Application of Risk-based Management System Standards to the Design of Regulatory Systems*

The definition and implementation of risk management strategies is at the core of several management system standards. This paper shows why and how these standards can provide guidance for policy-makers and which elements of management systems are not yet present in regulatory systems. It then addresses risk govenance deficits, and concludes by policy recommendations on filling in the gaps and raising the efficiency of regulatory systems.

The main argument is that ISO/IEC 27001:2005 'Information technology — Security techniques — Information security management systems (ISMS)— Requirements' is particularly suited to the analysis of a regulatory system as a whole and to help overcome challenges that regulators face in the development of a coherent risk policy.

It is important to note that we will not be considering implementation of the standard in the organizations that functions within the regulatory system. Instead, we will use ISO/IEC 27001:2005 as a model for the regulatory system itself[1].

1. Risk and Regulatory Policy: the Main Challenges

The concept of risks as triggers for regulatory intervention is widely recognized; and the development of risk management frameworks for regulatory systems is at the core of the policymakers' agenda and a subject at the crossroad of different fields of research. Similarly to the evaluation of the adequacy of security measures within a management system, risk as a concept can be used to evaluate how 'balanced' the regulatory system is, against two extremes: excessive regulations – regulations that are too stringent with respect to the risk they set out to address – and insufficient regulations that fail to address risks as perceived by the various stakeholders.

As noted in UNECE (2009) 'laws, administrative measures and technical regulations, complemented by voluntary standards and norms are one important response to risks'. At the same time, the recent OECD publication 'Improving the Governance of Risk' (OECD, 2010) presents a comprehensive description of risk governance within the OECD member states and notes that 'very few countries have attempted to develop a coherent policy on the management of risk through regulation'.

The eruption of the Icelandic Volcano, the environmental catastrophe in the Gulf of Mexico, the subprime crisis in the United States, are some recent examples that highlight how unforeseen hazards may have a very real impact on the lives of citizens on a regional, or even

---

* By Lorenza Jachia and Valentin Nikonov. The authors are respectively Chief of Unit and Consultant in the Regulatory Cooperation Unit of the United Nations Economic Commission for Europe. The views and opinions expressed in the paper are those of the authors, and do not reflect the views of the organization and its member states.

[1] ISO 31000 - the most recent risk management standard – also provides guidelines for risk management implementation within an organization. ISO ISO/IEC 27001:2005 is better suited to the purposes of this paper because it additionally provides management with specific guidance in the design and continual improvement of a management system.

a global scale. As noted in IRGC (2009) 'the potential consequences of risk governance deficits can be severe in terms of human life, health, the environment, technology, financial systems and the economy as well as social and political institutions'. Debates on decisions taken by authorities leading up to and in the unfolding of these events can be framed in the broader context of the management and governance of public risks.

OECD (2010) and IRGC (2009) contain a comprehensive description of risk governance challenges – and deficits; and provide insights on how they can be addressed.

This paper argues that some of these challenges and deficits could be overcome if an approach inspired to ISO/IEC 27001:2005 was applied to regulatory systems: it would allow filling in many of the gaps in existing regulatory systems that are at the basis of risk governance deficits.

2. What Can We Learn from ISO/IEC 27001:2005 to Improve Risk Governance?

An information security management system (ISMS), as described in the ISO/IEC 27001:2005 standard will function as follows. After an organization has established a way of coordinating its ISMS and an appropriate policy (containing specific risk acceptance criteria), it can start implementing processes for the management of its informational assets. These processes result in a constantly updated informational asset inventory and provide an answer to the question 'what needs to be protected'.

When the assets are identified, the organization performs risk identification and assessment according to an agreed methodology (to answer the question 'what are the threats to the assets'). The result of these processes is a list of risks that are ranged according to the level of their criticality. Taking into account the risk acceptance criteria, the organization decides for each risk whether to accept it, to avoid it, to transfer or to mitigate it, by implementing appropriate measures. These measures may be taken from the Annex A of the ISO/IEC 27001:2005, and incorporated into the risk treatment plan. The risk treatment plan, in turn, is the basis for the development of contingency plans. The system has the usual set of improvement processes: all procedures within the scope of the system are subject to regular internal audits, corrective and preventive actions; the characteristics of the system as well as of the risks are analyzed during periodic management reviews.

