmful, the burden of proof that it is not harmful falls on those who advocate taking the action”. In practice, regulatory authorities often refer to the precautionary principle when there is no available scientific evidence of a risk. Critics of the precautionary principle, however, contend that it could lead legislators to extend the scope of regulatory policies beyond desirable boundaries.

Risk management standards and best practice do not provide recommendations on how to define risk acceptance criteria, but they do offer insights into how to create processes that are necessary for efficient risk acceptance. The IEC/ISO 27001:2005 standard describes risk acceptance as a process with criteria as variables that can be analysed and changed. This calls for identifying processes for accepting risks and appropriately communicating decisions to stakeholders. The latter task – communication – is very delicate, for a number of reasons. It indeed involves an element of moral hazard, because it can signal the authorities’ priorities in the allocation of resources across sectors and across areas of responsibility (for example, as regards enforcement and monitoring of non-compliance in one sector of production).

It may well be that creating a system in which risk acceptance is, at the very least, well defined as an option can help structure the ongoing debate as to which risks are worth taking for society as a whole, and which are not. In business, for example, a manager’s decision to accept a high risk is a well-recognized option: even if the risk is high, it has to be accepted if the costs of mitigation are higher still. Risk acceptance involves an allocation of responsibilities for defining and approving risk acceptance criteria and for accepting the risks, developing contingency plans,

and so forth. This decision-making process should be adapted by regulatory authorities with the aim of developing sound risk acceptance criteria supported by an adequate institutional set-up.

3.5 Management of assets (traceability provisions)

Developing an asset inventory is the next function in the risk management process. Regulatory authorities should map out a process of communication and consultation for identifying key assets as objects or qualities that have value and that the system sets out to protect. Including traceability requirements for economic operators may – in certain sectors – facilitate the identification of assets.

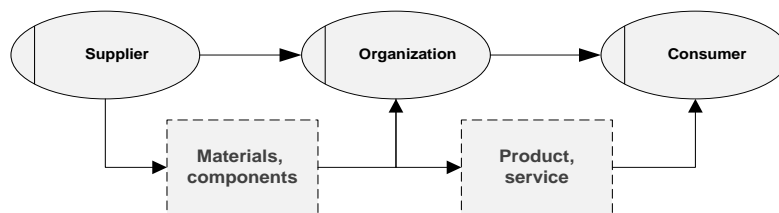
Traceability, a relatively new concept as applied within regulatory systems, has always been part of economic and social life. Figures of terracotta warriors created in ancient times were labelled with the names of craftsmen and can be traced back to their producers even today, throughout history, royal courts carefully checked and chose their suppliers.

Defined in the ISO 9000:2005 standard as “the ability to trace the history, application or location of that which is under consideration”, traceability means that any product on the market can be traced back along all the steps of its production chain. It allows regulatory stakeholders to get information on the original materials, components and processes used in production.

Regulatory stakeholders have an interest in ensuring traceability in supply chains. Consumers have always been concerned about the quality and safety of products and the origin of goods. Traceability allows companies to increase the stability and transparency of procurement and production processes. It helps regulators and market surveillance authorities take prompt and targeted action, such as withdrawing dangerous products from the market. Traceability is also an essential part of any system designed to fight counterfeit goods.

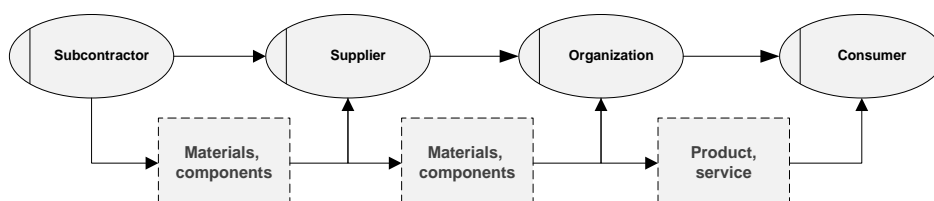
Traceability requirements are present in regulatory systems at various levels. Management system standards and managerial best practices, such as ISO 9001:2008 (the quality management system standard), require firms to provide the traceability of inputs used in their production processes within the supplier – organization – consumer chain.

Figure 3.2 Supplier-organization-consumer chain



ISO 20000:2005 (the international standard for information technology service management) takes the idea a step further, requiring that organizations be able to trace their products to the level of the “subcontractors of suppliers”:

Figure 3.3 Subcontractor-supplier-organization-consumer chain



In the area of feed and food, ISO 22005:2007, establishes the principles and requirements for designing and implementing a traceability system.

Traceability requirements in legislation are a key tenet of complex regulatory systems. The Food Safety Regulation of the European Union, for example, contains provisions and introduces mechanisms to achieve transparency in the food and feed chain. Likewise, in the United States, the Food Safety Modernization Act of 2010 also enhanced traceability of food on the market (United States, 2010). In another sector, the registration of chemical substances under the EU's REACH regulation (which deals with the registration, evaluation, authorization and restriction of chemical substances) is an example of a tool for achieving traceability and transparency (EU, 2006).

Traceability is a risk mitigation tool in its own right. Within a business entity, it ensures a consistent level of quality in supplies, a prerequisite for a high-quality end product. It also helps minimize the costs of incidents. For example, if an end product is compromised or does not meet quality requirements, an organization needs to be able to obtain full information on which components were used, where they came from and so forth so as to recall only those products whose components were faulty.

More generally, within regulatory systems, traceability helps to:

- (a) Protect consumers by minimizing the risks related to proliferation of dangerous products on the market
- (b) Enable accurate withdrawals of products from the market, when necessary
- (c) Achieve traceability within regulatory systems, which requires:
 - (i) Traceability of the production processes of businesses
 - (ii) Implementation of traceability tools by the regulator

Asset identification and classification, which can be achieved, inter alia, through traceability provisions, is an important preparatory step in the identification of risks. An asset can be identified as anything that has value for the regulatory system and that is needed to achieve its fundamental objectives. In other words, before trying to answer the question, “what are the threats?”, regulatory authorities must have a clear picture of what they are trying to protect. In this context, risk management is a way of protecting something that has value – an asset – and is therefore integral to the mission statement of any regulatory system.

Although risk is understood in IRGC (2006) as an uncertain consequence of an event or an activity with respect to something that humans value – a definition originally found in Kates et al. (1985) – in most of the risk governance frameworks (including ISO 31000:2009) this preparatory step is not explicitly addressed. But it is a crucial step, as the failure to properly identify the assets a regulator is setting out to protect may lead to regulatory failures. As the example below shows, in many sectors, management of assets is implemented by means of voluntary or compulsory registration (or reporting) of products and their components.

The establishment of a mandatory reporting system for nano-enabled products in commercial use across both the United States and the EU is considered essential for regulators to effectively manage the risks of nanomaterials. This is one of the main recommendations in the report “Securing the Promise of Nanotechnologies: Towards Transatlantic Regulatory Cooperation” by the London School of Economics and Political Science (LSE), the Environmental Law Institute (ELI), Chatham House and the Project on Emerging

Nanotechnologies (PEN) at the Woodrow Wilson International Center for Scholars.

Source: L. Breggin et. al. (2009)

There are thousands of different risks within any given regulatory system. One of the challenges regulatory stakeholders face is “failures to properly assess risks from the outset”, as identified in IGRC (2009). Creating an inventory of assets and then conducting a structured identification of risks beginning with those that affect the most critical assets helps reduce the likelihood of missing some important risks.

An assets inventory and its structure: an example

In an information security management system, an assets inventory entry might look like the following table:

Name	Confidentiality	Integrity	Availability	Criticality	Owner	Users
<i>Clients' database</i>	<i>High</i>	<i>High</i>	<i>High</i>	<i>High</i>	<i>Head of the sales division</i>	<i>Sales division</i>

In IEC/ISO 27001:2005, the main features of information assets that can be compromised by risks are confidentiality, integrity and availability. They are considered in determining the resulting level of criticality. This in turn allows an inventory to be developed with a ranking of organizational assets.

A similar inventory could be developed for a regulatory system. Once the assets have been identified, their critical features should be determined and incorporated into the table. If we think, for example, of railway transport as a system, then the assets are its tracks, staff, trains, etc. Classification guidelines should also be developed so that for each asset, the level of criticality is determined in a consistent manner.

The system of assets, their classifications and levels of criticality are key elements of any regulatory system. Because a risk mitigation measure taken to protect one asset may pose a risk to another asset, it is crucial to be able to forecast the interdependence of risks and of regulatory or non-regulatory responses. An up-to-date asset inventory is essential for this purpose, as are the processes required to keep the inventories up-to-date.

The EU food safety system (2)

The scope of the food safety system, as defined in the EU's food safety regulation (European Communities, 2002), is very broad and includes “all aspects of the food production chain as a continuum from and including primary production and the production of animal feed up to and including sale or supply of food to the consumer”. Risks that may affect human health (and that may have an impact on other areas specified in the objectives) may appear in any part of the food supply chain; but the sooner they are identified, the less impact they will have. The text explicitly states why this definition of scope was chosen: “Experience has shown that ... the inadvertent or deliberate contamination of feed, and adulteration or fraudulent or other bad practices in relation to it, may give rise to a direct or indirect impact on food safety”. The regulation introduces two main mechanisms for the identification of assets:

- Traceability requirements (the regulation calls for establishing “a comprehensive system of traceability within food and feed businesses”, since “experience has shown that the functioning of the internal market in food or feed can be jeopardized where it is impossible to trace food and feed”).

A traceability mechanism allows for assets identification “by request”. It requires “food and feed business operators [to] be able to identify any person from whom they have been supplied with a food, a feed, a food-producing animal, or any substance intended to be, or expected to be, incorporated into a food or feed”.
- Establishing a centralized system for collecting data. The second tool is a centralized “system for the collection and analysis of relevant data”. This system – a database registry of all substances and operators– is managed by the European Food Safety Agency.

3.6 Risk identification in regulatory systems

As previously mentioned, risks should be identified for each asset of an organization, starting with the most crucial ones. Regulators should cooperate with other stakeholders in identifying risks, as this makes the system more resilient by reducing the chances that certain risks may be overlooked.

All stakeholders in the system should be allowed to participate in identifying risks, for the following reasons:

- (a) Not only regulations but also voluntary standards help businesses and society deal with risk. Standards development organizations can provide key inputs for risk identification.
- (b) For market surveillance authorities, properly identifying the risks that may arise from placing products on the market is a prerequisite for developing timely and appropriate measures and ensuring marketplace safety.
- (c) Conformity assessment procedures act as risk mitigation tools by reducing the risk of placing dangerous products on the market. Conformity assessment bodies can spot risks that a regulator may not be able to identify.
- (d) Business operators may also inform the regulator about risks that, in their view, require regulatory intervention.

The EU food safety system (3)

The European Food Safety Authority (EFSA), which is responsible for risk identification within the food safety system, is required to “use all the information it receives in the performance of its mission to identify an emerging risk” (European Communities, 2002). This information, according to the legislation, may come from the following sources (of risk identification):

- Consumers, academia, other interested parties (“The Authority shall develop effective contacts with consumer representatives, producer representatives, processors and any other interested parties”).
- Business operators: there is a provision that “a food business operator shall immediately inform the competent authorities if it considers or has reason to believe that a food which it has placed on the market may be injurious to human health. Operators shall inform the competent authorities of the action taken to prevent risks to the final consumer”. This shows one of the roles of business operators in risk identification within the system. Both ensuring product safety and protecting consumers are defined in the text as the primary responsibility of economic operators.
- The rapid alert system, a notification system that was created because “recent food crises have demonstrated the need to set up an improved and broadened rapid alert system covering food and feed”. This system is a major source of risk identification, since “where a member of the network has any information relating to the existence of a serious direct or indirect risk to human health deriving from food or feed, this information shall be immediately notified to the Commission under the rapid alert system”.
- The Advisory Forum, which is run by the Authority and whose membership is open to representatives of competent bodies of the member States.
- Competent organizations designated by the member States: “The Management Board ... shall draw up a list ... of competent organizations designated by the Member States which may assist the Authority [in] identification of emerging risks”.

All risk identification methods listed in the previous chapter (section 2.4.2), such as brainstorming and interviews, can be used to perform this function. Ideally, this task should result in a common risk register.

3.7 Using the objectives of a regulatory system to evaluate risks

No matter what the source from which a regulator or other stakeholder learns of a risk, a mechanism should be in place to ensure appropriate follow-up through risk analyses and evaluation. Evaluation ensures that critical risks are dealt with in a timely manner.

Categories of impact in the context of regulation

In chapter 2 we presented several techniques for conducting risk evaluation. One approach we mentioned for prioritizing and comparing risks is to identify possible categories of impact and to

determine what is meant by “critical”, “medium” and “low” risks for each category. Within a regulatory system, the objectives of the regulatory system can serve as categories of impact. In the shipbuilding regulatory system, for example, the table of categories of impact might look as follows:

Category	Passenger safety	Costs for business	Environment
Critical consequences	At least one victim	More than \$10,000 in additional costs	CO ₂ emissions greater than X
Medium consequences	Traumas involving more than 20 passengers	Additional costs of \$5,000 - \$10,000	CO ₂ emissions less than X but greater than Y
Low consequences	Traumas involving less than 20 passengers	Additional costs of less than \$5,000	CO ₂ emissions less than Y

3.8 Available risk treatment strategies

Based on the results of the risk assessment, and acting in consultation with the system’s stakeholders, regulators choose an appropriate risk treatment strategy. Regulators can adopt one of the four strategies (tolerating, avoiding, mitigating or transferring a risk) presented in chapter 3. We will now focus on how these strategies can be implemented within a regulatory system.

In the regulatory context, tolerating a risk means that the regulators decide they are unwilling or unable to take measures to reduce the probability and expected impact of a risk. However, it is important that when a risk is tolerated, this is communicated to all interested parties appropriately and becomes an input to the contingency planning function of the regulatory agency and other regulatory stakeholders.

The resistance to accepting risks is apparently on the rise, partly because of the interplay of political and media processes. Most policymakers, who generally have short time horizons, would not want to be blamed for possible accidents during their terms and would prefer imposing red tape to limit hazards, thus eroding productivity in the long term.

Killer Trees

In 2008, the British Standards Institute proposed a new British standard on tree safety inspection, BS 8516. It recommended expert inspections of trees at least every five years (in addition to less expensive inspections more regularly). These inspections would be a “systematic and diagnostic process of visual inspection by a competent person (e.g. an arboriculturist) from ground level using binoculars, mallet and probe as necessary in order to gain sufficient understanding of a tree’s structural condition, so as to inform, where appropriate, re-inspection interval and management recommendations (risk control measures) including detailed inspection”. “Detailed inspection” involved aerial access to view upper parts of the tree and perhaps decay mapping equipment. The proposal was put out for consultation and generated enough controversy that it did not progress further. Trees can kill people when they fall, so there is a safety risk in having trees. On average, six people per year die in the United Kingdom as a result of accidents

involving trees. For a population of 60 million, that is an annual risk of 1:10 million. But if safety is an absolute, the risk is unacceptable, since it may result in death.

Source: Macrae, Donald (2011)

Risk intolerance has also been widely attributed to the interaction among societal stakeholders, including the media, civil society and lobbyists. One example of the outcome of risk intolerance can be found when tolerance levels for residues of contaminants on fruit and vegetables for human consumption are set to the lowest level that can be detected by measuring equipment. In the absence of risk acceptance criteria, the decision on the threshold limit is then based not on societal consensus, as represented by policymakers, but on scientific and technological developments.

The Risk and Regulation Advisory Council of the United Kingdom promoted a wide political debate on acceptable risk levels (RRAC, 2009). One of the conclusions that can be drawn from that United Kingdom debate is that regulatory and standardization activities should not be based on the technical feasibility of achieving a greater level of safety, but instead on a form of risk benefit analysis. The public is, however, apparently becoming more and more risk-averse, and the Government is being pressured to make regulations more stringent.

One explanation of this trend can be found in OECD (2010 c), which notes that “while the world is generally getting safer, public concern about risks ... even continues to grow, for a number of reasons”. These reasons include rising longevity, increasing wealth, advancing technology and other factors.

Avoiding a risk in the context of a regulatory system often involves banning activities or processes in which the risk might be incurred.

The EU food safety system (4)

Examples of a risk avoidance strategy are found in the EU’s food safety regulation. It states that:

“Where it is evident that food or feed ... is likely to constitute a serious risk to human health, animal health or the environment, ... the Commission ... shall immediately adopt one or more of the following measures, depending on the gravity of the situation:

- (a) in the case of food or feed of Community origin:
 - (i) suspension of the placing on the market or use of the food in question;
 - (ii) suspension of the placing on the market or use of the feed in question;
 - (iii) laying down special conditions for the food or feed in question;
 - (iv) any other appropriate interim measure;
- (b) in the case of food or feed imported from a third country:
 - (i) suspension of imports of the food or feed in question from all or part of the third country concerned and, where applicable, from the third country of transit;
 - (ii) laying down special conditions for the food or feed in question from all or part of the third country concerned;
 - (iii) any other appropriate interim measure.”

Transferring a risk within the regulatory context means sharing the responsibility for managing the risk with economic or social actors (such as families and businesses). Vaccinating children is a good example, as in many countries, and for some diseases, this is not mandatory but it is recommended.

Mitigating a risk in this context means developing a regulatory or non-regulatory response to reduce its probability and expected impact:

- A regulatory action implies not only developing a new regulation or revising an existing one, but also choosing appropriate conformity assessment procedures and market surveillance measures. The regulatory process that is required for implementing this option is described in the following chapter.
- Non-regulatory action, on the other hand, includes such options as educational or information campaigns, and subsidies or incentives to economic operators' activities. One risk mitigation measure is an information campaign which can involve a whole series of stakeholders, including regulatory authorities, government agencies, mass media and civil society.

The EU food safety system (5)

The use of full disclosure to minimize risks can be found in the EU's food safety regulation: "Regard shall be had ... to the information provided to the consumer, including information on the label, or other information generally available to the consumer concerning the avoidance of specific adverse health effects from a particular food or category of foods".

Risk-mitigating information campaigns: An example from Africa

Culturally specific, and culturally appropriate, information campaigns have been widely used throughout the world to mitigate health- and disaster-related risks, and the use of such campaigns is on the rise, thanks to social media and other new IT applications. The early warning systems set up by many national Governments to help prepare their citizens for hurricanes, cyclones, earthquakes and tsunamis have averted, or mitigated, the impact of these disasters. Campaigns to discourage the use of tobacco, drugs and alcohol are also common.

Campaigns to raise awareness of the risk of spreading HIV/AIDS through unprotected sexual activity have proven highly successful in changing the behaviour associated with the spread of the disease. They are also an excellent use of non-regulatory action to mitigate risks, as shown by the following example from Uganda (USAID, 2002). HIV prevalence there fell considerably, which has been largely attributed to the country's behaviour change communication strategy, launched nationally in 1986. While epidemiological, socio-cultural and political factors also contributed, in this case "HIV knowledge, risk perception, and risk avoidance options" were crucial.

The study concludes that "although we may never fully know 'what really happened in Uganda,' the experience there and in other countries that have achieved some success suggests that a comprehensive behaviour-change-based strategy, ideally involving high level political commitment and a diverse spectrum of community-based participation, may be the most effective prevention approach".

CFCs and ozone depletion

In the 1930s, when chlorofluorocarbons (CFCs) were first employed on an industrial scale, a lack of comprehensive scientific knowledge made it impossible to anticipate that these chemicals would affect stratospheric ozone. Rather, they were considered non-toxic and stable. However, once scientists made the discovery in 1974 that the breakdown of CFCs in the stratosphere was causing the depletion of stratospheric ozone (Molina and Rowland, 1974), efforts to monitor these consequences of CFC production were quickly mounted. Indeed, monitoring of anthropogenic CFC emissions and of ozone loss and recovery has been carried out systematically and carefully since the late 1970s, using ever more sophisticated technologies. The discovery of the ozone “hole” over Antarctica in 1985 heightened the already-growing international concern about ozone depletion.

In 1987, the Montreal Protocol on Substances that Deplete the Ozone Layer was signed. It entered into force two years later, leading to regulated production and a scheduled phasing-out of ozone-depleting substances. As a result of the Protocol’s regulations, the combined levels of ozone-depleting gases in the stratosphere decreased substantially from their peak values of 1992-1994 (WMO et al., 2007). Although emissions reductions for many ozone-depleting substances have been significant, atmospheric concentrations decrease much more slowly because of the long atmospheric lifetimes of some of these compounds, which can be 50-to-100 years. It is expected that because of the “resounding success” of the Montreal Protocol, CFCs and other harmful emissions could fall below the levels that produce an ozone hole by around 2070 (Hansen, 2007).

To ensure that this goal remains realistic and that actions continue to be effective, continual monitoring of compliance with the Protocol, of emissions levels, and of ozone depletion and recovery must continue.

Source: IRGC (2009)

3.9 Implementing risk treatment strategies

Regardless of the strategy chosen, implementing risk management treatment in a regulatory system requires monitoring compliance and evaluating the effect of the treatment on other regulatory processes, stakeholders and areas of activity. This involves:

- (a) Integrating regulatory and other risk management measures with existing processes
- (b) Establishing coordinating mechanisms among competent authorities and stakeholders
- (c) Giving guidance and establishing an appropriate budget for the institutions responsible for monitoring compliance (conformity assessment and/or market surveillance authorities)
- (d) Deciding on penalties for non-compliance

Choosing and implementing a risk treatment strategy might yield the following table entry:

Example of an entry table for a risk treatment strategy

Risk	Measure	Costs for various stakeholders	Responsible party	Deadline	Regulation No.
Inappropriate consumption of food	New labelling requirements	\$100,000 for the regulator, \$10 per product type for operators	Department	X	X

The following parameters would then need to be determined for each risk within the system: what to do with it, how much the related risk treatment will cost, who will implement the measures and when they must be implemented.