Information security presents a number of analogies with regulatory systems since they both are complex cross-organization and cross-discipline fields. As regulators establish the rules of the game for a specific sector or across the board, top management of an organization similarly develops principles that all departments must comply with. Indeed, not just the IT services, but all departments are informational asset owners and play an indispensible role in addressing informational security risks. Their work is then affected by information security measures. Similarly, regulations will have a strong impact on all economic operators. Departments within an organization may see risks that top management doesn't, just like economic operators may identify risks that regulators have missed. The internal audit department within an organization performs functions that are similar to the work of market surveillance authorities. 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, its clients, and suppliers.

ISO/IEC 27001:2005:2005 is not a purely risk management standard: it shows how risk management processes should be applied for granting information security. The core

processes of the system are not specific to the IT field: specific information security measures are in fact provided in a separate annex of the standard. This makes the standard particularly suited for application to regulatory systems.

Many analytical frameworks have been laid out to describe risk governance, and most of them include several elements of the risk management process as described above. OECD (2006) divides risk policy into three sequential phases: assessment, management and review with all three stages linked to communication. Risk assessment involves forecasting the probabilities and consequences of hazards. Risk management – choosing and implementing risk management strategies. The review phase involves evaluation of the effectiveness of policy solutions.

IRGC (2006) describes the following phases of the Risk Governance Framework: pre-assessment, risk appraisal, risk characterization, risk evaluation and risk management. The first four phases are similar in essence to OECD risk assessment; IRGC (2006) further explains risk management strategies as follows. For example, abandoning the development of a specific technology or taking action in order to fully eliminate a certain risk, are risk avoidance strategies. Risk transfer refers to ways of passing the risk on to a third party. Self-retention as a management option essentially means taking an informed decision to do nothing about a risk and take full responsibility both for the decision and any consequences occurring thereafter. Risk management by means of risk reduction can be accomplished by many different means.

UNECE (2009) also describes in some detail the roles that the different stakeholders in the regulatory system - economic operators, regulators, standardization bodies, conformity assessment bodies, market surveillance authorities and consumers – play in addressing risks. In a nutshell, within a well- designed system any stakeholder can identify a risk which may or not require regulatory intervention. When the regulator identifies or is informed about a risk, it may choose among different risk management strategies: it can decide to accept, avoid or mitigate it. Risk avoidance and risk mitigation imply regulatory intervention. If these options are chosen and a regulation is enforced, it requires conformity assessment (pre-market control) and/or market surveillance (post-market control). Each of the stakeholders, at each of the different stages of the regulatory action, is empowered to identify the risks and inform the regulator.

Finally, the New European Legislative Framework is an example of a legislative text that takes some of the steps of risk management process within regulatory system as requirements. For example, it requires that Market Surveillance Authorities perform risk identification to determine which products that present a risk, shall evaluate the risks and cooperate with economic operators in development of appropriate measures. If the importer, distributer or manufacturer determines that a product presents a risk, it also has an obligation to inform the Market Surveillance Authority.

All the descriptions of the risk management process quoted above are not as systemic and detailed as is ISO/IEC 27001:2005. Moreover, risk governance frameworks don't set out to describe a regulatory system and actually only address the regulatory process. None of them can be considered as a standard that could be used to assess the performance of a regulatory system. Undoubtedly, the development of coherent and consistent risk policies requires an understanding of the whole regulatory system, which is a set of interrelated processes. All stakeholder need to understand the overall structure of the system. Interfaces between risk management process and other processes of the system should be transparent, efficient and subject to continual analysis and improvement. The regulator and other stakeholders should

have a clear picture on how the change in one process would impact other processes. The lack of a description of the system leads to gaps in functions which can be filled in by elements such as those described in the ISO/IEC 27001:2005 standard.