The development of an integrated risk treatment plan will help in understanding the interrelated nature of risks and in avoiding controversial measures. An agreed methodology will provide transparency and a clear division of responsibilities for risk assessment and risk management.

If a risk mitigation strategy is chosen and a regulation becomes a means of implementing it, all the regulatory processes that apply in the country's regulatory system will be carried out. A model of these processes - from the development of a regulation to the ex-post analysis processes – is presented in chapter 5.

3.10 Crisis management in regulatory systems

As noted earlier, technical regulation, conformity assessment and market surveillance play a crucial role in preventing and addressing crises in various fields. All regulatory stakeholders, including economic operators and consumers, share an interest in developing and applying tools that allow crisis situations to be effectively anticipated and, if necessary, resolved. In many cases, however, crises have led to the imposition of disproportionate regulations. To be effective, crisis management should be an integral function of the risk management process of any regulatory system: effective preparedness and/or response to crises requires systematic management of risks, and vice versa (Jachia and Nikonov, 2011b).

Since there are some risks that are unavoidable and almost impossible to forecast, and there are also some risks that are accepted within a regulatory system, regulators should prepare a plan of what is to be done if the harm associated with the risk occurs; who should act; and how. The need for contingency plans is widely recognized, but such plans will be efficient only if they exist in a system in which contingency planning is an integral part of the risk management treatment. To better integrate crisis management tools into regulatory practice, regulatory authorities and other stakeholders can apply the UNECE Recommendation “Crisis Management in Regulatory Frameworks”. This recommendation provides guidance on which functions should be embedded into regulatory practice in order to increase crisis preparedness and the resilience of regulatory systems.

The main phases of crisis management include preparation for a crisis, stabilization, continuing critical functions, recovery and follow-up.

Regulatory authorities should recognize that situations which are beyond the capacity of normal organizational structures and processes require adequate resources and prior planning in accordance with available international best practice. They should thus design the crisis management function so that it provides effective coordination of the actions to be taken in a crisis situation by various stakeholders, including conformity assessment bodies, market surveillance authorities, economic operators and consumers. The way this function is organized depends on the internal and external context of the regulatory system, available resources, regulatory objectives, communication technologies and other factors.

A crisis management unit (or any other form of assigning responsibility for crisis management) that is functioning within a regulatory system should be endowed with the necessary resources, which may include:

1. Access to emergency funding
2. People, skills, experience and competence
3. Tools, methods and supporting infrastructure for managing a crisis
4. Communication systems
5. Information and knowledge management systems

Contingency planning is one of the primary tools for crisis management. Regulatory authorities should establish contingency plans and build contingent capacity that can be quickly released during a crisis as a tool for reducing the impact of a risk should one occur. Regulators, in coordination with other stakeholders, should develop, test and implement:

- Generic contingency plans with general responses for risks, whether or not they have been identified, so as to allow for effective responses in the early hours of a crisis
- Specific contingency plans, where appropriate, for risks that have been identified and processed within the system

The EU food safety system (6)

The EU's food safety regulation calls for crisis management "where the Commission identifies a situation involving a serious direct or indirect risk to human health deriving from food and feed, and the risk cannot be prevented, eliminated or reduced by existing provisions".

The crisis management function is implemented in the EU's food safety system in the following manner:

The Commission, in close cooperation with the Authority (the EFSA) and the member States, draws up a general plan for crisis management in the field of food and feed safety. The plan specifies the types of situation involving direct or indirect risks to human health; the practical procedures necessary to manage a crisis, including the principles of transparency to be applied; and a communication strategy.

In a crisis situation, as defined above, the Commission immediately notifies the member States and the Authority and sets up a crisis unit. The Authority participates in the unit and provides scientific and technical assistance as necessary.

As in the business environment, the Commission is responsible for contingency planning and for

developing the procedures to be applied during a crisis: “These organizational procedures should make it possible to improve coordination of effort and to determine the most effective measures on the basis of the best scientific information. Therefore, revised procedures should take into account the Authority’s responsibilities and should provide for its scientific and technical assistance in the form of advice in the event of a food crisis.”

Australia/New Zealand standard AS/NZS 5050:2010 on *Business continuity – Managing disruption-related risk* provides a set of recommendations on developing contingency planning. In addition, regulatory authorities should prepare communication and consultation processes as a part of crisis management in order to:

- Build awareness, confidence and understanding of crisis management processes by regulatory system stakeholders
- Effectively exchange information and consult with stakeholders in crisis situations, in particular to provide information to stakeholders in the early hours following a crisis
- Encourage, where appropriate, the use of opportunities provided by alternative media

Regulatory authorities should ensure that appropriate mechanisms are established in a crisis situation for the following, at a minimum:

- Placing immediate focus on affected individuals
- Launching reliable data collection processes
- Activating a crisis management team (which may include a subject expert, top management, professional crisis managers, affected individuals, etc.)
- Ensuring follow-up to the crisis

In ensuring follow-up, regulatory authorities should gather relevant data and analyse the causes of the crisis and the effectiveness and relevance of actions taken as part of the immediate response. Adoption and continuation of regulatory measures related to particular crises should be subject to the normal review processes.

Many risk governance deficits arise in situations where risks (whether expected or unexpected) do eventually occur. As already stated, although contingency planning is an important function of the risk management process, it is missing from many risk governance frameworks.

Better crisis management has value not just in and of itself: it can also help save lives and assets and have a positive impact on the regulatory system as a whole, as it can enhance public trust and ensure that regulatory action is not taken as a hasty response to a risk.

3.11 Monitoring and review

Regulators or other interested parties should also have in place processes that ensure the continuous improvement of the whole regulatory system. These may include performing regular internal audits and analysing and reviewing processes and methodologies that function within the system. The purpose of these activities is to enhance the efficiency of process interfaces and to develop common understanding of regulatory system policy among all the system’s stakeholders.

Building organizational capacity for risk management is a key task of the regulator. As noted above, this requires a systematic approach to the management of risks within a regulatory system. An important element to consider in designing a regulatory system is a regular high-level methodological review of the system as a whole, its methodologies, processes and efficiency.

Such a review should go beyond the evaluation of current risk treatment strategies. It should include a comprehensive analysis of risk management processes and methodologies and should attempt to identify opportunities for improvement. Errors in the risk management methodology can lead to systemic errors. The implementation of management review is something that regulatory systems can learn from management system standards (such as ISO 9001:2008), which would allow regulators to embed within the system mechanisms for continuous improvement that are necessary for increasing efficiency and developing a coherent risk policy.

3.12 Application of the model

Function-by-function implementation of the model presented in figure 3.1 will require the participation of all the institutions involved in a regulatory system, including regulatory authorities, standardization bodies, economic operators, conformity assessment bodies and market surveillance authorities. Implementation is intended to:

- Enable regulatory authorities to establish a risk language that is shared by all regulatory system stakeholders and a common risk management process within a regulatory system
- Establish effective mechanisms for performing accurate cost-benefit analysis
- Enable economic operators to participate more actively in regulatory processes and to call the attention of regulatory stakeholders to risks that economic operators cannot manage on their own
- Enable standardization bodies to ensure that their activities address the most critical risks across regulatory systems
- Enable conformity assessment bodies and market surveillance authorities to ensure that their activities and action plans are consistent with the objectives and expectations of other stakeholders
- Ensure that adequate funding provisions are made for each of the stakeholders to perform its tasks efficiently and effectively

Broad application of this model will enhance coordination among stakeholders at the national, regional and international level. It will also lead to a more consistent and systematic application of risk management tools in regulatory work.

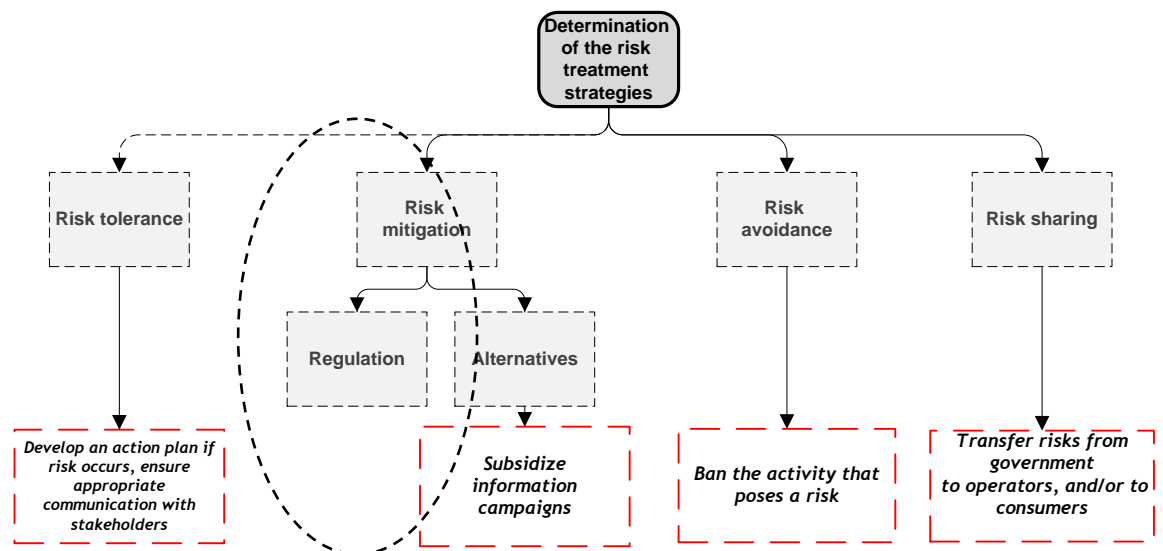
4 Regulation as a risk mitigation tool



complemented by voluntary standards and norms, as key tools for managing risks in the regulatory system as a whole.

In the previous chapter we described a methodology for the application of risk management tools to the needs and goals of a regulatory system. The model presents laws, administrative measures and technical regulations,

Figure 4.1 Regulation as a risk mitigation tool



From the risk management standpoint, developing a regulation is only one possible outcome of the more general risk management process that runs through a regulatory system. Regulation is nonetheless one of several major risk mitigation tools available to policymakers.

The quality of the process for developing and implementing a regulation largely determines how effective it will be as a risk treatment strategy. This chapter sets out to describe the process of developing regulations and ensuring compliance with them in simple and general terms. Our focus is mainly on a subset of regulations, or technical regulations, which are the various requirements that authorities set for products and production processes (such as labelling requirements, safety measures for operators, requirements on energy efficiency, etc.). As we will see, developing and implementing technical regulations is becoming increasingly complex as products become more sophisticated and as the ability of the average user to assess their quality gradually lessens or even disappears altogether. As such, it requires the coordinated actions of a number of stakeholders.

4.1 What is regulation?

Regulation is a very broad term. The World Bank (2006) defines it as “government-imposed controls on business activity”. Sunstein (2011) explains that “the term ‘regulation’ covers a great deal of territory [and] can refer to efforts to reduce air pollution; to safeguard against terrorist attacks; to protection against discrimination on the basis of religion or sex; to consumer protection; to rules to protect worker safety”. Mattli and Woods (2009) define regulation more broadly as “the organization and control of economic, political, and social activities by means of making, implementing, monitoring and enforcing [of] rules”. Baldwin (1999) suggests using the word “regulation” “in the ... sense of a specific set of commands – where regulation involves the promulgation of a binding set of rules to be applied by a body devoted to this purpose”; as “a deliberate State influence – where the regulation has a more broad sense and covers all State actions designed to influence industrial or social behaviour”; and as “all forms of social control or influence”.

In *Regulatory Policy and the Road to Sustainable Growth*, the OECD (2010a) explains that “a regulation may be defined as any instrument by which governments, their subsidiary bodies, and supranational bodies (such as the EU or the WTO) set requirements on citizens and businesses that have legal force. The term may thus encompass a wide range of instruments: from primary laws and secondary regulations to implement primary laws, subordinate rules, administrative formalities and decisions that give effect to higher-level regulations (for example, the allocation of permits), and standards”. The OECD also includes “soft law” in the term.

Many regulations are introduced in response to specific risks; environmental legislation, for example, has been passed to mitigate risks to health from the emission of toxic substances into the atmosphere, water and soil. Of course, regulations may also be introduced for purposes unrelated to risk, such as creating a conducive environment for investment or facilitating trade through the establishment of portals or single windows. While we will be broadly addressing regulations, our main focus is technical regulations that have been introduced to mitigate risks, whether directly or indirectly.

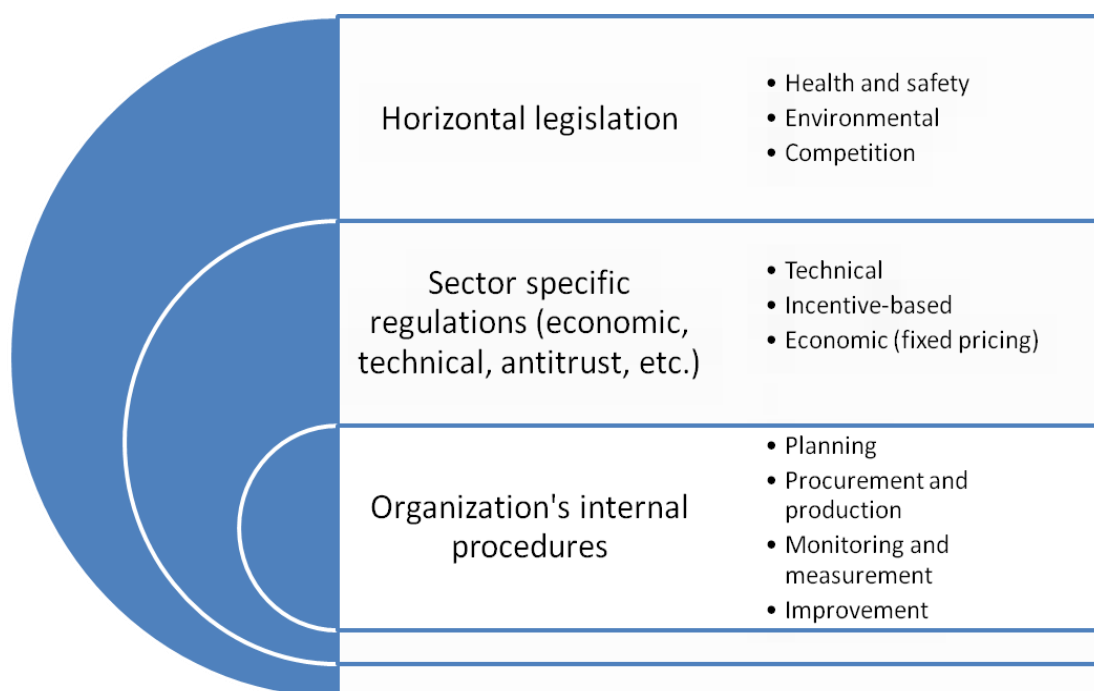
4.2 Assessing the consistency of the regulatory portfolio

When a new regulation is introduced to mitigate a risk, or to serve another regulatory goal, it will be added to a portfolio of regulations with which economic operators and civil society must comply. Complying with regulations, and proving such compliance, is a major business cost. It has also become an important factor of business competitiveness across countries.

One of the most frequent complaints of businesses is that regulations contradict one another. For a regulator, it may be useful to take a look at the effort of compliance from the business viewpoint. Figure 4.2 below may be of help. Businesses are typically concerned by three layers of their regulatory environment:

- Horizontal regulation
- Sector-specific regulation
- The business’s governance framework and management procedures

Figure 4.2 Regulation portfolio of an economic operator



Horizontal regulation

The first layer contains horizontal requirements with which organizations from different sectors must comply. For example, the horizontal sector of the EU environmental legislation covers “various matters which cut across different environmental subject areas, as opposed to regulations which apply to a specific sector, e.g. water or air” (European Commission, 2008). Similarly, all organizations have to comply with occupational health and safety regulations, no matter which sector they operate in.

Sector-specific regulation

The second layer contains economic and technical requirements for specific economic sectors and products. Examples include regulations in the areas of food safety (such as the above-mentioned food safety regulation of the European Union), finance (e.g. Central Banks’ regulations) and chemical products (e.g. the REACH regulation of the European Union).

Internal business governance and managerial procedures

All organizations have their own “regulatory” systems of internal rules, commonly referred to as “management systems”, which comprise the third layer of the business regulatory environment. Such systems encompass all the mandatory requirements of the first two layers but also an organization’s own requirements (related to the quality of products and services, and business processes). These requirements – often based on international standards like ISO 9001:2008 – determine an organization’s competitiveness and may therefore be stricter than the mandatory requirements. They are embedded in the organization’s processes, which, in keeping with a de facto world management system standard, follow the “plan-do-check-act” cycle. These processes include planning, design and development of products and services, procurement, production and service provision, sales and shipping, and so forth.

Interrelationship among different layers of regulations

Regulations that apply to business (with each layer of a regulation containing a substantial number of requirements) also have an impact on one another. This should be taken into account whenever a new regulation is introduced or an existing regulation revised.

As was pointed out earlier, ideally, regulations should be mutually reinforcing, but this is not always the case. Regulations that are clustered within one business regulatory space can be:

- (a) Independent: i.e. the new regulation has no influence on the impact of other regulations.
- (b) Complementary: the new regulation helps achieve the objectives of another regulation (e.g. a ban on smoking in cafés and higher taxes on cigarettes).
- (c) Contradictory: the new regulation prevents the objectives of other regulations from being met. For example, a technical regulation can easily create a monopoly (if there is only one organization that is able to comply with the new standard), even if antitrust regulation is in place.

The regulatory guillotine

The “guillotine” aims at reviewing a large number of business-related regulations, and eliminating those no longer needed without lengthy and costly legal action. It works like this. The Government instructs all ministries and agencies to draw up inventories of their regulations by a certain date. As the lists are prepared (involving consultation with the private sector and oversight from a central body), unnecessary, outdated, and illegal rules are eliminated. Combining all the ministries’ and agencies’ lists creates a centralized list. At the deadline, any regulation off the list is automatically cancelled without further legal action. The list becomes a comprehensive registry of all regulations in force, and serves as the legal database of regulations for purposes of compliance.

Source: Impact Alliance (2010)

The 2011 US Presidential Order referred to earlier (United States, 2011), which sets out to improve the quality of the American regulatory system, starts from the observation that “some sectors and industries face a significant number of regulatory requirements, some of which may be redundant, inconsistent, or overlapping”. In May 2012, another Executive Order on “Identifying and Reducing Regulatory Burdens” strengthened and broadened the first, to “promote public participation in retrospective review, to modernize our regulatory system, and to institutionalize regular assessment of significant regulations” (United States, 2012b).

4.3 Types of regulations that can be used to mitigate risks

Various economic theories, analytical frameworks and methodologies provide the background for regulatory action in specific domains, including the extent to which the economy should be regulated, the means available to authorities to address market failures, and the setting of tariffs and regulated prices for utilities.

Figure 4.3 sets out a possible categorization of different types of regulation to which we will refer later on. Regulations can be direct or indirect. Indirect regulations are an attempt to influence behaviour by changing the parameters used by economic and social actors when making decisions. One example is price incentives and taxes, such as taxes on cigarettes to discourage smoking. Direct regulations, on the other hand, are a Government’s attempt to control

behaviour directly by imposing specific characteristics or limits on products and production processes.

Figure 4.3 Types of regulations



There are three broad families of direct regulations: those that are introduced to protect competition (antitrust regulations); economic regulations; and regulations aimed at protecting health, safety and the environment and at responding to other societal concerns.

4.4 The structure of the regulation development process

A number of publications set out guidelines for the “how” of regulation and regulatory reform. OECD (2010a) states that “if regulatory policy is to support economic and social renewal, its core institutions and processes [should include] a strengthening of evidence-based impact assessment to support policy coherence; institutional capacities to identify and drive reform priorities; and not least paying more attention to the voice of users, who need to be part of the regulatory development process”. It also calls for “reviewing the role of regulatory agencies and the balance between private and public responsibilities for regulation with a view to securing accountability and avoiding [regulatory] capture” or corruption and renewing “emphasis on

consultation, communication, co-operation and co-ordination across all levels of government and beyond, including not least the international arena”.

To mitigate risks effectively, the regulatory process should provide:

1. A set of requirements, which can be tariffs, technical requirements, price regulations, etc.
2. When appropriate, provisions for pre-market controls: This could consist of processes that allow only those who meet the requirements to operate on the market, and could take the form of certification or licensing.
3. Organization of post-market controls: This could comprise processes that remove non-conforming products or services from the market, which could be referred to as supervision, market surveillance or oversight.

Many crises occur because of inadequacies in one of these three core elements. Mattli and Woods (2009) contend that the recent financial crisis can be explained by “inadequate regulation that generated a mismatch between private reward and public risk; and failure of regulators to comply with their supervisory duties” (post-market control). In the case of the 2010 Gulf of Mexico oil spill, some experts have argued that these two factors were compounded by the inadequacy of British Petroleum’s oversight processes.

A model of a regulation development process is presented in the figure 4.4 below.

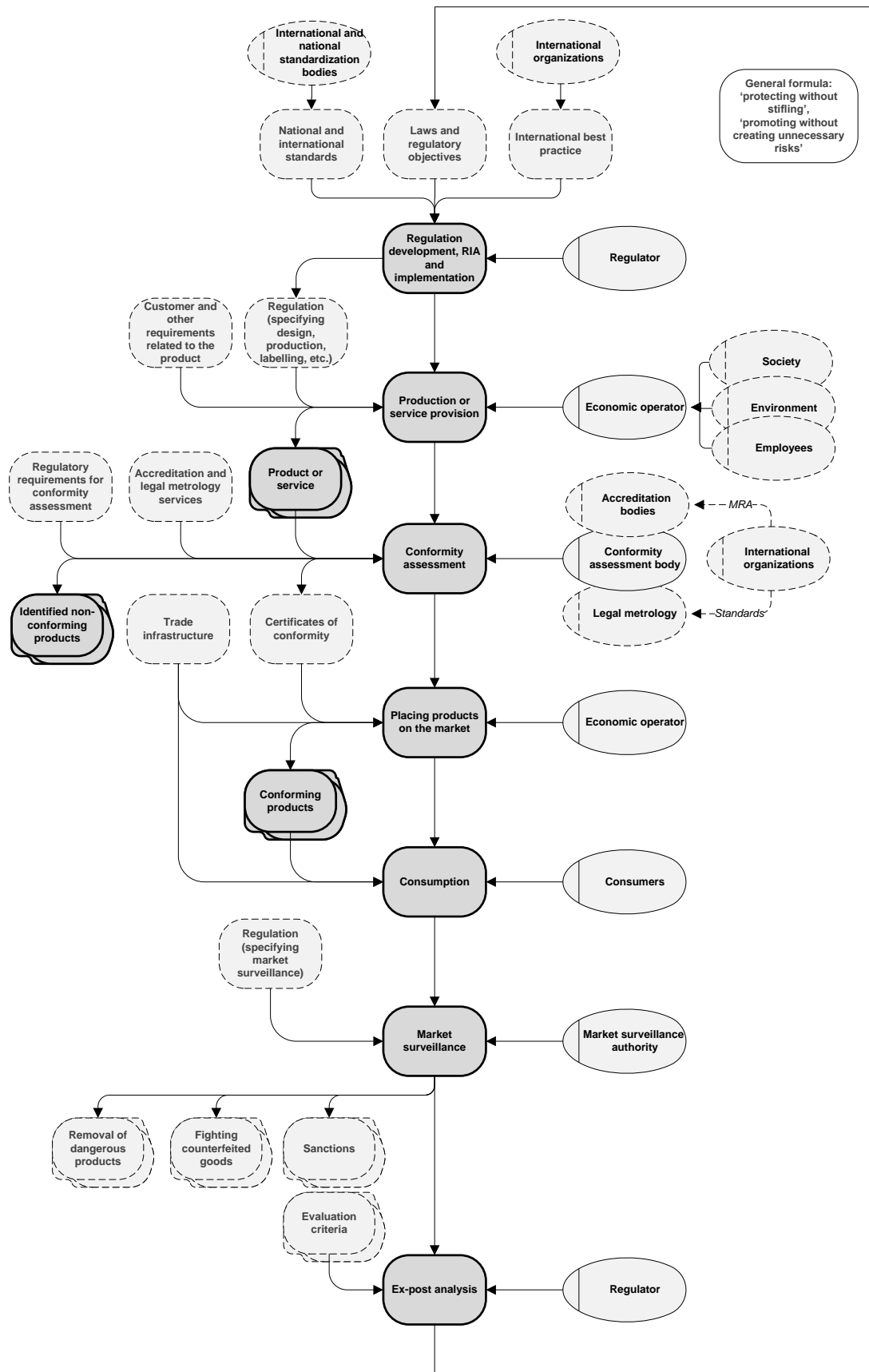
The figure details the main steps of the regulatory process, including the definition of objectives. It also sets out the inputs and outputs of each step in the process with reference to the participating stakeholders.

The first step is **development, assessment and implementation of a regulation**, which sets the rules for all economic operators. These rules, along with market demand for the product and other factors, provide an input to **production or service provision**. Performed by an economic operator, these processes create economic value. However, they may also bring risks to other stakeholders.

Before products and services are placed on the market, the regulatory system ensures that they meet the requirements specified in the regulation by means of **conformity assessment** processes (pre-market controls). In some cases (depending on the level of risk of a product), such processes result in the issuance of certificates that allow economic operators to start **placing products on the market** (the next block in the model). The objective of the processes is to ensure that only compliant products are released for **consumption**.

However, no conformity assessment can guarantee that it is only compliant products that are placed on the market; such assessment must be followed by **market surveillance activities** (such as inspections) by competent authorities as a form of post-market control. Market surveillance is intended to identify non-compliant goods and – if the non-compliance is serious – to remove them from the market. Sometimes it is possible to bring products into compliance (for example, businesses may be required to meet previously missing labelling requirements). If non-compliance does not pose a risk to consumers, market surveillance authorities may also limit their action to ensuring that the next batch of products which is placed on the market is compliant. In other cases, they may impose sanctions on non-compliant businesses. Collaboration with Customs is crucial to ensuring that not only products which originate from the Customs territory but also imported products are in conformity with a country’s regulatory requirements.

Figure 4.4 Structure of a regulatory system: a reference model



The results of market surveillance activities and other aspects of regulation are assessed by regulators during the **ex-post analysis**, which results, if necessary, in changing the regulation so that the cycle begins anew.

In the next chapter we present a case study to show how these steps can be implemented in practice and provide a detailed description of how they function.

It is interesting that the observations and recommendations we make about technical regulations for regulatory systems can generally be used to evaluate other systems, such as financial systems. Technical regulations are in fact a complex regulatory subsystem with respect to both the “how” (substance) and the “what” (processes) of regulation. Regulatory substance is sophisticated because of the large number of parameters that must be regulated (certainly exceeding the minimum-quality-of-service standards). Regulatory processes are similarly complex because of the need to assess conformity with a large number of parameters and to appraise the physical damage associated with failure to conform to the requirements.

5 How does regulation work in practice? An example

Following on our discussion of the structure of a regulatory system (figure 4.4), we will now focus on the roles of various stakeholders in regulation and show “who does what” when



the development and implementation of a regulation is chosen as a risk mitigation tool. Rather than providing an exhaustive description of all functions, which would not be possible even in a series of publications, we will use an example – an imaginary case study – to present the most interesting aspects of each of them.

All of the steps in regulation are deeply intertwined. Like all models, the model in figure 4.4 is a simplification of reality, as most of the linkages cannot be illustrated. Another simplification is that the model depicts these processes as consecutive, whereas in practice, of course, many of them function simultaneously. Still, it does create a useful framework for analysing regulation.

To enliven the description of regulation as a risk mitigation tool, in a series of boxes we will consider the imaginary case study of a company that has received an order to build a cruise ship. We will see how the regulatory processes impact shipbuilding and operating in order to make ships safe, while also ensuring the sector’s competitiveness.*

Case study: building a cruise ship (1)

As stated in Mattli and Woods (2009), “The sinking of the Titanic, in 1912, exposed the risks posed by increasingly large steamships and triggered the setting of an agenda for regulatory change”. Recent accidents, such as the Costa Concordia’s will likely lead to a repeat in this regulatory cycle.

In our example – and in real life – the regulatory authority responsible for the shipbuilding industry and transport is tasked with establishing and implementing a set of requirements for ensuring the ship’s safety. Such requirements will be legally binding on both the shipyard and the company that will own and operate the ship – the cruise line.

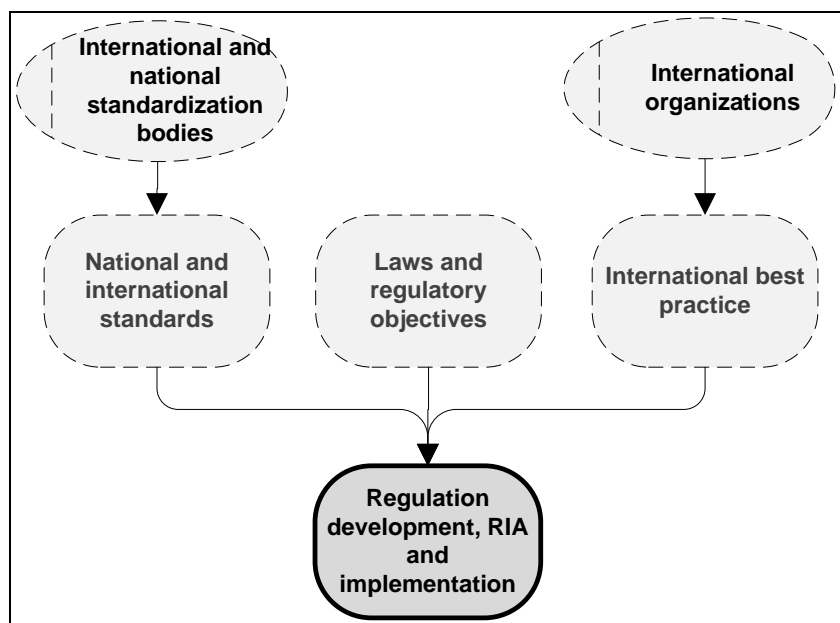
* This example reflects real current trends, since the shipbuilding industry “had previously remained largely unregulated for millennia, despite posing large and obvious risks”, and “has gone ... to having an extensive framework of conventions” (Mattli and Woods, 2009).

5.1 Inputs to a regulatory system

Before describing the many steps or processes involved in regulation, we will give an overview of some of the elements on which the entire regulatory system is based. The following can be thought of “inputs” in regulatory system processes:

- Clearly defined objectives for the whole regulatory system
- Solid legal basis (laws on how to make laws)
- Available national and international standards
- A codified references to standards system
- International best practice

Figure 5.1 Important inputs to a regulatory system



Let us then look at each of the five inputs listed above and depicted in Fig. 5.1

1. **Clearly defined objectives for the whole regulatory system.** In setting a new regulation, or in revising it, a policymaker strives to contribute to the achievement of the objectives of the regulatory system as a whole. For example, in the food sector, the regulator aims at making safe food available to the population at a reasonable cost. These objectives should be defined with reference to the whole country’s development strategy, and support its societal and economic goals, including health and safety. Any regulatory requirement that is not conducive to meeting those objectives can be considered redundant. Well-defined objectives for the regulatory system are an important input at all stages of regulation, particularly during *ex-post* evaluation
2. **Solid legal basis (laws).** Any regulatory system, which by its very nature produces laws and regulations, should itself have a solid legal basis. For a regulatory authority to influence production processes, its responsibilities and mandates should be legally defined. The World Bank (2006) lists the legal framework as one of the most important benchmarks for evaluating regulatory systems, contending that the “basic regulatory principles, practices, procedures

and policies to be followed should be articulated in law (preferably in a statute or primary law)". The regulatory agency "should also be created in a law that fully articulates its jurisdictional authority, powers, duties, and responsibilities". These principles are applied in many regulatory systems. For example, EU Regulation 178/2002 establishes the system in the area of food safety: it describes the functions of the regulatory authority (the EFSA), the main processes of the system, and other key aspects of this regulatory system.

Building a cruise ship (2): Regulatory objectives and legal basis

Established and recognized objectives set a direction for a regulatory system and ensure that all the necessary regulations are in place. The objectives of the regulatory system for the shipbuilding industry are no different from those of any other transport industry. We will not list them all, but in order to create a consistent example, let us assume that such objectives would include:

- Protecting passenger safety:
 - minimizing accidents
 - minimizing the consequences of accidents
- Minimizing the environmental impact
- Avoiding escalating costs for businesses

Regulatory objectives play a major role in evaluating regulations and can be used to ensure that all the objectives are covered by regulations. They can also serve as evaluation criteria and help to avoid situations in which a regulation meets one objective but makes it impossible to achieve another (e.g. when ships are made safe but not competitive).

We will assume that in order to achieve these objectives, the regulator will develop a regulation covering three areas: 1) the quality of steel used to make ships, 2) contingency planning, and 3) the number of lifeboats.

The legislation establishing a regulatory system creates a platform that ensures the legal value of the requirements. For the shipbuilding industry, legislation should define:

- The regulatory authority (such as the Ministry of Transport)
- Regulatory objectives (discussed above)
- Regulatory processes

3. **Available national and international standards.** A standard is a "document approved by a recognized body that provides, for common and repeated use, rules, guidelines, or characteristics for products or related processes and production methods, with which compliance is not mandatory" (WTO, 1994b). International standards – developed by such international standardization bodies as ISO, IEC and the International Telecommunication Union (ITU) – are among the main building blocks of any regulatory system, for the following reasons:

- They systematize and summarize collective wisdom and internationally recognized best practice across various fields and are important business tools for both regulators and economic operators. Available international standards help economic operators establish efficient business processes.
- International standards can be adopted by national standardization bodies as national standards (taking national specificities into account), and

conversely, national standards can become international. In other words, the world standardization system allows for national knowledge to add to “international wisdom” and for “international wisdom” to be applied at the national level. Adoption of international standards helps international best practice become part of a national regulatory system.

4. **References to standards in legislation.** If a regulation refers to a standard, it is as if it contained all the requirements of the standard. Available national standards (based on international standards) enable recent technological developments to be fed into the national regulatory system, thereby enhancing the efficiency of economic operators and the level of economic integration. This also helps minimize the differences between national regulations that are among the major barriers to international trade. Reference to standards is an important option, but if done inappropriately it can lock in reference to dated technologies, or unnecessarily constrain the legislator’s control over the regulated activity. For this reason, one of the recommended approaches is to refer to the latest nationally adopted version of the standard. As the national authority will be involved in the national adoption, it may insert any concerns it may have into the national version. By referring to the most recent version, it will avoid creating regulatory requirements which may harm the industry’s competitiveness.
5. **International best practice.** A set of documents developed by international organizations – such as the WTO, the International Trade Centre (ITC) and UNECE – that represent international best practice in the development of technical regulations are available for use by regulators. Such documents include the TBT Agreement (WTO, 1994b), UNECE Recommendation “L”, which lays out the “International Model for Technical Harmonization” (UNECE, 2001) and ITC’s *Roadmap for Quality* (ITC, 2004).

Case study: Building a cruise ship (3)

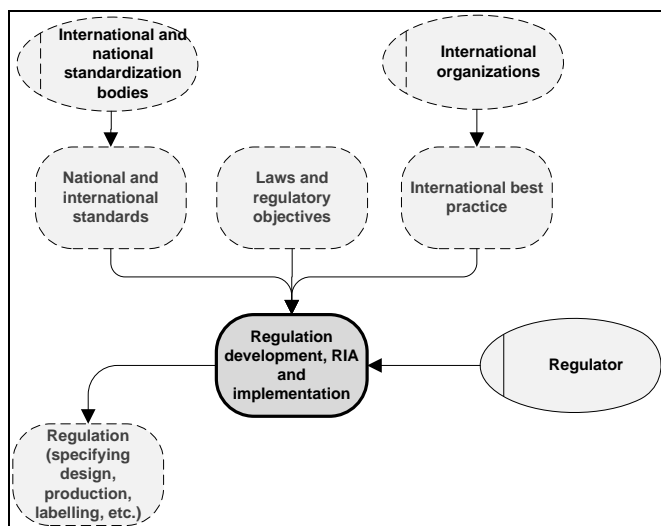
International standards and best practice

The importance of standards in the regulatory system can be considered from various perspectives.

1. The shipyard may use the knowledge and know-how described in standards in its production processes. In choosing its suppliers, it may refer to a nationally adopted version of ISO 9001:2008 to evaluate the quality management system of suppliers, which would help ensure good-quality supplies. Or, when the shipyard develops a contingency plan, it may apply ISO 31000:2009, the internationally recognized best practice in this field.
2. When the regulator sets requirements for the quality of steel the shipyard must use, or when it decides on the minimum number of lifeboats, it may consider referring to international standards. When it drafts regulations, it may refer to national versions of such international standards and thus rely on the knowledge of experts who helped develop the standard. If the ship is built according to international standards, it will meet internationally recognized benchmarks.

5.2 Different stages of rule-making

Figure 5.2 Building blocks of rule-making



Drafting regulations

The pre-assessment, drafting and implementation design of a regulation are critical processes because they create a “footprint” for the regulatory system. Such processes are the responsibility of regulatory authorities and result in a set of regulations and regulatory requirements that determine the “substance” of the regulatory system and the rules for economic operators and the market.

The regulatory authority is accordingly the most important player in these processes. For any given industry, we define the “regulator” as the government agency that develops and reviews new legislative or non-legislative requirements in the public interest. Different organizations can perform this role for different sectors, including ministries, agencies and State committees. In the banking sector, it is usually the central banks.

Regulators should have an approved regulation development plan, i.e. a document setting out priorities for legislative action for a given period. This document should stipulate:

- Which regulations should be developed within a given timeframe
- Parties responsible for the development of each regulation in the list
- Approximate time frames for the development of regulations
- Costs related to the development processes
- International best practice and standards

Regulation development plans should be discussed and approved at a higher level than that of the regulatory authority (e.g. by the office of the Prime Minister), since high-level overview helps to ensure the consistency of the resulting regulatory portfolio (see section 4.2 above).

It is good practice for a regulatory authority to have an internal document, e.g. “a code of practice”, which provides a comprehensive description of the procedures and methodologies applied to drafting regulations. Such procedures are to a large extent determined by the scope

and specific characteristics of a regulatory system. The paragraph below highlights some aspects of the process that can be applied to all regulatory systems.

Drafting a regulation is a complex project that calls for the participation of a number of stakeholders and a detailed project plan. The project plan starts with a definition of the scope of the regulation under development and, in particular, the risks which the regulation sets out to address. The objectives of the regulation should be complemented with well-defined critical success factors, which are a set of parameters that will be analysed when the regulation is developed so that a regulator can assess whether the original requirements have been met. The assumptions and constraints that the regulatory authority will use as an input to the planning and development process are other key factors that should be specified in the project plan.

In general, the drafting project has the following phases:

1. Drafting the regulation
2. Obtaining internal comments on the draft
3. Revising the draft
4. Obtaining comments from other regulatory authorities
5. Revising the draft
6. Obtaining public comments (including from international partners)
7. Revising the draft
8. Approval
9. Publication

After the regulator has broken down the tasks that must be undertaken, he or she can determine:

- How much time is necessary for each of the tasks
- Which tasks can be implemented in parallel and which should be sequential
- What the budget requirements are for each task
- Which tasks can be realized by the regulatory authority itself, and which require the participation of external experts and stakeholders, such as standardization bodies, scientists, industry and consumer associations, etc.

This information is sufficient to define the project time frame and budget, and also to identify the competences that must be represented on the project team. In many cases, regulators outsource parts of the drafting process to other institutions, but even in these cases the responsibility for the coordination of the processes remains with the regulatory authority. In addition, since regulations alter the behaviour of economic operators, their participation in the development process is important in order to create a balanced regulatory system. Therefore, each project for drafting a technical regulation implies establishing a working group so that all participating stakeholders can express their views.

The project plan for drafting a regulation should determine the communication processes that will be applied, e.g. when and how often meetings will be held, and how the progress will be reported. It is also highly advisable for the project plan to reflect how the regulatory authority will manage the project's risks, quality, and, if necessary, procurement.

The project plan, describing the typical phases of drafting a regulation that are outlined above, should also contain all the tasks related to supplementary activities, such as searching for experts, checking the quality of the regulation and so forth, so as to ensure a timely completion of the process.

The actual drafting of a regulation, i.e. defining the regulatory requirements, is an activity that varies across regulatory systems. Two widely used models are prescriptive regulations and performance-based regulations. Performance-based regulations set out the desired characteristics of a good, service or process, leaving it up to the economic operator to choose the most appropriate means for attaining it. Prescriptive regulations contain technical requirements in the text of the regulation or refer to relevant standards. Each of these approaches may be suitable to treat different kinds of risks. For example, serious risks, such as risks to life or workers' safety, or risks related to the incompatibility of goods/techniques, may require a prescriptive approach. The requirements of a prescriptive approach may also be easier to understand, implement and monitor, with the result that the related risks may be easier to monitor and manage.

Most prescriptive technical regulations are developed with reference to standards, meaning that the text of the technical regulation summarizes essential safety requirements only, whereas all the details and technical requirements can be found in the international standards to which the regulation refers in the text. Performance-based regulations may also contain a list of standards, but it is up to the economic operator to choose whether to comply with these standards in order to achieve the performance goals or whether to use other means.

The reference-to-standards approach has proven more convenient than spelling out all the requirements in the text of the regulation, one of the reasons being that the regulators do not have to change the entire text whenever a new version of a standard relevant to this particular regulation appears. This approach will also make the resulting regulatory text better aligned with international best practice. A broad adoption of this process at the international level would make national regulations and regulatory frameworks more similar to one another, contributing to minimize regulatory barriers to trade (see also sections 5.1 and 5.3).

In order to make the drafting process more efficient, the responsible organization should prepare an initial draft for discussion at the first meeting of the working group. Even if the first draft looks provisional, having something on the table will make it easier to manage the discussion.

A wide range of factors complicates the process of drafting legislation. One key factor that the authority will take into account is the need to respect international obligations. International conventions are developed in each field by the international organization responsible for cooperation among countries and for setting recognized standards and rules. In the field of atomic energy, for example, international agreements are drawn up by the International Atomic Energy Agency (IAEA) and adopted by its member States, bearing such titles as the Convention on Early Notification of a Nuclear Accident and the Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency. It is noteworthy that all WTO members are required to notify the WTO TBT Committee in due course of any upcoming changes in technical regulation.