It may well be that comparing the processes described in ISO/IEC 27001:2005 with a mix of various risk governance framework sounds like comparing Warhol with Tom Waits (both good – but slightly different). Still, a number of the elements that characterize an ISMS can be useful in describing and managing a regulatory system. The next pages describe how the standard could help regulators to overcome the challenges they currently face.

3. Overcoming Risk Governance Challenges and Deficits: which Elements of ISO/IEC 27001:2005 Could Help?

IRGC (2009) identifies 23 risk governance deficits, numbered progressively within specific subcategories (A1, A2,.., B1, B2,…). In our view, many of these deficits are related to the design and organization of any system, no matter if it is a management system for quality, environment, information security, or a regulatory system for any given field. For example, the lack of adequate knowledge about a hazard (A1) is akin to inefficient risk identification processes in an organization. The lack of adequate knowledge about how risks are perceived by stakeholders (A2), and failures to adequately identify and involve relevant stakeholders (A3) are problems common to any risk-based management system that covers cross-organizational and multi-dimensional fields. The understanding of complex interconnected systems (A7) and re-assessing in a timely manner fast and/or fundamental changes in risk systems are key issues that management system standards help to address (e.g. the 'systemic approach' principle of ISO 9000).

Evaluating the acceptability of risks (A5) and objectively determining risk appetite is a task that business organizations have to solve on a daily basis and is one of the processes described in ISO/IEC 27001:2005.

OECD (2010) sums up the challenges that regulators face in development of a coherent risk policies. OECD (2010) also describes challenges such 'failures to properly assess risks from the outset', 'subjective perception of risks', as well as 'problems of risk communication' and 'difficulties of separating risk assessment and risk management'. These challenges are complementary those identified by IRGC, for example, overcoming the challenge of 'the interrelated nature of many risks' requires an understanding of complex risk-based systems.

Some important elements of management standards are missing in regulatory frameworks, leading to a more general deficit: the 'failure to build or maintain an adequate organizational capacity to manage risk' (B9 risk governance deficit in IRGC (2009)).

We will not cover all of the elements that regulatory systems are currently perceived as lacking, nor all those that are covered in the literature referenced above but will concentrate on the most important. We will then attempt to show which risk governance deficits these elements could help overcome:

1. Policy statement and system coordination;
2. Management of assets within regulatory systems;
3. Approved risk management methodology for the whole system;
4. Transparency in determination of risk acceptance criteria and acceptance of risks;
5. Continuity management as a necessary step in the risk management process;
6. Management Review.

3.1 Policy Statement and System Coordination

Regulatory systems are complex cross-industry systems that unite a broad range of stakeholders with their own incentives, values and perceptions. In general, regulatory systems do not start from a policy statement; a document which could be a unifier for the system stakeholders and could provide clear guidance on what the objectives of the system are.

One of the challenges faced by regulators in implementation of a risk governance framework has been referred to as a 'failure to adequately identify and involve relevant stakeholders', and, complementary to that one - 'subjective perception of risks'. Taking different risk perceptions as given, a necessary condition for an effective regulatory system is strong top-down coordination which sets the 'system of coordinates'. For this purpose, inter alia, ISO/IEC 27001:2005 requires organizations to develop a policy, which, among other things should 'align with the organization's strategic risk management context in which the establishment and maintenance of the ISMS will take place' and 'establish criteria against which risk will be evaluated'. There are many options for determining such criteria; choosing among them is a responsibility that the standard clearly assigns to the organization's top management.

Another important insight that the standard gives is that regulatory system will function only if it is a part of the country's overall risk management system. The Global Risk Report (WEF, 2010) highlights the importance of the systemic management of risks at the governmental level; however these systems are not yet mature, and in practice it is very hard to align regulatory system with the overall risk management of the country, provided it exists. Recognition of risk management activities on a country level is nevertheless a necessary condition for a regulatory system to function efficiently.

Establishing system coordination is an important element of ISO/IEC 27001:2005. Collaboration among stakeholders is crucial, for example to "organize systematic feedback from society and, equally, to include risk perceptions as an important input to deciding on whether something should be done about a certain risk and, if so, what'. (Jaeger et al. 2001)

ISO/IEC 27001:2005 states that the activities of ISMS 'shall be coordinated by representatives from different parts of the organization with relevant roles and job functions', and that the 'appropriate contacts with relevant authorities shall be maintained'. In regulatory system, coordination is not performed in a systemic manner. The EU New Legislative Framework referenced above provides an example of system coordination and shows how this issue is high on the regulators' agenda.

3.2 Management of Assets within Regulatory Systems

The logic of the ISMS as described in ISO/IEC 27001:2005 implies that before organization starts identifying risks, it implements asset management and classification processes. An asset is defined in ISO/IEC 27001:2005 as 'anything that has value to the organization'. In other words, before trying to give answers to questions 'what are the threats?' organization must have a clear picture of what it protects. 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 system or organization.

Although in the IRGC (2006) risk is understood as an uncertain consequence of an event or an activity with respect to something that humans value (definition originally in Kates et al. 1985), in most of the risk governance frameworks (including ISO 31000) this preparatory step is not explicitly addressed. This makes risk identification way more complicated. But it is a

fundamental step: indeed, the lack of a proper identification of the assets a regulator is setting out to protect may be at the basis of the regulatory failures that we are currently experiencing.

Even in the ISMS of a medium-sized organization, there are thousands of information security risks; in a regulatory system this number would be much higher. One of the challenges organizations face, the one that the ISO/IEC 27001:2005 helps to overcome is the same as in IGRC (2009) - '*failures to properly assess risks from the outset*'. Results of risk assessment come later than decisions to address these risks; risk identification is not structured and blurry, etc. One of the solutions that may help overcome this challenge is first to make an inventory of assets, range them against their criticality and then, starting with the most important asset, to perform risk identification. It will guarantee that important assets and thus important risks will not be missed.

In the information security management system, the assets inventory may look like the following table:

Name	**Confidentiality**	**Integrity**	**Availability**	**Criticality**	**Owner**	**Users**
Clients database	*High*	*High*	*High*	*High*	*The head of sales division*	*Sales division*

In ISO/IEC 27001:2005, the main features of informational assets which can be compomized by risks are confidentiality, integrity and availability. They are considered while determining the overall level of criticality of an asset, which in turn allows the ranking of organizational assets. For a regulatory system, the inventory could be structured in a similar way.

Once the assets are identified, their critical features should be determined and substituted into the table instead of those of informational assets. For example, in the system of railways, assets are tracks, staff, trains, etc. Classification guidelines should be developed so that for each asset, criticalities are determined in a consistent manner.

Asset management processes will help overcoming other challenges: 'the interrelated nature of many risks', 'understanding complex systems' and 'failures to re-assess in a timely manner fast and/or fundamental changes in risk systems'. 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 essential to be able to forecasts the interdependence of risks as well as of regulatory or non-regulatory responses. For this purpose, an up-to-date asset inventory is a key asset, as are the processes required to keep the inventories up-to-date.

3.3 An Approved Risk Management Methodology for the Whole System

One of the requirements in ISO/IEC 27001:2005 is to 'identify a risk assessment methodology that is suited to the ISMS' which shall 'ensure that risk assessments produce comparable and reproducible results'. ISMS will not work unless all stakeholders within the system will use a common risk management methodology. If this is not the case and, say, information security and marketing departments identify and understand risks differently, results of risk assessments will be compromised due to technical errors and inconsistencies in the ranking of risks. The same will happen if market surveillance authorities, regulators,

economic operators and other stakeholders don't have a common risk management methodology.