The authority that drafts regulations will also be under pressure from different groups, including consumers, industry and environmental lobbyists. Consumers and civil society will be influenced by the industry's track record (accidents, fatalities, competitiveness, share in the country's total employment and economic output, etc.). Public opinion will typically favour strict regulations for new economic sectors, or sectors that have made headlines in connection with large-scale accidents, regardless of what actually caused the accident. For example, a number of nuclear reactors have been closed down worldwide largely in response to public outcry over the dramatic accidents that have characterized this sector.

Another major interest group is the industry itself, or large individual firms within an industry. Such firms may try to influence regulations so that they closely mimic their own

corporate specifications and standards to change the market structure to their advantage. Ultimately, the outcome of the regulatory activity will in part reflect how the concerns expressed by these constituencies play out.

It is important to remember that regulations should remain understandable by the end clients and others whose behaviour they are supposed to change (society and economic operators), and not only to lawyers.

In order to obtain comments from the public, a regulatory authority should consider cooperating with professional organizations and societies. These organizations, in turn, can upload the drafts of regulations onto their websites and use other means of communication to collect input from the business sector.

Another key task of a regulatory authority is to manage changes in the drafting project. This includes updating the project plans so that they remain current and relevant, and respond to external changes.

It may appear, sometimes, that applying a more rigorous and systematic process of rule-making and implementation is a somewhat utopian exercise. Nonetheless, referring to international best practice in rule-making, including the best practice presented in this publication, may be a valid support for regulatory authorities as they strive to develop a fair system that is well balanced and adapted to meeting the needs it has identified.

Regulatory convergence

It is widely accepted that regulatory convergence is necessary for overcoming barriers to trade. At the same time, harmonization helps develop common approaches to managing risks that confront societies internationally, as well as to controlling transborder hazards.

One approach that regulators can apply for harmonization purposes is described in the UNECE Recommendation “L” (UNECE, 2001). It contains an international model – i.e., a set of principles and procedures that countries can implement to approximate technical regulations among themselves. At the core of the model is the concept of common regulatory objectives (CROs).

CROs address legitimate Government concerns for each sector with regard to public health, safety or environmental protection. They are preferably defined with reference to international standards. They specify:

- International standards that contain product-related requirements
- How compliance with these standards is assessed, and which conformity assessment bodies are recognized as competent
- How market surveillance will be performed

Recommendation “L” promotes the “reference-to-standards” approach, which is also one of the cornerstones of the European regulatory model.

The European regulatory model (adapted from www.ec.europa.eu)

The EU’s “New Approach” was introduced in a European Council resolution of May 1985. It is based on the principle that “the objectives being pursued by the Member States to protect the safety and health of their people as well as the consumer are equally valid in principle, even if different techniques are used to achieve them”.

The resolution lists the main principles for the division of labour in technical regulation among the parties involved and calls for a “a clear separation of responsibilities between the EC legislator and the European standards bodies CEN, CENELEC and ETSI in the legal framework allowing for the free movement of goods”.

The main concept behind this regulatory model and the corresponding regulatory process is the following:

- European Commission directives define the “essential requirements” for goods, which primarily cover health and safety issues.
- Once the essential requirements have been defined, the European standards bodies are tasked with developing the corresponding technical specifications whose application would enable the essential requirements of the directives to be met. Compliance with these standards will provide a presumption of conformity with the essential requirements. The specifications are referred to as “harmonized standards”. Such standards must offer a guarantee of quality with regard to the essential requirements of the directives.
- A producer thus has several options for showing proof of conformity with the essential requirements, including:
 - Products manufactured in conformity with harmonized standards are presumed to be in conformity with the essential requirements.
 - Standards are not mandatory, and a producer may choose other ways to show proof of compliance.

The flexibility of the New Approach is linked to the following features:

- It indicates what has to be achieved, but not the details of the corresponding technical solutions.
- It presents different options for conformity assessment.
- It does not necessitate regular adaptation to technical progress.

Recommendation “L”

This approach works well when a country formally and substantively participates in the work of the international standardization system. It entails taking part in technical committees, adopting international standards and involving the business community in the process of developing and implementing standards.

Reference to standards is widely applied because it allows regulators to:

- **Take advantage of available expertise and best practice internationally.** This is explained in the Physikalisch Technische Bundesanstalt (PTB)/ITC guide to *Technical Regulations: Recommendations for Their Elaboration and Enforcement* (Inklaar, 2009), as follows: “Developing technical regulations requires expertise in a variety of fields, which could be not sufficiently available in State authorities. Rather than developing these competencies – including by having the regulators

participate in the work of technical committees within standardization bodies – it is certainly much more efficient to take ... standards and use them for the purposes of legislation. This use would include the different methods of incorporation – the word-for-word reproduction of a standard or excerpts of a standard in a regulation – and especially of reference to standards”.

- **Eliminate technical barriers to trade.** When developing a regulation, regulators will want to align their requirements with those of their trading partners in order to avoid having different or contradictory requirements in different export markets. If trading partners refer to the same international standards, as shown in the figure below, this will help minimize the differences in the requirements and also facilitate trading procedures (also as shown in the figure). The legislation of countries “A” and “B” refers to the same international standards and hence provides harmonization of requirements.

The concept of “reference to standards” is used not only in technical regulations but also in other domains. An example of how this mechanism functions in the financial sphere is presented in the box below.

Reference to standards: an example from banking

“The Basel Committee [on banking supervision] ... formulates broad supervisory standards and guidelines and recommends statements of best practice in the expectation that individual authorities will take steps to implement them through detailed arrangements – statutory or otherwise – which are best suited to their own national systems. In this way, the Committee encourages convergence towards common approaches and common standards without attempting detailed harmonization of member countries’ supervisory techniques” (Bank for International Settlements, 2001).

UNECE Recommendation “L” provides a description of the basic steps in the processes of harmonizing regulations. These include:

- **Identifying a need for harmonization of technical regulations.** The need might be identified through the following mechanisms:
 - Studies by specialists from a particular sector or industry which are commissioned by Governments, international organizations, business groups or NGOs and which are discussed in national, regional or international forums
 - Initiatives by one or more countries to harmonize their technical regulations at an international level
 - “Complaint-based” initiatives, for situations where a country is responding to complaints from foreign or national business operators about its technical regulations regime
- **Call for participation.** At least three countries wishing to harmonize their technical regulations with other countries should issue a “Call for Participation” to all United Nations Member States through the UNECE secretariat. The Call should contain the information needed to formulate CROs (cf. Annex B of the Recommendation). Countries wishing to participate in the work under such a Call should respond to the secretariat within three months of its transmission by the

UNECE secretariat. Countries that have expressed an interest can begin the technical harmonization process three months after transmission.

- **Setting up an open-ended task force.** Based on the responses to the Call, an open-ended joint task force composed of interested countries is set up to develop CROs on safety, health, environmental protection and other legitimate Government concerns about the products or group of products in question.
- **Agreeing on the working procedures.** The task force should inform the UNECE secretariat about its work, which will be made publicly available through the appropriate means (such as the Internet).
- **Drafting the CROs.** CROs are a mutually agreed document registered by UNECE and made publicly available. By drafting CROs, the interested countries agree on such elements as:
 - Statement of scope
 - Product requirements
 - Reference-to-standards clause
 - Compliance clause
 - Market surveillance and protection clause
- **Publishing CROs on the UNECE website.** Countries that have agreed on CROs submit them to (WP.6) through the UNECE secretariat.
- **Incorporating CROs into national legislation.** A country that has agreed on CROs submits them to the process stipulated in its own legislation for adopting the technical requirements specified in the CROs. Any other country may at any time inform the UNECE secretariat of its intention to implement and use the CROs. Within 60 days following its adoption of the CROs in its own legislation, the country notifies the UNECE secretariat in writing of the date on which it will begin to apply them.
- **Applying CROs to trade procedures.** Countries that have agreed on CROs must ensure that products which comply with them can be placed on their market for free circulation without being subject to any additional product or conformity assessment requirements (such as testing or certification).

UNECE is currently engaged in a number of sectoral projects based on the International Model for Technical Harmonization. These projects include the Telecom initiative, the “Earth moving Machinery initiative”, the “Initiative on Equipment for Explosive Environments” and the “Initiative on Pipeline Safety”. These projects represent the highest possible degree of regulatory cooperation under United Nations auspices and aim at establishing fully harmonized technical regulations within their respective sectors.

Building a cruise ship (4): Regulation development

We have said that important objectives of the regulatory system for the regulator include protecting passenger safety, minimizing the environmental impact and avoiding escalating costs for businesses. Meeting these objectives requires the introduction of legally binding requirements. Regulatory actions for the shipbuilding industry that can complement these objectives may include:

- Defining industry-specific requirements and developing industry-specific regulations on:
 - The number of lifeboats relative to the number of passengers
 - The required quality of steel and other materials
 - Requirements for contingency planning
- Defining processes that can ensure the parameters will be kept up to date
- Identifying the processes for supervising and monitoring implementation of the regulation

A regulatory authority can either determine these requirements itself or refer to available international standards. If the regulator applies the concept of reference-to-standards and uses international standards for the quality of steel, contingency planning and the number of lifeboats when drafting its regulation, this can 1) help ensure that the regulation reflects the most recent trends in technology, and 2) increase the chances that a country's regulation is convergent with those of its trading partners.

If the countries to which our cruise ship is expected to travel have different requirements – for example, regarding contingency planning on board – this will incur additional costs for the shipyard. The shipyard will need to implement processes to meet the requirements of the foreign standard, and also to pay for certification that the ship conforms to those requirements (which may be necessary even if the requirements are similar). If, however, a regulation on contingency planning refers to international standards that describe the best practice in contingency planning, this will help ensure that the requirements are similar. And if the foreign country recognizes certificates issued in the home country, the shipyard will not have to pay twice for certification.

Conformity assessment will be discussed below.

Regulatory impact assessment

In a number of countries and regional groupings, a regulatory impact assessments is a compulsory step of regulatory action, for example in the European Union. It consists of a comprehensive analysis of the expected impact of a proposed regulation on various interest groups, trade, existing legislation and other areas on which a regulation may have an impact. The assessment also includes such components as risk analysis, analysis of other options, and feasibility studies.

Regulatory impact assessment as a tenet of regulatory policy was to a large extent developed by the Organisation for Economic Co-operation and Development (OECD). The OECD explains that “RIA looks at how policies will be implemented, enforced, reviewed and complied with. It can help to ensure that all potential impacts of a policy are considered in advance, and that the regulation decided on by government is the optimal approach to take”. Descriptions of this methodology can be found in a number of OECD publications, including 1997a, 1997b, 2005, 2007, 2008a, 2008b and 2009. Introducing RIA into the development and implementation of technical regulations increases both the efficiency of the system and the stakeholders' involvement in the project, and also helps mitigate most of the common implementation risks. Inklaar (2009) states that “a rapidly growing number of countries have introduced the obligation to carry out RIA for different kinds of regulations – especially for proposed technical regulations”.

Regulatory impact assessment is one of the critical building blocks of any risk-based regulatory system. Whenever regulation is considered as a possible risk treatment option, RIA enables an optimal solution to be found for achieving the regulatory objectives. The approach promoted in this publication has a broader scope, that of enhancing the coherence of risk management at the country level. This helps avoid situations where risks are disproportionately mitigated across sectors, as for example when railways receive excessive protection from authorities but road safety is low.

Case study: Building a cruise ship (5)

During the process of drafting regulations, regulators perform regulatory impact assessments, which in the most simple case consist of such questions as the following (adapted from Inklaar, 2009):

1. Who will be affected by the new regulation, and to what degree?
2. Are there any alternatives to the regulation?
3. Do the benefits of the regulation justify the total costs of the regulatory exercise?
4. Will the primary affected parties be able, from a technical and economic viewpoint, to comply with the requirements of the regulation?
5. Is the regulation compatible with existing national legislation?

Answering these questions (along with many others that can be found in RIA methodologies) will ensure that the regulation is indeed well drafted and that it can be implemented.

Implementing regulations

Ultimately, technical regulations are designed to change the characteristics of products and the way production processes are carried out. The implementation of a new regulation should be planned to ensure that the industry is aware of the new regulation and of how to comply with it and that it is able to meet the new requirements. It should also ensure that the resources needed to enforce the regulation are set aside for both pre-market and post-market controls.

Implementing regulations is a complex organizational project that should be efficiently managed. The following are critical requirements for the successful implementation of technical regulations:

- Cooperation and communication among various stakeholders (most of whom have different interests)
- Availability of the necessary infrastructure (e.g. for conformity assessment and market surveillance)
- Planning, budgeting and other aspects of systematic project management

In most countries, the participation of interested parties in implementing a new technical regulation is defined in the implementation plan. The plan contains a list of actions that must be performed by all stakeholders.

Considering all project management areas (such as project communication, risk, budget, quality, etc.) when developing the implementation plan is essential to running successful implementation projects (see PMI, 2008 and IPMA, 2012).

Building a cruise ship (6): Implementing regulations

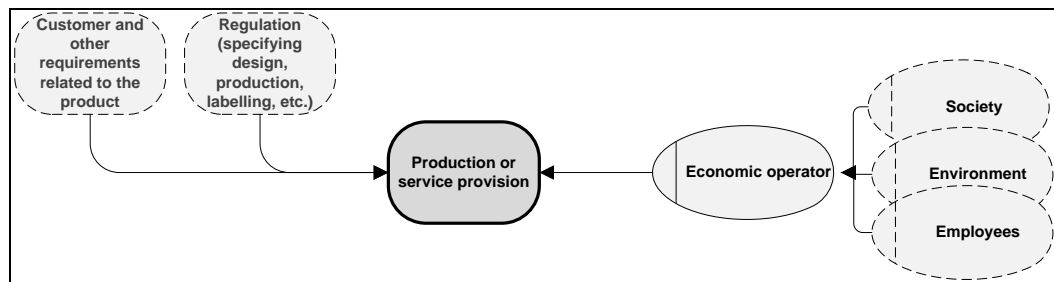
Implementing regulations is a complex project. One of the regulations that the shipbuilding regulator has decided to introduce concerns contingency planning. We will use this imaginary regulation as an example of the implementation process. In order to implement the regulation, the regulator needs to clearly identify:

1. The objective of the implementation project, its critical success factors and its stakeholders
2. The tasks that must be performed to achieve the project goals and the proper sequencing of those tasks
3. Project risks and risk management strategies
4. The budget required to carry out all the tasks that have been identified
5. How to organize communication among the stakeholders, and how to manage changes that may occur in the project
6. Other parameters necessary for successful project implementation

Following these steps will ensure that regulations are efficiently embedded in the shipyard's business processes.

5.3 Production or service provision

Figure 5.4 Inputs, outputs and participants in production and service provision



In order to demonstrate the interfaces between regulatory and business processes, we will assume that the business processes of an economic operator functioning within a regulatory system are organized in accordance with the ISO 9001:2008 management system standard. This assumption is valid because ISO 9001:2008 is the most widely used such standard, applied by more than one million companies worldwide. We will focus on how regulatory processes affect the following main phases of a production cycle:

- Determination of product-related requirements
- Design and development
- Purchasing
- Production

The regulatory system model that we are discussing depicts economic operators as the key players in this phase. It also indicates that production processes directly or indirectly involve society in general, employees and the environment. Their roles should be considered as well.

The requirements of regulations that set rules for a sector or market, along with customer requirements for a product (which determine the market demand for the product), constitute a major input to production processes.

This is explicitly reflected in ISO 9001:2008. According to the standard, one of the first steps in the product life cycle after the production processes have been planned is to identify and review the **statutory and regulatory requirements related to the product or service**. This process builds an interface between production processes and regulations. Statutory and regulatory requirements are identified, along with:

- Customer requirements that determine the market demand for the product
- Requirements that are not specified by the customer (customers may actually not be aware of them) but that are necessary for the product's use
- Any additional requirements considered necessary by the organization

Regulatory requirements are not limited to the quality of the product. Horizontal legislation (as opposed to sector-specific regulation) may contain requirements for minimizing the environmental impact of the economic operator, for ensuring worker safety, and so forth. These requirements also have a significant impact on the organization's business processes and should thus be considered as well.

A key recommendation of ISO 9001:2008 is that, once an organization has identified the requirements, it should review them and determine whether it has the capacity to meet them. That mitigates the risk that the organization will sign a contract it is unable to honour.

Product-related requirements, including regulatory requirements, serve as an input to the design and development process, on which ISO 9001:2008 provides recommendations. It requires that along with "functional and performance" requirements, inputs include "applicable statutory and regulatory requirements". During the review, verification and validation of the outputs, the organization must constantly ensure that the input requirements have been met.

At this point, the regulatory and other product-related requirements will already have been fed into the design of the final product and referred to in the design document itself. The next stages of the production process create a material outcome (or service provision) from what was designed at the previous stage.

Regulatory requirements may also cover purchasing processes and set specific rules for choosing suppliers. In any case, if an organization operates in accordance with ISO 9001:2008, it will "ensure that the purchased product conforms to specified requirements". For this purpose, the organization "shall evaluate and select suppliers based on their ability to supply the product in accordance with the organization's requirements".

Purchased products are material inputs to production processes. Depending on the nature of the regulation, it may or may not contain specific requirements on how such processes can be organized. A basic distinction can be drawn between two types of regulatory frameworks in this regard. Goal-setting regulations set a goal but leave economic operators free to select their preferred means of attaining it. This means that an organization has some degree of freedom in choosing technologies and establishing production processes. Prescriptive regulations, by contrast, set specific requirements, which can be deterministic or risk-based. Deterministic regulations involve setting precise and mandatory safety measures, which can lead to constraints being placed on economic operators as to the choice of technologies to be applied. Risk-based regulations constitute a special type of requirement in which the economic operator is expected

to analyse unintended events that might occur and take appropriate measures to prevent their occurrence and minimize their consequences.

The regulatory requirements for production processes can raise business costs considerably. The processes also need to be organized in accordance with all the relevant regulations, including those concerning occupational and environmental health and safety.

Whatever the nature of the relevant regulations, regulatory requirements will be considered together with the general requirements of ISO 9001:2008, which stipulates that production and service provision processes be performed under what is referred to in the standard as “controlled conditions”. Such conditions include the availability of work instructions, the use of suitable equipment, and the availability and use of monitoring and measuring equipment.

ISO 9001:2008 requires the identification and traceability of products throughout the production process, the protection of customer property, and the assurance that the product will be safe during internal processing and its delivery to the client.

Building a cruise ship (7): Meeting regulatory and customers’ requirements

At this stage, our shipyard has learned of a new regulation that sets the requirements for the quality of steel, the number of lifeboats, and contingency planning on board. These requirements are based on international standards and hence reflect recent technological developments.

The shipyard, however, needs to identify other regulatory requirements that are not necessarily product-specific, including those for protecting the environment and ensuring occupational safety. Most importantly, it needs to understand the market demand for cruise ships. It needs to specify:

- The cruise line’s requirements, as defined in part on behalf of the end-users (the passengers), such as amenities, quality of materials, available cabin space, etc.
- Other requirements, such as the number of lifeboats and the quality of steel, which are dependent on such variables as the type of routes the ship will travel, the number of passengers, existing regulations, etc.

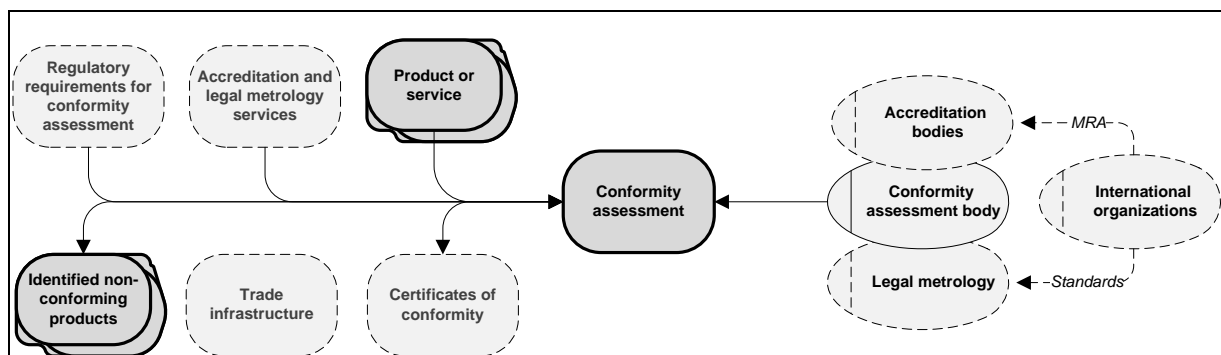
These requirements can be identified during negotiations with the cruise line and can be referenced in the relevant contracts between the shipyard and the cruise line; they will all be taken into account in designing the ship. In addition to all the technical parameters, at this stage the quality of the ship (number and size of cabins, quality of materials, etc.) will be determined.

The ship design document will contain references to all the standards to be used in the ship’s production. The design will specify the standard for assessing the quality of the steel purchased and will cite the regulation that defines the number of lifeboats and so forth. It will also furnish the information needed to plan the procurement processes. Unless the shipyard has its own steel plant, it will need to find suppliers that can provide the quality of steel needed to comply with the standard referred to in the corresponding regulation. In identifying the criteria for choosing suppliers and for issuing a tender, the shipyard will need to specify all requirements, including those defined in the standard.