The process could be organized in the following way, similarly to the one of ISMS. As the standard requires risks to be identified for each informational asset, in the regulatory system risks should be identified for every asset within its scope. Several approaches are available for risk identification. One approach implies spontaneous (any stakeholder – business, society, market surveillance authority, etc. can register a risk when she sees it) and systematic risk identification. Systematic risk identification is conducted by the department which is responsible for information security in the case of ISMS, and by the regulator in case of the regulatory system. This does not mean that either the information security department or a regulator identifies the risks: risks are identified by the owners of the assets. The Information security department in the ISMS and the regulator in the regulatory system moderates the process - its responsibility is to make risk identification happen, to accumulate and analyze the information, to evaluate the risks. As a result, we get a list of risks that starts with the most critical ones at the top (the least critical at the end of the document). After the threats are identified, the regulator can turn to determination of risk management strategies and develop a risk treatment plan. Within an ISMS, this may look like the following table.

Risk	Measure, proposed by an asset owner	Cost	Responsible	Deadline	№ of control in ISO/IEC 27001:2005
Unauthorized personnel in secure areas	**Implementation of a biometric access control system**	**X**	**Security department**	**X**	**A.9.1**

For each risk within the system the following parameters should be determined: what to do with it, how much it will cost, who will implement the measures and when the measures must be implemented.

The development of an integrated risk treatment plan will help understanding the interrelated nature of risks and will allow preventing controversial measures. An agreed methodology would also provide transparency and a clear separation of responsibilities for risk assessment and for risk management.

3.4 Transparency in Determination of Risk Acceptance Criteria and Acceptance of Risks

Evaluating the acceptability of risks is one of the risk governance deficits as identified in IRGC (2009). Defining acceptable risk is one of the key problems regulators face in using risk as the basis for regulatory intervention, an option for risk acceptance is a key and necessary feature of a risk based regulatory system.

Explicitly or implicitly, regulatory policies contribute to define for which risks a government intervention through regulation or other means is warranted, which risks society and economic operators will accept to take, and who will be bearing the responsibility for contingencies

There is a perceived and increasing resistance in accepting risks. This is in part the result of political processes, where policy makers have a short term horizon and will not be blamed for the constant erosion of their country's productivity as it progressively becomes tied up in red tape, but will instead bear the brunt of the latest poorly managed hazard that makes the news. Risk intolerance has also been widely attributed to the interaction among societal stakeholders – the media, the civil society, the lobbying groups.

As one result, for example, tolerance levels for residues of contaminants on fruits and vegetables for human consumption are often set to the lowest level that measuring equipment is able to identify. In the absence of risk acceptance criteria, the decision on the threshold limit is apparently shifted from society as represented by policymakers to (an only apparently neutral) progress in science and technology.

A full description of risk acceptance in regulatory systems goes well beyond the scope of this paper. Ultimately, a strategy that seeks to seeking a shield from all hazards is not only not feasible – leading to a situation where controls are so spread out that they're not effective – but is also not desirable – because foregoing the development of a new technology that may entail risks may also result in even greater risks - if that technology could result in advances in science or medicine that could have contributed to saving human lives.

Risk acceptance challenges could be grouped into two clusters. The first group contains problems that are related to defining the acceptable level of risk and the second group – to building an organizational infrastructure that is necessary to making the application of this strategy feasible.

One approach to addressing acceptable level of risk is perhaps designing threshold numbers, though OECD (2006) states that 'very few RIA guidelines documents or government risk publications provide clear statements about the threshold between acceptable and unacceptable risks'. Water Quality: Guidelines, Standards and Health of WHO provides some approaches on how acceptable risk can be defined (on the basis of arbitrary defined probability, level that is already tolerated, public health professionals say it is acceptable, etc), each of them though has some advantages and disadvantages.

Another widely used concept in this context is the precautionary principle, a cornerstone of EU legislation (see European Commission (2000)). It states that 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'. Critics of the precautionary principle highlight how it may lead the legislators to extend the reach of regulatory policies beyond what would be desirable.