A ship that is produced in accordance with all of the requirements above, including those for the product, processes and supplies, will meet the requirements of regulations that reflect international best practice.

5.4 Pre-market control: conformity assessment

Figure 5.6 Inputs, outputs and the main participants in conformity assessment



Pre-market control through conformity assessment and related processes is one of the major building blocks of a regulatory system. ISO/IEC 17000:2004 defines conformity assessment as “demonstration that specified requirements relating to a product, process, system, person or body are fulfilled”. Conformity assessment procedures, such as testing, inspection and certification, offer the assurance that products meet the requirements specified in regulations and standards.

The objectives of conformity assessment in a regulatory system are threefold:

1. To provide good-quality assessments and prevent products not in conformity from being placed on the market
2. To avoid unnecessary costs being incurred by economic operators
3. To contribute to the elimination of technical barriers to trade (“tested once – accepted everywhere” principle)

Conformity assessment-related costs: a real-life example

For an economic operator, and indirectly for a consumer, the costs associated with conformity assessment can be substantial, especially for equipment and products for which national certificates are still required. One private company, active in the sector of instruments for level measurement, flow measurement and pressure measurement reported product type certification costs of more than 100,000 euros per year and delays of 1.2 years in reaching global markets (Klotz-Engmann, 2010). These costs have a major impact on both business competitiveness and consumers, that ultimately bear the additional costs.

As stated in the TBT Agreement, conformity assessment procedures should not be more strict or applied more strictly than is necessary to give the importing member adequate confidence that products conform with the applicable technical regulations or standards. However, OECD (1996), estimated that standards and technical regulations, combined with the cost of testing and compliance certification, represent between about 2 and 10 per cent of overall production costs.

In the following pages we will describe the main elements of a conformity assessment system and the main principles of its functioning, focusing on the various conformity assessment options and on international cooperation in this field. We will also look at how conformity assessment bodies (organizations that provide conformity assessment services) collaborate with:

- Accreditation bodies (which check the quality of conformity assessment services and ensure international recognition of certificates).
- Metrological organizations (which provide the metrological infrastructure for conformity assessment and metrological services). If the measuring equipment is of poor quality, the results will be compromised and a poor-quality product may not be identified; conversely, a good-quality product may not be placed on the market.
- International organizations (such as international accreditation forums) that work in this field.

From the perspective of a regulator, the most fundamental choice in this domain is the choice among different conformity assessment options, including: first-party conformity assessment, based on a producer's own internal testing system, and resulting in the "supplier's declaration of conformity" (SDoC) and third party conformity assessment. These two options are described in detail below.

The Network on Metrology, Accreditation and Standardization for Developing Countries recommends that conformity assessment procedures be chosen "based on an assessment of the risks involved with a particular product or process, and on an understanding of the impact the associated costs and benefits will have". (DCMAS, 2010).

In general, and in keeping with the DCMAS guidance, most regulators require a SDoC for low-risk products, while demanding third-party certification or inspection, undertaken by an independent service provider for more complex and risky products and equipment.

The box below provides an example of how the EU legislative framework determines the choice of conformity assessment procedures.

Choosing conformity assessment procedures: A European example

The principle underlying the European conformity assessment system is that "conformity assessment procedures shall not be more strict or be applied more strictly than is necessary", taking account of the risks that non-conformity would create. Hence, the framework places the procedures into eight different modules, ranging from the least stringent (the manufacturer's declaration of conformity) to the most stringent (full-quality assurance certification). Legislators in the European Union may choose from this menu and assign various conformity assessment procedures to different types of products. For some products, internal production control is sufficient. This means that the manufacturer makes its technical documentation available to national authorities and declares conformity with essential requirements. At the other end of the spectrum is "full-quality assurance". This choice of conformity assessment means that the manufacturer operates an approved quality management system and that the certification body conducts the surveillance of the system (Sacchetti, 2010).

First-party conformity assessment: internal monitoring and measurement

Monitoring and measurement performed by a producer are essential in any production cycle. They verify that the product requirements have been met as originally defined. Simply put, they are intended to check the quality of the product before it goes on the market.

Monitoring and measurement are common business practices and a requirement of management system standards. Other things being equal, in-house detection of poor-quality goods will result in smaller losses than if the poor quality is detected only by authorities or consumers. Regulations may specify requirements for internal quality checks, and in some cases, such checks are sufficient to place a product on the market.

To perform internal monitoring and measurement, an organization needs “monitoring and measuring equipment to provide evidence of conformity of the product to determined requirements”. In order to ensure valid results, ISO 9001:2008 recommends that the organization’s measuring equipment be calibrated, verified, adjusted or re-adjusted. The regulatory system should provide good-quality metrological services for carrying out these functions.

The availability of metrological services to economic operators and the application of international standards to metrology are essential requirements for producing competitive goods and facilitating international trade.

Third-party conformity assessment

Pre-market control in various forms is implemented in practically all markets. In some spheres, such as finance, conformity assessment is conducted through licensing. In technical regulation, it is performed as part of a set of complex processes involving international players and based on internationally recognized standards.

Conformity assessment is performed by means of certification, inspection and testing. A comprehensive description of these processes is presented in ITC (2004). Conformity assessment best practice can be found in standards and guides, including European Norm (EN) 45014:1998, ISO Guides (2, 7, 22, 60, and 65), ISO 17024 and 17025, and EN 45000.

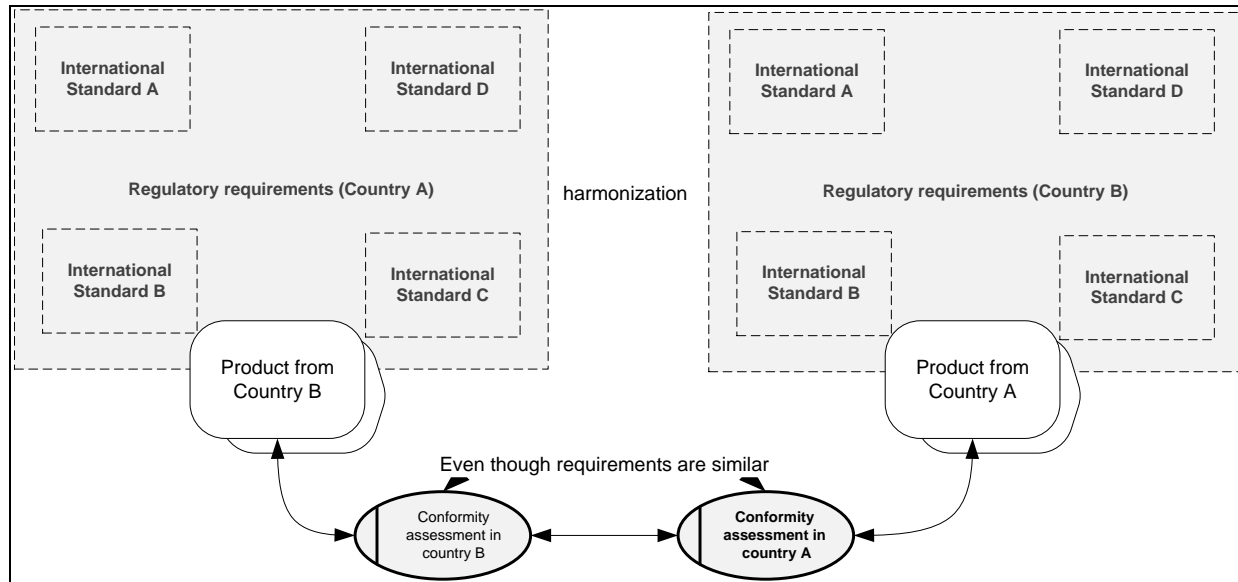
Accreditation and international cooperation on conformity assessment

Accreditation and legal metrology services are another major input to conformity assessment processes, which contribute to all three of the above-mentioned objectives (providing good-quality assessments, avoiding unnecessary costs, eliminating technical barriers to trade). Accreditation plays a number of important roles. First of all, it assures businesses and end-users that the conformity assessment body providing certification to a standard has the required competence and impartiality to do so, as evidenced by fulfilment of international standards and requirement. As defined in ITC (2004), “accreditation is the formal recognition of competence to provide a specified service”. Hence, the quality of accreditation services determines the quality of conformity assessment in the country and is highly dependent on the competence of the accreditation body’s staff.

Most countries have their own accreditation body to approve the competence of conformity assessment bodies. However, another key role of accreditation is that it supports the “tested-once – accepted-everywhere” principle. Even if national regulations are based on the same international standards, if conformity assessment requirements are different, products may be subject to double testing, or to a different type of testing, as shown in the figure below (in which we have added a conformity assessment block to the figure used to describe the reference-

to-standards principle). Even if regulations are similar in several trading countries, economic operators may be required to prove conformity with the same regulations several times. This leads to additional costs for business and hampers international trade.

Figure 5.7 Regulatory cooperation in conformity assessment and its impact on trade



As stated in DCMAS (2010), “products may be denied market access because the testing procedures or results are not recognized, or because those who performed the tests do not belong to a peer assessment scheme or are not accredited”.

Although international cooperation in the field of conformity assessment is well under way, better convergence of regulatory approaches is still needed in this area. Regulatory cooperation on conformity assessment – whether bilateral or multilateral – helps to avoid unnecessary regulatory differences, reduces duplicate regulatory requirements and related burdens and promotes better-quality regulation (UNECE, 2010d). In the following pages we will introduce international accreditation schemes, mutual recognition agreements (MRAs) and other forms of international cooperation in the field of conformity assessment.

International accreditation schemes

In order to increase the level of recognition of the certificates issued by the accredited conformity assessment bodies, accreditation bodies should belong to the international accreditation system. The two best-known bodies are the International Accreditation Forum (IAF) and the International Laboratory Accreditation Cooperation (ILAC). They facilitate global trade by allowing members to recognize one another’s accreditations as equivalent.

One of the purposes of IAF and ILAC is to establish multi-lateral recognition arrangements (MLAs) between their accreditation body members. As the name implies, the objective of these arrangements is to ensure mutual recognition of accredited certification between signatories to an MLA, and subsequent acceptance of accredited certification in many markets based on one accreditation. In other words, the benefits of an MLA to business are that, if standards, specifications and conformity assessment methods are the same, one certificate or certification can be recognized worldwide, thereby lowering the cost of accredited certification and reducing the risk that products or services may be rejected by international trading partners.

Mutual recognition agreement

A related form of regulatory cooperation in the area of conformity assessment is mutual recognition agreements (MRAs), which are signed between Governments (as opposed to MLAs, which are established by international accreditation organizations).

There are different types of MRAs, but the most widely used are traditional MRAs that provide “recognition of results of compulsory certification required by a Party of the certificates issued by conformity assessment bodies in the territory of another Party” (Sacchetti, 2010b), and those based on common rules and standards. Traditional MRAs enable certification to the other party’s rules by a local conformity assessment body rather than by a conformity assessment body located in the first party. It does not require harmonization of technical regulations or standards. MRAs based on common rules and standards are broader and more difficult to establish, but they eliminate duplicate testing and improve market access for both sides (for details see Sacchetti, 2010b). For example, an MRA between the EU and Switzerland covers such sectors as machinery, toys, electrical equipment, motor vehicles and many more.

MRAs and other forms of international cooperation in the field of conformity assessment were discussed at the twentieth annual session of UNECE WP.6 (UNECE, 2011d). Delegates noted that, based on experience with MRAs, while they are an important tool, they entail burdensome designation procedures and generally heavy maintenance costs, with low perceived benefits.

Other forms of international cooperation on conformity assessment

At the international level, conformity assessment is also addressed by the WTO’s TBT triennial reviews. Regardless of the type of conformity assessment (e.g. first-party, second-party, third-party*) and of what is being assessed (product, service, or management system), the importance of using international standards and guides has been underscored in all recent reviews.

UNECE WP.6 is another key platform for producing regulatory cooperation. At its twentieth annual session, it proposed that the following forms of cooperation should be considered as part of the solution for making conformity assessment more efficient:

- Strengthening the cooperation between manufacturers and third-party conformity assessment bodies, in particular by encouraging the latter to avoid repeating tests already performed, under certain conditions
- Increasing interlaboratory cooperation – and in particular proficiency testing – as a basic condition for achieving homogeneity of testing, measurement and conformity assessment procedures.
- Building on the positive experience of the multilateral schemes for assessing conformity to standards, such as the Worldwide System for Conformity Testing and Certification of Electrotechnical Equipment and Components (IECEE) and the IEC System for Certification to Standards relating to Equipment for use in Explosive Atmospheres (IECEx System)

* First party conformity assessment – an organization assesses conformity of its products itself (e.g. supplier’s declaration of conformity), second party – an organization assesses conformity of its suppliers, and third party – an independent certification body assesses conformity of an organization.

Conformity assessment schemes

The IECEE and IECEx are two examples of multilateral schemes for assessing conformity with standards in the respective fields of electrotechnical equipment and equipment and services for use in explosive environments.

Members of these schemes apply the principle of mutual recognition (reciprocal acceptance) of test results for obtaining certification or approval at a national level, thus realizing the aforementioned “tested-once – accepted-everywhere” rule.

Under these schemes, testing and certification is carried out by bodies that are accepted into the systems through agreed procedures and by peer assessment.

The schemes reduce obstacles to international trade which arise from having to meet different national certification or approval criteria.(See www.iec.ch, www.iecex.com and UNECE, 2011c).

Metrology

Conformity assessment procedures, both internal and external, often require various kinds of measurements, which is where the metrology system becomes the key player. It guarantees that measurements can be performed, that they are correct, that the instruments work properly and that the results of the measurements can be trusted. This applies to conformity assessment procedures in general.

Before we begin discussing metrology, let us imagine that your plane has arrived late and you are afraid you may be late for a meeting. You are not sure that your watch is telling the right time. You can always ask someone else what the time is, but you realize that that person’s watch may also be wrong. You look up at the wall clocks to make sure, only to discover that they also show two different times. You do not know which clock to believe, and you have no idea whether you are late or on time, whether you will have to take a taxi to the meeting or can calmly wait for a bus.

This example illustrates the importance of metrology in the economic system. In the example, it is metrology that can determine whether the wall clock is functioning according to a reliable source. Metrology assures you that your watch is telling the right time, that you can check it against a wall clock, and that the wall clock can also be trusted. Although the example is simplistic, it illustrates the principal layers of the metrology system, involving economic operators, laboratories, national metrology institutes and international metrological organizations.

As stated in ITC (2004), “without metrology nothing else will work”. When assessing a country’s regulatory system, then, the following aspects should be considered:

- **A functioning metrological infrastructure** that can perform high-quality metrological services
- **Availability of metrological services** to economic operators and application of international standards to metrology
- **International cooperation** among national metrology institutes, which is a sine qua non for efficient procedures that support international trade

Building a cruise ship (8): First party conformity assessment

To make sure that the results of measurement can be trusted, the shipyard needs to have its instruments calibrated or verified by a metrology institute and needs to be issued an official certificate indicating that this has been done. If these services are unavailable, the quality of the ship will not be assessed. Once the shipyard finds that the ship meets the requirements set out above, it can move on to the next phase of the regulatory system: pre-market control.

Even if first-party conformity assessment has been performed, however, the ship cannot yet take its first passengers on board and set out on its maiden voyage; it must still obtain certificates attesting that the steel from which it was made meets the requirements of the standard referred to in the regulation; that the number of lifeboats meets the requirements; and that it has a contingency plan.

Let us assume that, as a high-risk product, the ship requires extremely stringent conformity assessment procedures. The shipyard should present the regulator with a certificate that the steel is of good quality or that appropriate contingency plans were indeed developed. But if the regulator does not trust the company that issued the certificate, then holding the certificate will not increase the chances that the ship is indeed safe, and will not result in permission being granted to take the first passengers on board. If, however, the cruise line presents the regulator with a certificate issued by a certification body that was in turn checked by an accreditation body and proven competent (i.e., an internationally accredited certification body), the chances are much greater that the certificate can be trusted.

Another important fact for the cruise line to consider is that the ship will travel abroad. Even if the countries of origin and of destination have similar requirements on contingency planning, this does not necessarily mean that the certificate issued in the country of origin will be accepted. A regulator is fully entitled not to trust another country's conformity assessment body if it has not checked the quality of that country's conformity assessment services. In this case, the cruise line may have to pay for additional certification in the country of destination, to be carried out by a certification body accredited by that country. If the new ship is certified by a conformity assessment body accredited by an accreditation body that, like its counterpart in the country of destination, participates in MLAs, a certificate issued in the country of origin will have to be accepted in the country of destination.

A key point of this example is that if legal metrology services are not available or are of poor quality, checks performed by the shipyard and by the conformity assessment bodies using the measuring instruments will not be reliable. And if the legal metrology services are not accredited internationally, even if they are reliable, they will not be recognized, thus resulting in additional costs.

To make sure that the results of measurement can be trusted, the shipyard needs to have its instruments calibrated or verified by a metrology institute and needs to be issued an official certificate indicating that this has been done. If these services are unavailable, the quality of the ship will not be assessed. Once the shipyard finds that the ship meets the requirements set out above, it can move on to the next phase of the regulatory system: pre-market control.

Even if first-party conformity assessment has been performed, however, the ship cannot yet take its first passengers on board and set out on its maiden voyage; it must still obtain certificates attesting that the steel from which it was made meets the requirements of the standard referred to in the regulation; that the number of lifeboats meets the requirements; and that it has a

contingency plan.

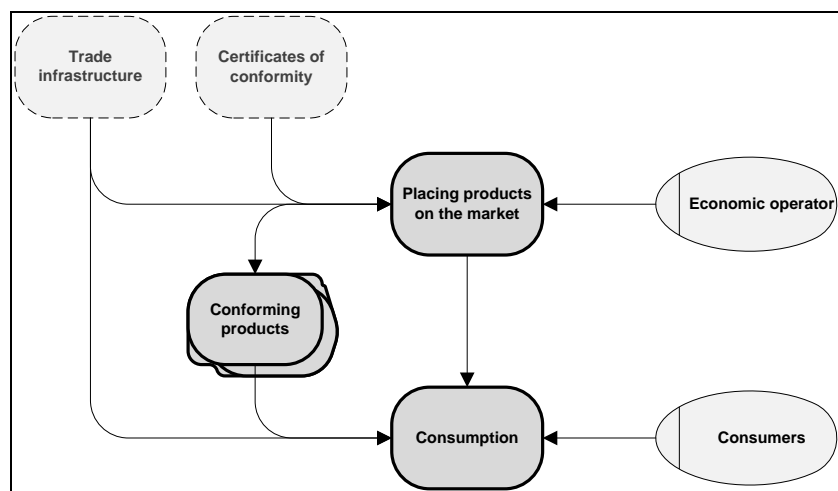
Let us assume that, as a high-risk product, the ship requires extremely stringent conformity assessment procedures. The shipyard should present the regulator with a certificate that the steel is of good quality or that appropriate contingency plans were indeed developed. But if the regulator does not trust the company that issued the certificate, then holding the certificate will not increase the chances that the ship is indeed safe, and will not result in permission being granted to take the first passengers on board. If, however, the cruise line presents the regulator with a certificate issued by a certification body that was in turn checked by an accreditation body and proven competent (i.e., an internationally accredited certification body), the chances are much greater that the certificate can be trusted.

Another important fact for the cruise line to consider is that the ship will travel abroad. Even if the countries of origin and of destination have similar requirements on contingency planning, this does not necessarily mean that the certificate issued in the country of origin will be accepted. A regulator is fully entitled not to trust another country's conformity assessment body if it has not checked the quality of that country's conformity assessment services. In this case, the cruise line may have to pay for additional certification in the country of destination, to be carried out by a certification body accredited by that country. If the new ship is certified by a conformity assessment body accredited by an accreditation body that, like its counterpart in the country of destination, participates in MLAs, a certificate issued in the country of origin will have to be accepted in the country of destination.

A key point of this example is that if legal metrology services are not available or are of poor quality, checks performed by the shipyard and by the conformity assessment bodies using the measuring instruments will not be reliable. And if the legal metrology services are not accredited internationally, even if they are reliable, they will not be recognized, thus resulting in additional costs.

5.5 Product market placement and consumption

Figure 5.8 Inputs, outputs and the main participants in product market placement



At the product market placement stage, the regulatory system provides economic operators with confirmation that the products and services indeed meet the requirements of the regulation and thus can be placed on local and international markets.

This phase of the regulatory system cycle is conducted primarily during trade-related procedures, including those required for product shipment, trade finance and so forth. At this stage, the regulatory system should provide special controls to ensure that only those economic operators which received all the necessary certificates and other proofs of conformity can place their products on the market. Although conformity assessment (as any other measure) cannot guarantee that non-compliant, unsafe or counterfeit goods will not be placed on the market, it does increase the chances that only those products which actually meet the requirements defined in the regulations will reach consumers.

Trade infrastructure is another major component needed for these processes to be efficient. International trade facilitation best practice in drafting legislation, organizing electronic data exchanges and the like can be found in the UNECE Recommendations on Trade Facilitation (www.unece.org/cefact/index.html).

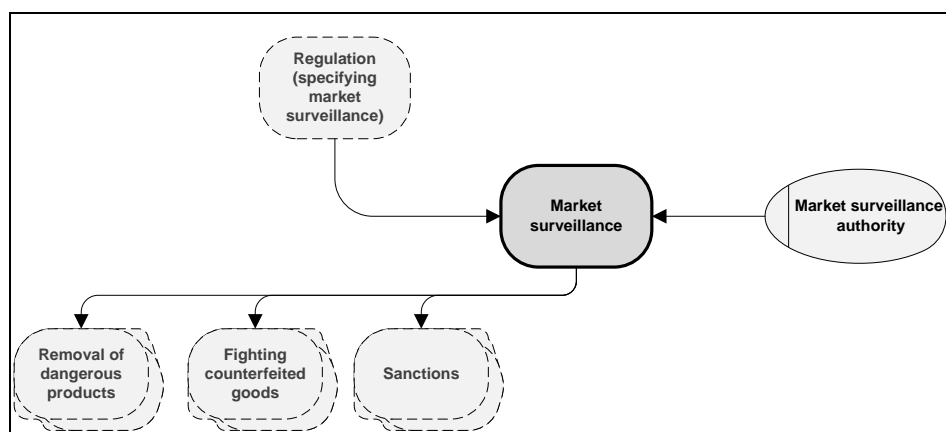
Building a cruise ship (9): the maiden voyage

At this point, the cruise line can start selling tickets and preparing for its maiden voyage. How this phase is organized has a major impact on the ship's competitiveness: if trade procedures are poorly designed, economic operators will not be competitive.

Assuming that the ship does eventually conform to all the requirements, its first trip will hopefully be more successful than that of the Titanic in 1912.

5.6 Post-market control: market surveillance

Figure 5.9 Inputs, outputs and the main players of market surveillance



Market surveillance is the last main component of the regulatory process and increases the overall value of the whole system. Despite the good quality of existing regulations and conformity assessment tools, from time to time dangerous and counterfeit goods – such as hazardous children's toys, contaminated milk, and bogus or faulty spare parts for cars – cause a public outcry on national markets worldwide. The proliferation of these products poses a serious threat to human health and the environment. It also undermines local industry, which is frequently unable to compete against a massive inflow of cheaper but inferior goods. Market

surveillance is the main regulatory response for ensuring that products placed on the market, whether imported or produced locally, conform to national technical regulations and are not counterfeit or pirated.

Market surveillance can be defined as “the set of activities carried out and measures taken by designated authorities to ensure that products comply with the requirements set out in relevant legislation and do not endanger health, safety or any other aspect of public interest protection” (UNECE, 2011a).

There are two fundamental reasons why countries need to develop an efficient market surveillance system:

1. To remove illegal and unsafe products from the market. Since conformity assessment that is conducted before products are placed on the market cannot prevent all faulty products from slipping through the net, public authorities must monitor products *after* they have been made available to buyers.
2. To ensure that market conditions are fair. Suppliers who follow the rules, bear the related administrative costs and put up with the delays should not be at a disadvantage vis-à-vis those who do not.

The example in the box below shows how appropriate market surveillance practices can help reduce the number of accidents in the workplace.

Occupational health and safety risks: Protecting the safety of workers

When the United States Occupational Health and Safety Administration (OSHA) began operations in the early 1970s it started work to promote established safety standards and reduce the rate of worker injury through tougher enforcement policies. Early evaluations of OSHA’s activities (1972 to 1975) found no evidence that the reported injury rate had been reduced by the increased risk of inspection and punishment for violations. As a result, OSHA shifted its enforcement policy to emphasize inspections and punishment in workplaces with a history of serious violations. After this shift in practice, OSHA achieved an estimated 5%-to-10% reduction (1975-1983) in the workplace injury rate (Viscusi, 1992).

Source: IRGC (2009)

Like conformity assessment (one of the previous phases of the regulatory system process), market surveillance is a form of market control. There are, however, significant differences between the two:

- Market surveillance is a form of *post*-market control, which begins when a product is placed on the market and may start as early as at the border, whereas conformity assessment is a form of *pre*-market control.
- Market surveillance is carried out by public authorities, while conformity assessment may be carried out by both public and private actors.
- Market surveillance is conducted solely to ensure that products comply with mandatory requirements, whereas conformity assessment (e.g. in the form of certification) has additional standards, such as audit criteria, based on both commercial and regulatory requirements.

As is the case with conformity assessment requirements for a particular market, market surveillance procedures should be defined in regulations. Within any regulatory system, assuming that resources are available, a regulator needs to strike the right balance between post-market and pre-market control. Assuming equal amounts of resources, market surveillance can

be less intensive where conformity assessment requirements are stringent. By the same token, a regulatory system may depend more on market surveillance when conformity assessment is not strict. Striking the right balance depends on the availability of resources, the nature of the market being regulated, and the efficacy of the State's conformity assessment and market surveillance infrastructure. In many sectors regulators are tending to move towards market surveillance (UNECE, 2004).

There are several internationally recognized guidelines on how to structure and conduct market surveillance. The EMARS (2010) handbook highlights the following principles to be implemented within the market surveillance framework of a regulatory system:

1. Taking a preventive approach to enforcement and employing effective communication strategies to advise and protect consumers and businesses
2. Using data capture and risk analysis to target unsafe products, services and practices and to set enforcement priorities
3. Taking a coordinated approach to enforcement programmes and practices to ensure greater operational efficiency and consistency
4. Dealing swiftly and proportionately with the problems identified to ensure that offending products, services and practices present the lowest possible risk
5. Resolving problems at source and in a coordinated manner by adopting a home/lead authority approach
6. Ensuring that market surveillance officials are appropriately trained, are aware of the economic context in which they operate, employ best practices and are supported by continuing professional development
7. Ensuring that all policies and strategies are relevant and clearly understood by means of an appropriate consultation process

The handbook also provides a thorough description of how to run a market surveillance system, based on the project management approach, and following widely recognized international best practice. It discusses such issues as project organization, human resources management, financial aspects, risk management and communication strategies. Other phases of market surveillance, including implementation, analysis of the results and planning follow-up actions, are considered as well. It then goes on to explain how to plan market surveillance projects, taking into account market surveillance vision, long-term programmes, Government safety policies and other key factors. Prioritizing the areas that require market surveillance is one of the most crucial tasks at this stage, and should be based on accident reports and statistics; reports from consumers, consumer organizations, the media, manufacturers, importers and retailers; and data from information systems and previous market surveillance activities. Another main task at the planning stage is to consolidate project management plans into an overall plan for market surveillance activities.

UNECE WP.6's Advisory Group on Market Surveillance (MARS Group) also developed a "General Market Surveillance Procedure" (GMSP) (UNECE, 2009b). This has a broader coverage than the EMARS handbook as it covers both consumer and non-consumer goods. It offers a process-based description of a market surveillance system and illustrates how market surveillance processes interface with other elements of a regulatory system. Like EMARS, the GMSP model stresses that if a market surveillance system is to be effective in countering the proliferation of dangerous and substandard goods, it will need adequate financial resources and a strong, shared political commitment. To simplify and optimize the tasks of market surveillance authorities, surveillance procedures need to be streamlined, while also allowing for sector-specific adaptations.

The GMSP proposes a holistic model that can be applied to all non-food products. The model breaks down the tasks of the authorities dealing with the various sectors into three phases:

- Preparation of a market surveillance plan
- Execution of the plan
- Contacts with stakeholders

According to the model, each phase is composed of a series of actions the authorities should undertake, which are outlined in detail. Some of them can entail multiple subprocedures, which are described in UNECE documents (e.g. UNECE, 2009b).

The GMSP provides the background for the UNECE “Recommendation on good practices in market surveillance policies” (UNECE 2011e). The recommendation stresses the need for international cooperation in the area of market surveillance, noting that “currently, due to the increasing volume and variety of products on the market, the number and seriousness of notifications about dangerous products and the technical complexity of regulations and standards, market surveillance authorities struggle to fulfil their mandate” of removing dangerous products from the market. Differences in surveillance practices across countries may compromise cross-border cooperation, to the detriment of fair competition, user safety and environmental protection. Thus the need to promote cooperation and harmonize market surveillance approaches internationally. This requires a new vision for a market surveillance system, one that can meet the challenges of global production chains and buck the trend to reduce the involvement of authorities in the pre-market phase.

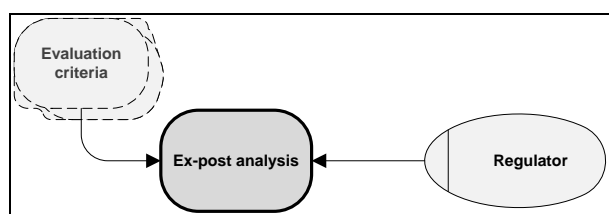
Building a cruise ship (10): Checking at ports of call

From time to time, the ship is checked by public authorities at its ports of call to provide additional guarantees that all the regulatory requirements have been met, including the updating of contingency plans on board, checking the number of lifeboats and ensuring that the quality of the steel complies with the standards.

If the requirements are not met, the cruise line may be fined or the ship may be taken off the market and not allowed to operate.

5.7 Ex-post analysis

Figure 5.10 Inputs, outputs and the main players of ex-post analysis



Ex-post analysis completes the regulatory system cycle and is performed after the regulations have been implemented. Its task is to examine “the relevance, effectiveness, and impacts of regulatory decisions, as well as [to identify] unintended outcomes, reasons for failure, and factors contributing to success. The results [of] this new regulatory management tool provide key knowledge input for decision makers, creating a feedback loop that completes the policy-regulatory cycle” (OECD, 2003).

Ex-ante analysis is based on hypothetical simulations and scenario analysis, while ex-post analysis is more evidence-based. Its overall objective is to review and improve existing regulations, although it can also be used as a tool for reviewing regulatory processes.

Ex-post analysis involves establishing a set of criteria for evaluating a regulatory system. (OECD, 2003), for example, cites “environmental efficiency” and “economic efficiency” as two of the main criteria for evaluating environmental policy instruments. It also proposes more specific criteria, such as administration costs. Evaluation criteria are largely determined by the substance of the regulatory system.

Ex-post analysis has already become systemic in many countries. According to the European Risk Forum, New Zealand’s Code of Good Regulatory Practice (CGRP) requires regulators to monitor regulations systematically for their continued compliance with their objectives. Canada’s Cabinet Directive on Streamlining Regulation (Canada, 2007) contains provisions on “measuring, evaluating and reviewing regulation”. It obligates departments and agencies to “collect performance information on the results of existing regulation and provide Canadians with this information in a timely manner”. Australia has also implemented a structured process for the ex-post evaluation of regulatory decisions.

As a result of the review process, regulators may decide to recommence the regulatory cycle presented in figure 4.4.

Building a cruise ship (11): Ex-post analysis – making sure all is well

In the ex-post analysis stage, the regulator identifies a set of criteria – including meeting the objectives of the regulatory system – for evaluating the regulatory impact of imposing requirements on the number of lifeboats, quality of steel and contingency planning. The regulator may want to know if a given regulation has led to changes in ticket prices or steel supply chains. If the regulator determines that the quality requirements for steel are too stringent or not stringent enough, the ex-post analysis will initiate changes in the regulation and bring us back to the first stage in the process – the drafting, assessment and implementation of regulations.

6 Risk management at UNECE WP.6



This publication has presented the main results of the risk management work under way in the UNECE Working Party on Regulatory Cooperation and Standardization Policies (UNECE WP.6) since 2009. This work has been entrusted since 2010 to the Working Party's Group of Experts on Risk Management in Regulatory Systems (UNECE GRM).

The goals of UNECE WP.6 include contributing to the “establishment of an open, equitable, rule-based, predictable and non-discriminatory multilateral trading and financial system”, as referred to in the Millennium Development Goals. Building efficient regulatory systems is a prerequisite for achieving this goal, and “promotion of best practices based on good governance principles with respect to technical regulations, standardization, conformity

assessment and related activities such as quality and environment management, consumer protection and market surveillance” is one of the Working Party's main activities. Most of UNECE WP.6's work is concentrated on regulatory systems and targets technical regulation in particular.

Technical regulation is indeed risk regulation: countries develop technical regulations and apply standards to guide production and service provision so that products and services do not pose unnecessary risks. Essential for providing safety, this complex process has a strong impact on economic development and international trade. Regulatory requirements should provide the required level of safety and at the same time not hamper business development and economic growth. In the context of international trade, technical regulation and standardization policies applied by countries should not create unnecessary obstacles and technical barriers.

Risk management and the promotion of regulatory convergence constitute two important and complementary areas of work of UNECE WP.6. By developing recommendations on the application of risk management tools in regulatory systems, the Working Party helps member States to develop regulations that are proportionate to the risks they address. By adding risk management to projects aimed at promoting regulatory cooperation and harmonizing regulatory systems, the Working Party contributes to eliminating technical barriers and unnecessary obstacles to trade without compromising safety.

A number of international organizations coordinate different aspects of cooperation among countries to avoid technical barriers to trade, which may be caused by different and sometimes conflicting regulations. This is one of the objectives of the WTO, specified in its Agreement on Technical Barriers to Trade (WTO, 1994b). The Agreement underlines that member States should apply international standards as a basis for regulations “except when such international standards would be ineffective or inappropriate”.

The International Model for Technical Harmonization developed by UNECE WP.6 (contained in its Recommendation “L”, UNECE 2001) takes regulatory cooperation to the next level, by assisting countries to adopt common regulatory objectives that are further used as a basis for harmonization and for the application of international standards. Common regulatory objectives, when approved by the Working Party, are reproduced in the national legislation of member States, thus removing some of the most common technical barriers to trade.

Common regulatory objectives are mutually agreed documents developed through a consultative process (in which the interested member States are engaged), registered by UNECE and made publicly available. By drafting common regulatory objectives, interested countries agree, *inter alia*, on such elements as:

1. Requirements for achieving regulatory objectives: including technical requirements with references to available international standards
2. Pre-market control provisions: establishing conformity assessment, e.g. in the form of a supplier’s declaration of conformity or certification
3. Post-market control provisions: describing market surveillance mechanisms for removing non-conforming products or services from the market

UNECE is currently engaged in a number of sectoral projects based on the International Model for Technical Harmonization. These projects include the TELECOM Initiative, the Sectoral Initiative on Earth-moving Machinery, the Initiative on Equipment for Explosive Environments and the Initiative on Pipeline Safety. They represent the highest possible degree of regulatory cooperation under United Nations auspices and aim at establishing fully harmonized technical regulations within their respective sectors.

At its twenty-first annual session, UNECE WP.6 approved two new recommendations, developed by the UNECE WP.6 Group of Experts on Risk Management in Regulatory Systems (GRM), for guiding regulatory stakeholders in the consistent and systematic application of risk management to regulatory systems. These recommendations are not sector-specific and can be applied across various fields.

The recommendations summarize the main results of the risk management work under way in UNECE WP.6 since 2009, which was presented in detail in previous chapters.

The first recommendation, entitled “Risk Management in Regulatory Frameworks”, and which reflects the main idea described in chapter 3, proposes a general model of a regulatory system in which the risk management process is the driving force behind the system, with regulation presented as just one of several options for managing risks. The second recommendation – “Crisis Management in Regulatory Frameworks” – focuses on how crisis management, an essential function of a risk management process, can be effectively integrated into a regulatory system.

These two recommendations result from previous activities of the Working Party, such as:

- The International Conference on Risk Assessment and Management, held back-to-back with the WP’s nineteenth annual session in 2009. The event drew more than 150 participants, representing Governments, international organizations, standardization bodies, conformity assessment bodies, market surveillance authorities and economic operators. The conference outcome document (ECE/TRADE/C/WP.6/2010/2) describes the roles of regulatory stakeholders in performing the various risk management functions within a regulatory system. It

is based on the idea that risks which affect society can be properly managed only if each stakeholder fulfils its function in the risk management process operating within a regulatory system.

- Development of a reference model for management of risks within a regulatory system. In following up on the issues raised at the 2009 conference, the Working Party secretariat in 2010 developed a model for building a regulatory system based on the risk management process. The model, which was subsequently presented at the Working Party's twentieth annual session, was used to develop a methodology for conducting a risk management needs assessment survey.
- Needs assessment survey. In order to gather more detailed information on the needs and problems faced by regulatory stakeholders in performing risk management functions, the Working Party secretariat conducted a risk management needs assessment survey (ECE/TRADE/C/WP.6/2010/5).

6.1 The UNECE Recommendation on risk management in regulatory frameworks

This recommendation lays out in detail the risk management roles of all the key actors in the regulatory process and shows how risk management functions can be incorporated into overall regulatory functions. Implementing the model involves developing a timely and comprehensive management of risks. This should be a “stand-alone” process, which may – but need not necessarily – result in the development or review of a regulation.

The recommendation calls for a more consistent and systematic application of risk management tools in regulatory work. The expected benefits are manifold. At a countrywide level, this recommendation emphasizes the fact that absolute safety is unattainable and that regulation – along with other means – necessarily strikes a balance between safety and measures that have costs both for consumers and citizens and for business operators. At the national, regional and international levels, a common understanding and assessment of risk will contribute to a more coherent and cohesive response, and to increased regulatory convergence.

The recommendation shows how the following risk management functions should be performed within a regulatory system:

- Setting the regulatory objectives
- Providing traceability in supply chains and management of assets
- Risk identification: identifying the risks to those assets (including intangible ones, like public health)
- Risk analysis and evaluation: understanding the most important risks
- Choosing risk treatment strategies
- Implementing risk treatment strategies
- Crisis management (including developing a plan to deal with disruption-related risk)
- Monitoring, reviewing and improving the risk management process

Some of these functions are commonly included in a description of the risk management process (see, for example, ISO 31000:2009, IEC/ISO 27001:2005 and COSO, 2004). As the names of the functions suggest, the recommendation does not contain anything new in principle, but rather adopts and systematizes risk management best practices so that they can be applied to a regulatory system.

In setting the regulatory objectives, the recommendation specifies that “absolute safety is not regarded as a regulatory goal” and that “regulatory objectives are used for setting the criteria against which the risk is evaluated”.

Providing traceability within regulatory frameworks, is closely linked to the management of risks and performs a function that is similar to the process of asset management within management systems. The recommendation states that “a process of communication and consultation of regulators with stakeholders [should] set out to identify the relevant assets or objects, which the framework sets out to protect”.

The recommendation also stresses that regulators should “cooperate effectively with other stakeholders in identifying risks, as it increases the resilience of the framework by reducing the chances that certain risks might be overlooked”, listing conformity assessment bodies, market surveillance authorities and business as participants, since they may “inform the regulator about risks that, in their view, require regulatory intervention”.

The recommendation is based on the notion that a regulator performs comprehensive risk identification on a systemic basis, which normally results in identification of many risks. As is the case in all risk management frameworks, the “risk identification” clause is hence followed by “risk analysis and evaluation”, which states that “no matter from which source a regulatory authority knows about a risk, a risk analysis and evaluation must follow, ranking the risk according to its seriousness” to ensure that “critical risks are dealt with in a timely manner”.

To assist regulators in determining a risk treatment strategy, the recommendation provides a regulator with four options to choose from. They include:

- (a) Avoiding the risk by banning activities or processes where it has occurred
- (b) Sharing the responsibility for managing the risk, including sharing responsibility, if it occurs, with economic or social actors (families, firms)
- (c) Mitigating the risk: developing a regulatory or non-regulatory response to reduce the probability and expected impact of a risk:
 - (i) A regulatory action implies not only developing a new or reforming an existing regulation, but also choosing appropriate conformity-assessment procedures and market-surveillance measures.
 - (ii) Non-regulatory action, on the other hand, includes options such as educational or information campaigns, and subsidies or incentives for appropriate activities by economic operators.

The recommendation reminds stakeholders that implementing risk treatment “requires monitoring compliance, evaluating the effect of a risk management treatment on other regulatory processes, other stakeholders and areas of activities. This involves:

- (a) Integrating the regulatory and other measures with existing processes;
- (b) Performing regulatory impact assessment;
- (c) Establishing coordinating mechanisms among competent authorities and stakeholders;

- (d) Giving guidance and establishing an appropriate budget for the institutions responsible for monitoring compliance (conformity assessment and/or market surveillance authorities);
- (e) Deciding on penalties for non-compliance.”

Given that “there are risks that are unavoidable and some are almost impossible to forecast”, the “crisis management” clause of the recommendation requires a regulator to “prepare a plan setting out: if the harm associated with the risk occurs, what is to be done, who should do it and how”. This clause of the recommendation establishes an interface with a separate document approved by UNECE WP.6 – the recommendation on crisis management in regulatory systems, described below.

An important clause of the recommendation on risk management in regulatory systems states that “all functions of the risk management process, as they are presented in the text of this recommendation, should be consistently described in legislation that lays out the regulatory framework at a general level or for a specific sector. Legislation should specify allocation of responsibilities for performing the risk management functions outlined in the model”. This clause is intended to help legislators improve the consistency of legislation when risk management is the driving force of a regulatory system. If the logic of the recommendation is followed, then important functions of the risk management process will not be omitted, which will already constitute a step forward in improving existing legislation and designing new legislation.

6.2 The UNECE recommendation on crisis management in regulatory frameworks

The second recommendation emphasizes the role of technical regulation, conformity assessment and market surveillance in preventing and addressing crises in various fields. It presents crisis management as “an integral part of the risk management process and of any regulatory framework”. It stresses that “some risks are almost impossible to identify, and that all risk, even if identified, cannot be totally mitigated”, and has “preventing situations where crises resulted in disproportionate regulations” as one of its major goals.