ISO/IEC 27001:2005 doesn't advise business on how to define the risk acceptance criteria but it provides insight on how to build processes that are necessary for efficient risk acceptance.The standard describes risk acceptance as a process with criteria as variables that could be analyzed and changed. This requires a determination of processes for accepting risks and appropriately communicating them to stakeholders. This last task – communication – is very delicate in itself. It indeed involves an element of moral hazard, because it may send a signal that authorities will not allocate resources to the monitoring of delinquency or non-compliance within an area of responsibility.

It may well be, that building a system in which risk acceptance is a well-defined option could contribute to structure the ongoing debate on which risks, for society as a whole, are worth

taking, and which are not. ISO/IEC 27001:2005 requires an organization to 'develop criteria for accepting risks and identify the acceptable levels of risk'. Risk acceptance is defined in the standard as 'a decision to accept the risk' and it is mentioned as one of the strategies that organization can choose when 'identifying and evaluating risk treatment options'. In business, manager's decision to accept high risk is a well recognized option: even if risks are high but the costs of its mitigation are even higher, the risk could be accepted.

Risk acceptance also implies an allocation of responsibilities for defining and approving risk acceptance criteria and for accepting the risks, development of contingency plans, etc. ISO/IEC 27001:2005 requires a regular analysis of risk acceptance criteria and provides guidance on building a 'risk acceptance infrastructure'. Making such organizational arrangements is a necessary step in building an efficient regulatory system.

3.5 Continuity Management as a Necessary Step in the Risk Management Process

Many of the risk governance deficits are related to situations when risks (expected or unexpected) eventually occur. Contingency planning is an important function of a risk management process, although it is missing in many of the risk governance frameworks. ISO/IEC 27001:2005, though not literally, presents business continuity as a step in the risk management process. The standard requires 'developing and implementing continuity plans', their testing and analysis.

Zero risk could not be a regulatory objective; though even if it were, risks would still occur. There are risks that are unavoidable (volcanic eruptions), and some are almost impossible to forecast (9/11). The only thing that the regulatory could do with regard to such risks is to prepare a plan: who, what and when will do if and when the risk occurs. It is interesting to note that a contingency plan developed for one specific risks will very likely work to address a number of risks that were not forecasted, so it may prove useful as a safety net all around the system. The need for development of such plans is widely recognized; however it is important to note that they will be efficient only if they are prepared within a risk management system, where contingency planning is a step in the process.

We believe that this function should be added to the risk governance framework as a function in the risk management process. It is especially important to have contingency plans for at least those risks that have been accepted.

A better management of crisis is not only a value in and of itself: it will contribute to save lives and assets. It will also have a posive impact on the regulatory system as a whole, as it will increase public trust and ensure that regulatory action is not a hasty response to a risk that occurred.

3.6 Management Review

Building organization capacity for risk management is a key regulator's task. As noted above, this requires a systematic approach to management of risks within a regulatory system. An important element that should be considered in the design of regulatory system is regular high-level methodological review of the system as a whole, its methodologies, processes, efficiency, etc. Though 'Review' is present in many frameworks as a phase of risk management process and implies evaluation of implementation of risk mitigation measures, the idea of 'management review' of the system is slightly different. Processes for management of risk management processes in essence are similar to other processes: they

could be better and they could be worse; in any case, they need continual improvement mechanisms.

Efficient risk policy is a result of risk governance processes, and if the processes are inefficient, so will be the risk policy. While evaluation of efficiency of risk mitigation measures is very important, along with that, management system standards advise performing regular review of the system as a whole. It includes analysis of its processes, methodologies, results of effectiveness measurement, analysis of the opportunities for improvement, etc. Errors in the risk management methodology could lead to big mistakes in life. Implementation of management review is something that regulatory systems could learn from management system standards; it would allow regulators to embed the mechanisms of continual improvement in the system, which are necessary for raising its efficiency and for development a coherent risk policy.

4. Conclusion: ISO/IEC 27001:2005, Challenges, Solutions and Systemic Approach to Risk Governance

The objectives of regulatory systems and management systems (e.g. information security system) are fundamentally similar. The core objective of a regulatory system is to provide safety without hampering economic development. ISMS has a similar goal, but its scope is limited to a single organization, and to a specific area – information security. This difference is not substantial: the core processes of the system don't depend on the field and could therefore be applied to regulatory systems.