The recommendation calls for regulators to “design the crisis management function so that it provides effective coordination of the actions taken by various stakeholders, including conformity assessment bodies, market surveillance authorities, economic operators and citizens in a situation of a crisis”. One necessary step in designing such a function is to create a crisis management unit, endowed with the necessary resources, such as emergency funding, people with required skills, communication systems, etc.

Contingency plans are then presented as one of the means of crisis management. The recommendation urges regulatory authorities to “establish contingency plans and build contingent capacity that can be quickly released in a crisis to reduce the impact of the crisis situation”.

The recommendation takes into account the fact that many crises call for similar treatment. It accordingly emphasizes the need to develop both generic contingency plans with “general responses to risk, whether or not they were identified, to allow effective responses to any incidents in the early hours of a crisis”. Also, where appropriate, specific contingency plans (for risks that were identified at earlier stages) should be developed and processed within the system. Comprehensive analysis of crisis management best practice allowed the GRM to make a list of the most important elements to be covered in contingency plans.

Stressing the importance of communication and consultation processes in times of crises, the recommendation encourages regulators to prepare such processes in order to build awareness, confidence and understanding of crisis management processes by regulatory system stakeholders. These processes are even more important given that they allow regulators to effectively exchange information and consult with stakeholders in situations of crises, and, in particular, to provide information to stakeholders in the early hours of a crisis. The GRM was among the first to officially introduce to Governments the use of alternative media as an important means of communication with regulatory stakeholders.

The next part of the recommendation describes actions to be taken when a crisis occurs. Regulatory authorities should immediately focus on affected individuals, launch reliable data collection processes, activate a crisis management team and then organize a follow-up to a crisis. The follow-up is a function that builds a bridge between crisis management and the overall risk management process: regulatory authorities should analyse the causes of the crisis and the effectiveness and relevance of actions taken during the immediate response period, and data related to a crisis should constitute an input to regular risk identification performed within a regulatory framework.

6.3 The Group of Experts on Risk Management in Regulatory Systems (UNECE GRM)

The UNECE GRM has attracted a broad and diversified membership, created an Intranet site and developed technological solutions for organizing its work with limited resources. It has also contributed to the OECD recommendation on regulatory policy and governance and to the work of ISO Project Committee 262 on risk management.

Monthly webinars and electronic data exchanges have been the major forms of communication among GRM members. These activities enjoy high-level participation by representatives of a variety of regions and specialties, including all of the regulatory processes. The webinar reports are available on the Working Party's website, <http://www.unece.org/trade/wp6/riskmanagement.html>.

The GRM consists of 25 members (including two coordinators) from 13 countries as well as representatives of international organizations, including the World Bank, ISO, ITU and IEC (see Annex A for the list of members). Members of the Group represent the following areas of competence:

- Planning, developing and implementing technical regulations
- Choosing and implementing conformity assessment procedures
- Cooperation among businesses and regulators
- Risk management methodologies and standards
- Project management

The GRM is serviced by the secretariat of its parent body, the UNECE Working Party on Regulatory Cooperation and Standardization Policies.

6.4 Future plans

When developing its recommendations, the GRM did not create tools that had not existed previously, but rather systematized risk management best practice and laid out a framework that can be implemented in existing and newly designed regulatory systems.

There are many examples of inconsistencies related to risk management in existing legislation, and these discrepancies are even broader if one compares legislations in different sectors (Jachia and Nikonov, 2011a). The two recommendations described in this publication were developed so that they can be used by policy makers and legislators, both to check the consistency of existing legislation and in the development of new regulatory systems. We hope that these recommendations will help to improve regulatory processes and the management of the risks that confront our society.

The recommendations promote a common understanding of risk management by regulatory system stakeholders. Regulators can use them to establish a common risk language for use by all regulatory stakeholders and to develop a common risk management process for their regulatory system.

Businesses will also benefit from the implementation of these recommendations since they call for the active participation of business in regulatory processes, including calling the attention of regulatory stakeholders to risks that businesses and other economic operators cannot manage on their own.

The GRM also developed a comprehensive methodology for implementing the recommendations, which is described in chapter 7.

In the coming years, the GRM will continue developing recommendations on how to perform risk management functions, such as risk identification, risk analysis and evaluation. The Group also plans to run pilot implementation projects, starting with those sectors determined to be high priority by WP.6.

7 Evaluating risk management in regulatory systems

7.1 Introduction and objectives



This publication has attempted to promote and support change in the structure of regulatory systems – change that can be realized only through a well-managed portfolio of projects. In this chapter we will present a methodology for such a reform. The intention is to obtain an objective evaluation of the existing risk management practices of a regulatory system. Such an evaluation is a prerequisite to developing an action

plan for implementing risk management in a regulatory system.

Assessing the needs of regulatory stakeholders

The prototype for the models described in this publication was used by UNECE WP.6 in 2010 to perform a needs assessment survey of regulatory system stakeholders (UNECE, 2010c). That survey endeavoured to identify the outstanding needs of regulators, businesses, standardization and conformity assessment bodies, and other regulatory stakeholders in applying risk management tools to their work and in collaborating with other relevant parties. The reference models described in this publication were to a large extent designed as a response to the identified needs. The survey showed that these needs can be satisfied only if risk management is implemented on the level of a regulatory system as a whole. This finding provided insights for developing the reference models presented earlier.

The evaluation methodology is based on the reference model “Risk management in regulatory systems” (UNECE, 2010b). The proposed approach is similar to common management system auditing practices, except that instead of management system standards, the above-mentioned reference model is used as the basis for audit criteria.

The main phases of the evaluation project include the following:

1. Assigning responsibility and creating a working group
2. Preparing the evaluation: legislative analysis and training
3. Conducting the evaluation
4. Developing a project plan for implementing the reference models

In the following pages, we describe in more detail how the evaluation project could be carried out and offer some guidance for evaluators.

7.2 Assigning responsibility for the project

Once a regulatory system has been chosen, the next step is to assign responsibility and create a working group for the project. The project can be managed either internally (by an organization that functions within a regulatory system, e.g. a regulator) or externally (by policymakers or third-party organizations, such as international organizations, NGOs or consultants).

The managing organization should create a working group comprising the main representatives of regulatory system stakeholders. Evaluation of existing risk management practice will require the participation of all regulatory stakeholders, including regulatory authorities, standardization bodies, economic operators, conformity assessment bodies and market surveillance authorities. Other members can be added to conduct the preparatory tasks described in the table below.

Tasks	Outcome
Assigning responsibility	Responsibility for running a project is assigned to a given organization, either within or outside a regulatory system.
Creating a working group	The working group comprises the main stakeholders in regulatory system.

7.3 Preparing the evaluation

To gather objective evidence on risk management implementation, evaluators will need to conduct a series of interviews with the main regulatory system stakeholders. In preparing for the interviews, evaluators should gather preliminary data on how risk management issues are addressed within the regulatory system “on paper”. This can be done by analysing the legislation that establishes the regulatory system. It also helps in planning and structuring actual face-to-face interviews.

Before analysing the legislation, evaluators should gather all the legal documents with provisions on how the regulatory system should function. The idea is to see how each of the functions of the reference model is reflected in the legislation. The analysis should answer the following question: “Are risk management functions consistently described in the legislation establishing a regulatory system?”

Analysis of the legislation (which compares the legislation to the reference model) can lead to one of three major conclusions:

1. The legislation accurately describes the risk management process; the description is full and consistent (all functions are fully presented in the document in their logical sequence). In this case, evaluators will need to use the legislation to identify the key players and to plan the interviews. The purpose of the interviews is to elicit objective evidence on how these functions are actually implemented and whether anything hampers their implementation.
2. The legislation describes some of the functions of the risk management processes; however, the description is inconsistent and/or some functions are missing. In this case, the evaluator should use all the available information to structure the interviews and at the same time note which functions and terms are described inconsistently or are missing, so as to include them in the project plan.
3. The legislation does not cover risk management functions. In this case, the evaluator should identify all the key players in the regulatory system and use this information to structure the interviews. The task of restructuring the legislation should be added to the project plan.

In chapter 3, we discussed the example of the EU's food safety legislation. It was presented as a legal document that describes how risk management functions should be implemented within a regulatory system. This example can be used to get an idea of the possible outcomes of legislative analysis.

Once the key stakeholders in the regulatory system have been defined and the interview plan developed, evaluators should conduct a training session, with all of the system's key stakeholders assembled in one room. At the session, in order to perform the main risk management functions as described in chapter 3, the stakeholders should:

- Obtain theoretical information on risk management
- Analyse examples of how risk management is applied to regulatory systems
- Acquire important skills in performing the functions of the risk management process

The objectives of the evaluation and the interview plan should also be presented.

Tasks	Outcome
Legislative analysis	<p>Actions aimed at improving the legislation are defined.</p> <p>Respondents are identified and interviews structured and planned.</p>
Training	A common language and understanding of the project's objectives is established.

7.4 Evaluating the objectives of the regulatory system

The process for setting the objectives of the regulatory system was described in section 3.4, "Setting the objectives of the regulatory system and risk evaluation criteria". In order to evaluate how this function is performed, objective evidence is needed as to whether an established procedure exists for setting and updating the objectives of the regulatory system. An "established procedure" is one that has been developed, described and followed.

Evaluators are most likely to start the evaluation by asking the regulatory authority to show the documented procedure and the objectives of the regulatory system. If those objectives have not been set and there is no documented procedure describing the process, this should be identified as a significant gap and the corresponding tasks included in the project implementation plan. Other possible outcomes include the following:

- If respondents say that they know the objectives but that they are not listed in any document, the chances are high that there is no systematic process. This constitutes a major gap in the procedure for setting the objectives of the regulatory system.
- If such a procedure does exist, objective evidence should be gathered to show that it actually meets the requirements of the procedure. If not, the procedure should be redesigned and the changes included in the project plan.
- If there is no documented procedure, but the objectives of the regulatory system have in fact been set, the task of describing the process should be considered. This outcome represents a minor gap.

The objectives of the regulatory system should be known to other regulatory stakeholders, and an evaluator should consider asking economic operators, market surveillance authorities and other parties involved what the objectives are and how they receive information on them. If the objectives are not known, this can be considered as a major gap, and steps should be included in the project plan to improve the process.

7.5 Evaluating how assets are managed

To evaluate processes for asset management (described in section 3.5, “Management of assets”), the regulatory authority may first be asked about the most important assets within a regulatory system. If there are no processes for asset management, this should be noted as a significant gap.

If the process is well implemented, there should be some form of inventory (such as a database) of assets, and it should not be difficult to identify the most critical assets. If a regulatory authority applies risk management to a regulatory process without having implemented asset management, the evaluator should check how the priorities for risk identification are set. Inefficiencies in asset management can be considered as a major gap, as they may lead to incomprehensive risk identification.

Evaluators should also consider checking whether there is an established procedure for asset management (possible answers include “yes, and we use it”; “yes, but we don’t use it”; and “there is no procedure, and assets are not managed within the regulatory system”). An action plan should be developed depending on the answer, taking into account the information in section 3.5.

When analysing the asset management process, it is important to focus on which criteria are used for prioritizing the assets. These criteria could be the objectives of the regulatory system, among others. The criteria must be clearly defined – if they are not, this constitutes a minor gap – and if the assets are not prioritized, a process for doing so should be identified and implemented.

7.6 Evaluating risk identification

When evaluating the risk identification function, it is advisable to focus on the methods that are used to identify risks and also on stakeholder involvement. As mentioned in section 3.5, regulatory authorities should cooperate on risk identification with other stakeholders, since this makes the system more resilient.

Evaluators may ask regulatory authorities how they perform risk identification and how they analyse the most recent results of risk identification. One useful question may be, “what do you call the document that lists the risks?”, to see if risks are identified or not (the document can be a risk register, a risk profile, etc.). Another approach is to ask how comprehensive the risk identification usually is. If respondents have a clear picture of that, it means that the results of risk identification are analysed. To see how systematic the process is, respondents should be asked how often risk identification is performed. If there is no objective evidence as to systematic risk identification within a regulatory system, this can be considered a significant gap.

Other regulatory stakeholders may be asked similar questions. It is useful to determine how businesses, market surveillance authorities and standardization bodies are involved in risk identification (the more parties involved, the more comprehensive the results). To elicit objective evidence, evaluators may ask regulatory authorities how all of these parties inform them about a risk that businesses have perceived in their respective area of work. Evaluators may also ask how

many risks have been reported by economic operators and other stakeholders. The lack of stakeholders' participation can be considered a major gap.

Risk identification can be described as a separate function or as part of the risk management process. In either case, evaluators should obtain objective evidence that the process is being applied. If the methodology exists but there is sufficient evidence that it is not used, most probably it was set out only in writing. If risks are actually identified, it is important to verify if the risk identification methodology is systematically analyzed and improved.

It is important to focus on the link between asset management and risk identification. If risks are not identified starting with the most significant assets, this can be considered a major gap.

7.7 Risk evaluation

Risk quantification and assessment is one of the most complicated steps in the risk management process, and errors in risk quantification can compromise the results of risk management and lead to poor decisions on risk management strategies. For the purposes of the evaluation project, we need to know if there is a consistent methodology in place for considering the established objectives of the regulatory system and comparing the identified risks with one another.

In order to elicit objective evidence that risks are indeed analysed, evaluators can ask regulatory authorities to name the 10 most crucial risks and explain why they were considered the most crucial. The same question can be addressed in parallel to other regulatory stakeholders in order to show the level of consistency of the applied methodology. If risks are not prioritized, this is a significant gap.

If risks are analysed, the next field of the evaluation should be the methodology used for risk analysis. Having a methodology in place for risk quantification and assessment is a prerequisite for choosing appropriate, balanced risk management strategies. If there is no such methodology, this is a major gap, and the organization may require assistance in developing and implementing one. To elicit objective evidence as to the existence of a methodology, evaluators can ask which methods are applied in risk evaluation (consequence-probability matrix, risk indices, etc.). Some methods that can be used to evaluate risks are described in section 2.4.3, "Risk analysis and evaluation".

If a methodology exists for risk quantification, it is important to identify who is responsible for developing and maintaining it. This could be a risk officer or any other staff member, but whoever it is, we need to know if that person has actually been assigned that responsibility. If no one has been assigned, this can be considered a minor gap.

7.8 Evaluating how risk treatment strategies are chosen

Questions about the next function of the risk management process – choosing risk treatment strategies – follow the same pattern as those for risk identification and quantification. If there is no systematic process for selecting risk treatment strategies, this is a significant gap.

It is important to focus on the methodologies that are applied for selecting risk treatment strategies. A methodology should determine who is participating in decision-making, which parameters are analysed, and so forth. If there is no methodology in place, this should also be considered as a major gap.

Evaluators should also deal with one of the fundamental risk management challenges, which is to determine an acceptable level of risk. During the evaluation, it is not necessary to compare how this function is performed with any best practice. The idea is to obtain objective evidence that the issue is indeed recognized by a regulatory authority. Evaluators can ask regulatory authorities and other stakeholders if there are agreed criteria for tolerating risks in a system. If the answer is yes, it is advisable to ask for examples and for the percentage of risks that have been accepted within a certain period of time. If the answer is no, this should be considered a significant gap. Approaches to the application of the objectives of the regulatory system to determine an acceptable level of risks are described in section 3.4.

Similar questions can be addressed to regulatory authorities with regard to other risk treatment strategies in order to obtain objective evidence that tools and methods for choosing risk treatment strategies (discussed in section 3.8) are indeed applied. The lack of evidence of application of such tools can be considered a major gap.

Attention should further be given to how other regulatory stakeholders participate in the process. If their opinions are not taken into account, this should be considered a major gap.

In order to evaluate how risks trigger new regulations, evaluators may ask regulatory stakeholders for examples of how regulations can be associated with the risks they were set out to address. Examples of such linkages will not provide objective data but will create an impression of how risk management philosophy is utilized within a system. In order to obtain additional proof that the concept is applied, evaluators may ask for examples of situations in which tools other than regulations were used to mitigate the identified risks. If such examples are lacking, this can be considered a major gap, and should give rise to further analysis.

7.9 Evaluating how risk treatment strategies are implemented

In evaluating this function, evaluators should concentrate on analysing situations in which regulations were chosen as risk mitigation tools. The reference model presented in chapter 4 can be used as a basis for the questionnaire.

In order to obtain objective evidence that this function is being performed, evaluators should consider interviewing conformity assessment bodies, market surveillance authorities and economic operators. They should focus on the proportionality of regulatory requirements to the risks they were set out to address and on the efficiency of pre- and post-market controls.

Regulators may be asked to provide examples of how they assess the risks that an envisaged regulation could have on various economic parameters, such as trade and market structure. Evaluators should also try to identify the parties responsible for managing the risks that might arise when imposing a regulation. They can be asked about the applied methodologies. Any lack of regulatory impact assessment would be a significant gap in the system.

Regulators should be asked to show how risk management tools are used for choosing conformity assessment procedures. If risk management is not applied in making this choice, it should be considered a major gap. Similar questions should be addressed to market surveillance authorities.

Questions addressed to conformity assessment bodies, market surveillance authorities and economic operators in order to obtain objective evidence that the conformity assessment and market surveillance procedures indeed help mitigate risks can be easily derived from the reference model in chapter 5.

7.10 Evaluating crisis preparedness

To evaluate the level of crisis preparedness of a regulatory system, evaluators may ask which crisis management tools are applied. If, for example, contingency plans have not been developed, this exposes a major gap, and implementation of international best practice should be recommended.

Evaluators should also focus on the crisis management roles assigned to the staff of a regulatory authority. If there is no crisis unit and crisis management methodologies have not been developed, this can be considered as a major gap. Economic operators and other stakeholders can provide important data on previous crises, which will permit critical decisions to be made on the status of crisis management within the regulatory system. International best practice on crisis management can be found in sections 2.4.5 and 3.10.

7.11 Evaluating the improvement of risk management processes

The last set of questions should be addressed to regulatory authorities in order to determine whether risk management processes are subject to review and continual improvement. Evaluators should ask for examples of the results of risk management practice reviews. The lack of analysis of risk management procedures can be considered a significant gap in the system.

The end result of an evaluation project is to help regulatory stakeholders improve the regulatory system. The following open-ended questions should therefore be addressed to all respondents to give them an opportunity to list their needs and the areas in which they would like assistance:

<p>Please list the main obstacles you face in the application of risk management tools to the regulatory process:</p> <p>a. In setting regulatory objectives: _____</p> <p>b. In asset management : _____</p> <p>c. In risk identification: _____</p> <p>b. In risk quantification: _____</p> <p>c. In selecting a risk treatment strategy: _____</p> <p>d. _____</p> <p>Other: _____</p>
--

Tasks	Outcome
Evaluation of risk management functions	Identification of significant, major and minor gaps, on the basis of which an implementation project can be planned
Identifying the risk management-related needs of regulatory stakeholders	Identification of stakeholders needs and of relevant tasks necessary to meet those needs

8 Conclusions



Managing risks through regulations is not a new concept. The Code of Hammurabi – perhaps the oldest existing set of laws – provided that if a builder does not construct a house properly and the homeowner dies as a result, the builder should be put to death.

Since then, a large body of literature has been produced on the nexus between risk and regulations, most of which describes how risk management tools can be used by regulators. This publication has set out to expand that nexus. It introduces a broader paradigm in which regulation is presented as just one of several options for managing risks, with regulatory systems driven by the risk management process.

We have not endeavoured to analyse existing regulatory models or the collective experience of Governments and societies in managing risks. Instead, we have chosen to present a practical methodology that allows a regulatory system to be structured as a set of processes whose objectives, inputs and outputs are centred on mitigating risks.

These processes include setting regulatory requirements and performing pre- and post-market control to achieve regulatory objectives. We have analysed them in terms of their relationship the processes necessary for creating economic value. We have then produced a systematic representation of this process that includes its essential functions and embeds risk management concepts in regulatory actions.

Our methodology is designed to consider risks – along with societal expectations and national development goals – in the setting of regulatory requirements. It is also intended to help identify proportionate requirements when drafting laws and regulations. We have provided an overview of the actions taken when implementing a regulation in order to ensure that the actions are assigned to well-defined regulatory stakeholders. This makes them

responsible for safety in the regulated market and helps meet regulatory objectives. We have further integrated pre- and post-market controls into a model of a regulatory system so that the controls are fitted to the risks presented by a given product, service or production process.

The publication has drawn heavily on international standards. It has taken risk management standards and tools that were originally developed for and by business and applied them to the context of regulatory systems. It has also introduced a number of examples and tools to make the methodology easily applicable to the practice of policymakers.

We hope that these methodologies and tools will help stakeholders manage regulatory system reforms that protect citizens and communities without stifling innovation and growth. The ultimate result should be a better understanding of risks, better decision-making in situations of uncertainty, and increased crisis preparedness.

ANNEX

List of members of the UNECE GRM, at the time of publication

The Group is chaired by Mr. Kevin Knight and coordinated by Mr. Donald Macrae and Mr. Valentin Nikonov.

At the time of publication, members of the GRM included the following (for updates, see http://www.unece.org/fileadmin/DAM/trade/wp6/AreasOfWork/RiskManagement/ListOfMembers_Dec2011.pdf):

1. Mr. Alberto Alemanno (Professor of Law, Ecole des Hautes Etudes Commerciales (HEC), France)
2. Mr. Lorenzo Allio (European Risk Forum)
3. Mr. Gabriel Barta (International Electrotechnical Commission)
4. Mr. Eugenio Belinchón Güeto (Endesa, Spain)
5. Mr. Florentin Blanc (World Bank Group)
6. Mrs. Bo Yumin (National Accreditation Service for Conformity Assessment (CNAS), China)
7. Mr. A.M. Dolan (University of Toronto, Canada)
8. Mr. Graeme Drake (ISO/Comité pour l'évaluation de la conformité (CASCO))
9. Mr. Valery Hurevich, (BelGISS, Belarus)
10. Mr. Phil Kelly (Liverpool Business School, United Kingdom)
11. Mr. Kevin Knight (Chair of the ISO Technical Committee responsible for ISO 31000, Australia)
12. Mr. Sean MacCurtain (ISO/CASCO)
13. Mr. Donald Macrae (Coordinator of the GRM, United Kingdom)
14. Mr. Peter Morfee (Ministry of Economic Development, New Zealand)
15. Mr. Valentin Nikonov (Coordinator of the GRM, Russian Federation)
16. Mr. Massimo Polignano (Esaote, Italy)
17. Mr. Christophe Renard (Cotecna, Switzerland)
18. Mr. Mikhail Rogov (RusRisk, RusHydro, Russian Federation)
19. Mr. Dan Roley (Caterpillar, United States)
20. Mr. Marc Schädeli (Group Risk Management, Nestlé)
21. Mr. Paul Taylor (Federation of the European Risk Management Associations (FERMA), United Kingdom)
22. Mr. Olivier Testoni (ITU)
23. Mr. Jan van Tol (Ministry of Interior and Kingdom Relations, the Netherlands)
24. Mr. Simon Webb (The Nicholas Group, United Kingdom)
25. Ms. Carolyn Williams (Institute of Risk Management, United Kingdom)

References

- AS/NZS 3806:2006. Compliance programmes, Sydney.
- AS/NZS 5050:2010. *Business continuity – Managing disruption-related risk*. Sydney.
- Avanesov, Evgeny (2009). Risk Management in ISO 9000 Series of Standards. Paper presented at the International Conference on Risk Assessment and Management. Geneva, November.
- Baldwin, Robert (1999). *Understanding regulation: Theory, strategy and practice*. New York: Oxford University Press.
- Bernstein, Peter L. (1996). *Against the Gods: The Remarkable Story of Risk*. New York: John Wiley & Sons.
- BIS (2001). *History of the Basel Committee and its Membership*. Basel Switzerland.
- BIS (2010). *International regulatory framework for banks (Basel III)*, Basel Switzerland.
- Breggin, Linda et. al. (2009). Securing the promise of nanotechnologies. Towards transatlantic regulatory cooperation. Available from http://personal.lse.ac.uk/Falkner/_private/Nanotech%20report%20Sept%202009.pdf
- Canada (2007). *Cabinet Directive on Streamlining Regulation*. Available from www.tbs-sct.gc.ca/ri-qr/directive/directive-eng.pdf.
- Commission of the European Communities (2000). Communication from the Commission on the Precautionary Principle. COM(2000)1. p2 February. Available from http://ec.europa.eu/dgs/health_consumer/library/pub/pub07_en.pdf
- COSO (2004). *Integrated Risk Management Framework*, available from <http://www.coso.org/IC-IntegratedFramework-summary.htm>
- DCMAS (2010). Building corresponding technical infrastructures to support sustainable development and trade in developing countries and countries in transition. Background paper. Available from http://www.dcmas.net/public-docs/background_paper_2005.pdf.
- Downer, John (2009). “When failure is an option: Redundancy, reliability and regulation in complex technical systems”, Discussion Paper 53, Centre for Analysis of Risk and Regulation (CARR), the London School of Economics
- EMARS (2010). *Best practice techniques in market surveillance*. Brussels: PROSAFE. Available from http://www.prosafe.org/read_write/file/EMARS_Best_Practice_Book.pdf.
- European Commission (2008). *Handbook on the Implementation of EC Environmental Legislation*. Available from <http://ec.europa.eu/environment/enlarg/handbook/horizontal.pdf>.
- European Commission (2010). Smart Regulation in the European Union. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM(2010) 543 final. 8 October. Available from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0543:FIN:EN:PDF>.
- European Communities (2002). Food Safety Regulation of the European Union. Regulation (EC) No. 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety

Authority and laying down procedures in matters of food safety. Official Journal of the European Communities. 1.2.2002. Available from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:031:0001:0024:EN:PDF>.

European Union (2006). Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC, available from: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:396:0001:0849:EN:PDF>

European Union (2008a). Regulation (EC) No 762/2008 of the European Parliament and of the Council of 9 July 2008 on the submission by Member States of statistics on aquaculture and repealing Council Regulation (EC) No 788/96. Official Journal of the European Union. 13.8.2008. Available from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0082:012:en:PDF>.

European Union (2008b). Regulation (EC) No 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

Hansen, K (2007). NASA keeps an eye on ozone layer amid Montreal Protocol's success, September 13, 2007, http://www.nasa.gov/vision/earth/environment/montreal_protocol.html

IEC/ISO (2011) Directives, Part 2, 2011, *Rules for the structure and drafting of International Standards*. Edition 6.0, Geneva.

IEC/ISO 27001:2005. *Information technology — Security techniques — Information security management systems — Requirements*. Geneva

IEC/ISO 31010:2009. *Risk management – Risk assessment techniques*. Edition 1.0, Geneva.

ISO 9000:2005. *Quality management systems — Fundamentals and vocabulary*. Edition 3.0, Geneva.

ISO 14001:2004. *Environmental management systems -- Requirements with guidance for use*, Geneva.

Impact Alliance (2010). Croatia – Successful creation of an enabling business environment. Available from http://www.impactalliance.org/ev_en.php?ID=49144_201&ID2=DO_TOPIC.

Inklaar, Alex (2009). *Technical regulations. Recommendations for their elaboration and enforcement*. Guide No. 1/2009. Physikalisch Technische Bundesanstalt (PTB) and International Trade Centre (ITC).

IPMA (2012). International Competence Baseline. Available from www.ipma.ch

IRGC (2006). *Risk Governance: Towards an Integrative Approach*. Geneva.

IRGC (2009). *Risk Governance Deficits: An analysis and illustration of the most common deficits in risk governance*. Geneva.

ISO/IEC 17000:2004. *Conformity assessment -- Vocabulary and general principles*. Geneva.

ISO 20000:2005. *Information technology - Service management*. Geneva.

- ISO 22005:2007. *Traceability in the feed and food chain – General principles and basic requirements for system design and implementation*. Geneva.
- ISO 9001:2008. *Quality management systems – Requirements*. Geneva.
- ISO Guide 73:2009. *Risk management — Vocabulary*, Geneva.
- ISO 31000:2009. *Risk management – Principles and guidelines*, Geneva.
- ITC (2004). *Roadmap for Quality: Guidelines for the Review of the Standardization, Quality Management, Accreditation and Metrology (SQAM) Infrastructure at National Level*. Geneva.
- Jachia, Lorenza and Valentin Nikonov (2010). “Application of risk-based management system standards to the design of regulatory systems”, *EURAS Proceeding 2010*, ed. J.C. Graz and K. Jakobs.
- Jachia, Lorenza and Valentin Nikonov (2011a). “Applying risk management concepts in the design of legislation. Published in “*Organizational and regulatory issues of public-private cooperation for trade facilitation*” (materials from the Sixth International UNECE-EurAsEC seminar on Trade Development and Facilitation, 8 October 2010, Geneva).
- Jachia, Lorenza and Valentin Nikonov (2011b). Effective regulatory processes for crisis management: an analysis of codified crisis management in Europe. In *Governing disasters: the challenges of emergency risk regulation*, Alberto Alemanno, ed. Cheltenham, England: Edward Elgar Publishing Ltd., 2011.
- Kaufmann, Daniel and Tessada, José (2010). Natural Disasters, National Diligence: The Chilean Earthquake in Perspective
http://www.brookings.edu/opinions/2010/0305_chile_earthquake_kaufmann.aspx
- Kates, Robert W., Cristoph Hohenemser and Jeanne Kaspersen (1985). *Perilous Progress: Managing the Hazards of Technology*. Boulder, Colorado: Westview Press.
- Klotz-Engmann, Gerold (2010). Presentation made at the twentieth annual session of the WP.6. Available from
<http://live.unece.org/fileadmin/DAM/trade/wp6/documents/2010/Presentations/Klotz-Engmann.pdf>.
- Knight, Kevin (2011). Presentation made at the GRM webinar. 2 May.
- Kogan, Irena and Valentin Nikonov (2009). How can ISO management system standards contribute to mitigate business risks? Paper presented at the International Conference on Risk Assessment and Management, Geneva, November.
- Lloyds Bank (2011). *Business Risk Report*. Available from
<http://www.lloydsbankwholesale.com/economic-reports/risk-report-april-2011/>.
- Macrae, Carl (2007). Analyzing Near-Miss Events: Risk Management in Reporting and Investigation Systems. Discussion Paper No. 47. London: London School of Economics, Centre for Analysis of Risk and Regulations. Available from
<http://www2.lse.ac.uk/researchAndExpertise/units/CARR/publications/dpAbstracts.aspx>.
- Macrae, Donald (2011). Standards for risk assessment of standards: how the international community is starting to address the risk of the wrong standards. *Journal of Risk Research*, vol. 14, Issue 8 (September), pp. 933-942.

- Mattli, Walter and Ngaire Woods, eds. (2009). *The Politics of Global Regulation*. Princeton, New Jersey: Princeton University Press.
- Michel-Kerjan, Erwann (2009). Hedging Against Tomorrow's Catastrophes. In *Learning from Catastrophes: Strategies for Reaction and Response*. Michael Useem and Howard Kunreuther, eds. Wharton School Publishing.
- Moeller, Robert R. (2007). *COSO Enterprise Risk Management Framework. Establishing effective governance, risk and compliance processes*. New York: John Wiley & Sons.
- Molina, Mario J. and Rowland, Frank S., Stratospheric sink for chlorofluoromethanes: chlorine atomcatalysed destruction of ozone, *Nature*, 249, June 28, 1974, 810-12.
- Nano (2009). Report calls for global mandatory register for nanomaterials. Available from http://www.nanomagazine.co.uk/index.php?option=com_content&view=article&id=252:report-calls-for-global-mandatory-register-for-nanomaterials&catid=38:nano-news&Itemid=159.
- Netherlands (2010). Ministry of the Interior and Kingdom Relations, Central Government Reform Programme *Day of Risks: Conference Proceedings*. Available from <http://www.vernieuwingrijksdienst.nl/english/>.
- New Zealand (2006). Ministry of Economic Development, *Code of Good Regulatory Practice*. Available from: http://www.med.govt.nz/templates/MultipageDocumentTOC____22149.aspx.
- Nikonov, Valentin (2008). Applying ISO management system standards to enterprise risk management. ISO Management Systems. Special Report. January-February 2008.
- Nikonov, Valentin (2009a). *Risk Management*. Moscow: Alpina Business Books (in Russian).
- Nikonov, Valentin (2009b). Russian banks improves information security with ISO/IEC 27001. *ISO Management Systems*. September-October 2009.
- Nikonov, Valentin (2010). Trade Facilitation and Regulatory Cooperation Needs Assessment Project for Belarus. ECE/TRADE/C/NONE/GE.10-25413.
- Obama, Barack (2011). Toward a 21st Century Regulatory System. *Wall Street Journal*, 18 January 2011. Available from <http://online.wsj.com/article/SB10001424052748703396604576088272112103698.html#mjQuickSave>.
- OECD (1997a). *Regulatory Impact Analysis – Best Practices in OECD Countries*. Paris.
- OECD (1997b). *Ten good practices in the design and implementation of RIA*. Paris.
- OECD (2003). Proceedings from the OECD Expert Meeting on Regulatory Performance: Ex Post Evaluation of Regulatory Policies. Available from www.oecd.org/dataoecd/34/30/30401951.pdf.
- OECD (2005). *RIA in OECD Countries and Challenges for Developing Countries*. Paris.
- OECD (2007). *Indicators of Regulatory Management Systems*. Paris.
- OECD (2008a). *Building an Institutional Framework for Regulatory Impact Analysis: Guidance for Policy Makers*. Paris.
- OECD (2008b). *Introductory Handbook for Undertaking Regulatory Impact Analysis*. Paris.

- OECD (2009). *Regulatory Impact Analysis: A Tool for Policy Coherence*. Paris.
- OECD (2010a). *Regulatory Policy and the Road to Sustainable Growth. Draft Report*. Paris.
- OECD (2010b). *Risk and Regulatory Policy: Improving the Governance of Risk*. Paris.
- OECD (2010c). *Regulatory Policy: Towards a New Agenda. Pathways to the future*. Available from <http://www.oecd.org/dataoecd/57/22/47298590.pdf>
- OECD (2012). Recommendation of the Council on Regulatory Policy and Governance. Available from <http://www.oecd.org/dataoecd/45/55/49990817.pdf>
- Project Management Institute (2008). *A guide to project management body of knowledge: PMBOK Guide*, 4th edition. Newtown Square, Pennsylvania.
- RRAC (2009). *Response with responsibility, Policy-making for public risk in the 21st century*. London UK. Available from <http://www.berr.gov.uk/files/file51459.pdf>
- Sacchetti, Fabrizio (2010a). Experience of the European Union. Presentation made at the twentieth annual session of the WP.6. Available from http://live.unece.org/fileadmin/DAM/trade/wp6/documents/2010/Presentations/Sacchetti_ca.pdf.
- Sacchetti, Fabrizio (2010b). Using risk management. Presentation made at the twentieth annual session of the WP.6. Available from http://live.unece.org/fileadmin/DAM/trade/wp6/documents/2010/Presentations/Sacchetti_ca.pdf.
- Slovic, Paul and Elke U. Weber (2002). Perception of Risks Posed by Extreme Events. Paper presented at the conference on Risk Management Strategies in an Uncertain World. Palisades, New York, April. Available from www.sfu.ca/media-lab/archive/2004/226jan2004/notes/slovic_wp.pdf.
- Smith, Becca (2011). Risk Management in Non-DoD US Government Agencies and the International Community. Paper presented on behalf of the Center for Strategic & International Studies at the UN ERM workshop. June.
- Stigler, George J. (1971). The theory of economic regulation. *The Bell Journal of Economics and Management Science*, vol. 2, No. 1 (Spring), pp. 3-21. Available from www.giuripol.unimi.it/Materiali%20Didattici/Regolazione%20dei%20Mercati%20-%20Ammannati/STIGLER_economicRegulation.pdf.
- Sunstein, Cass R. (2011). Economic growth and public protection. Statement to the APEC Senior Officials Meeting. Washington, D.C., 15 March. Available from <http://www.whitehouse.gov/sites/default/files/omb/inforeg/speeches/economic-growth-public-protection-03152011.pdf>
- UNECE. Group of Experts on Risk Management in Regulatory Systems. Webinar Reports. Available from www.unece.org/trade/wp6/riskmanagement.html.
- UNECE (2001). Recommendation L: International Model for Technical Harmonization Based on Good Regulatory Practice for the Preparation, Adoption and Application of Technical Regulations via the Use of International Standards. Note by the secretariat. Available from www.unece.org/fileadmin/DAM/trade/wp6/Recommendations/Rec_L.pdf.
- UNECE (2004). *Market Surveillance in the UNECE Region*. (United Nations publication, Sales No. E.04.II.E.4).

UNECE (2009a). Outcome of the International Conference on Risk Assessment and Management, Geneva, 24-26 November 2009. Available from www.unece.org/fileadmin/DAM/trade/wp6/documents/2009/ConfRisk_Finaloutcome.pdf .

UNECE (2009b). Market surveillance: Draft guide to the use of the general market surveillance procedure. ECE/ TRADE/C/WP.6/2009/12. Available from www.unece.org/fileadmin/DAM/trade/wp6/documents/2009/wp6_09_GMS_012E.pdf .

UNECE (2009c). Market surveillance: General concept and how it relates to the activities of the Working Party. Note by the secretariat. ECE/TRADE/C/WP.6/2009/11. Available from www.unece.org/fileadmin/DAM/trade/wp6/documents/2009/wp6_09_011E.pdf .

UNECE (2010a). Risk assessment and management in the activities of the Working Party. Note by the secretariat. ECE/TRADE/C/WP.6/2010/2. Available from www.unece.org/fileadmin/DAM/trade/wp6/documents/2010/wp6_10_02e.pdf .

UNECE (2010b). Risk management in regulatory systems: a proposed reference model. Note by the secretariat. ECE/TRADE/C/WP.6/2010/3. Available from www.unece.org/fileadmin/DAM/trade/wp6/documents/2010/wp6_10_03e.pdf .

UNECE (2010c). Risk management in regulatory systems: a proposed survey. Note by the secretariat. ECE/TRADE/C/WP.6/2010/4. Available from www.unece.org/fileadmin/DAM/trade/wp6/documents/2010/wp6_10_04e.pdf .

UNECE (2010d). Report of the Working Party on Regulatory Cooperation and Standardization Policies on its twentieth session. Note by the secretariat. ECE/TRADE/C/WP.6/2011/20. Available from www.unece.org/fileadmin/DAM/trade/wp6/documents/2010/wp6_10_020e.pdf .

UNECE (2011a). *A Glossary of Market Surveillance Terms*. ECE/TRADE/389. Available from www.unece.org/fileadmin/DAM/trade/Publications/WP6-MARS-Glossary-389_EFR.pdf .

UNECE (2011b). “Recommendation on Risk Management in Regulatory Systems”. Available from <http://www.unece.org/trade/wp6/recommendations/recommendations.html>.

UNECE (2011c). “Recommendation on Crisis Management in Regulatory Systems”. Available from: <http://www.unece.org/trade/wp6/recommendations/recommendations.html>.

UNECE (2011d). “Report on the activities of the Group of Experts on Risk Management in Regulatory Systems” (GRM). Note by the secretariat. ECE/TRADE/C/WP.6/2011/3. Available from www.unece.org/fileadmin/DAM/trade/wp6/documents/2011/WP6_2011_3e.pdf .

UNECE (2011e). “Recommendation on good practices in market surveillance policies”. Available from www.unece.org/fileadmin/DAM/trade/wp6/Recommendations/Rec_N_Eng.pdf

United Nations Conference on Environment and Development, (1992). *Rio Declaration on Environment and Development*. Available from <http://www.unep.org/Documents.Multilingual/Default.asp?documentid=78&articleid=1163>.

United Kingdom (2008). Better Regulation Executive Department for Business, Enterprise and Regulatory Reform, *Code of Practice on Consultation*, London, Available from: <http://www.bis.gov.uk/files/file47158.pdf>

United States (2002). *Sarbanes-Oxley Act*, Available from: <http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf>

- United States (2010). *Food Safety Modernization Act*, Available from <http://www.gpo.gov/fdsys/pkg/PLAW-111publ353/pdf/PLAW-111publ353.pdf>
- United States (2011). *Improving Regulation and Regulatory Review - Executive Order 13563*. Available from <http://www.gpo.gov/fdsys/pkg/FR-2011-01-21/pdf/2011-1385.pdf>
- United States (2012a). *Promoting International Regulatory Cooperation - Executive Order 13609*, Available from <http://www.gpo.gov/fdsys/pkg/FR-2012-05-04/pdf/2012-10968.pdf>
- United States (2012b). *Identifying and Reducing Regulatory Burdens- Executive Order 13611* Available from: <http://www.whitehouse.gov/the-press-office/2012/05/10/executive-order-identifying-and-reducing-regulatory-burdens>
- USAID (2002). *What Happened in Uganda? Declining HIV Prevalence, Behavior Change, and the National Response*. Janice A. Hogle, ed. Available from www.usaid.gov/our_work/global_health/aids/Countries/africa/uganda_report.pdf .
- Viscusi, W. Kip , Joseph E. Harrington and John M. Vernon (2005). *Economics of Regulation and Antitrust*, 4th edition. Cambridge, Massachusetts: MIT Press.
- WHO (2001). *Water Quality: Guidelines, Standards and Health: Assessment of risk and risk management for water-related infectious disease*. Lorna Fewtrell and Jamie Bartram, eds. London: IWA Publishing.
- World Bank (2006). *Handbook for Evaluating Infrastructure Regulatory Systems*. Washington, D.C.
- World Bank (2011). *Doing Business 2011: Making a Difference for Entrepreneurs*. Washington, D.C.
- WEF (2010). *Rethinking Risk Management in Financial Services: Practices from other domains*. Available from <https://members.weforum.org/pdf/FinancialInstitutions/RethinkingRiskManagement.pdf>
- WEF (2011). *Global Risk Report 2011, Sixth Edition*. Geneva. Available from <http://reports.weforum.org/global-risks-2011/>.
- WEF (2012). *How safe are our safeguards? Global Risk Report 2012, Seventh Edition*. Geneva. Available from <http://reports.weforum.org/global-risks-2012/>.
- WMO (2006). *Scientific Assessment of Ozone Depletion*, Global Ozone Research and Monitoring Project—Report No. 50, 572 pp., Geneva, Switzerland, 2007.
- WTO (1994a). *The Agreement on the Application of Sanitary and Phytosanitary Measures (SPS Agreement)*. Available from www.wto.org/english/docs_e/legal_e/15sps_02_e.htm .
- WTO (1994b). *The Agreement on Technical Barriers to Trade*. Available from www.wto.org/english/docs_e/legal_e/17-tbt_e.htm .
- WTO. *Understanding the WTO: The Agreements*. Available from www.wto.org/english/thewto_e/whatis_e/tif_e/agrm1_e.htm (accessed 30 October 2011).