Our conclusions could be divided into two clusters. The first set generally aims at making risk governance more systemic, the second at enhancing risk governance processes.

I. Risk-based management system standards have elements that could be embedded into risk governance frameworks. These standards, many of which have risk management process at the core, describe a system with transparent process interfaces and linkages, something that risk governance frameworks lack. Risk management processes are linked with other processes of regulatory system, and these linkages should be transparent. Risk governance doesn't work on its own; it is a part of a regulatory system, an engine that makes it possible to drive the car. Clearly, the development of a coherent risk policy requires not just knowing how the engine works, but also some idea on the car in general. Existing frameworks and standards can be used to further analyses on how a regulatory system based on risk management can be optimized. Basic elements of the management system, such as policy and coordination, process approach, development of methodologies, management review and continual improvement should be included in the regulatory system design.

II. Risk management processes, as described in ISO/IEC 27001:2005:2005 have important functions that should be considered by regulators: like management of assets and contingency planning. As we discussed above, these functions are fundamental to sound risk management: risks affect something that we value, to manage risks we need to manage our assets. Risks will always occur, and we need to be prepared; if this is the case, the consequences could be minimized. ISO/IEC 27001:2005 doesn't provide any insight on how risk acceptance criteria should be defined; however it advises on how to organize the process of accepting risks: who should decide on the risk acceptance criteria, how often risk acceptance criteria should be analyzed, where it should be written. We believe that although defining risk acceptance criteria is a complex task, risk acceptance requires organization infrastructure, which if developed would make this strategy more broadly used. Development and sharing among all stakeholders, regular analysis and improvement

of risk management methodologies is also an important lesson that regulatory systems could take from management system standards.

Experience and structure of management system standards should be considered during regulatory system design; risk governance frameworks could be broadened by elements that make a set of processes a system. Learning from management system standards, applying them to the regulatory system as a whole, would allow overcoming at least some of the challenges and risk governance deficits regulators face in developing a coherent risk policy.

References

1. European Commission (2000), Communication from the Commission on the Precautionary Principle, Brussels. http://ec.europa.eu/dgs/health_consumer/library/pub/pub07_en.pdf

2. Kates, R.W., Hohenemser, C. and Kasperson, J.: Perilous Progress: Managing the Hazards of Technology. Westview Press: Boulder, 1985

3. Jaeger, C., Renn, O., Rosa, E. and Webler, T.: Risk, Uncertainty and Rational Action. Earthscan: London 2001

4. ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements. ISO, 2005

5. ISO/IEC 9001. Quality Management Systems - Requirements. ISO, 2008

6. ISO 31000. Risk management — Principles and guidelines on implementation. ISO, 2009

7. Organization for Economic Cooperation and Development, Emerging Systemic Risks in the 21st Century: An Agenda for Action, OECD, Paris. http://www.oecd.org/dataoecd/23/56/19134071.pdf

8. Otsuki, Tsunehiro, John S. Wilson and Mirvat Sewadeh (2001) "Saving two in a billion: quantifying the trade effect of European food safety standards on African exports", http://www.botanischergarten.ch/Mycotoxins/Otsuki-Saving-Food-Policy.pdf

9. Risk and Regulatory Policy: Improving the Governance of Risk. OECD, April 2010

10. Risk Governance: Towards and Integrative Approach. International Risk Governance Council, Jan 2006

11. Risk Governance Deficits: An analysis and illustration of the most common deficits in risk governance. International Risk Governance Council, 2009

12. UNECE (2009): "Provisional programme of the International Conference on Risk Assessment and Management" http://www.unece.org/trade/wp6/documents/2009/wp6_09_002E.pdf

13. UNECE (2010) "Final outcome of the International Conference on Risk Assessment and Management" http://www.unece.org/trade/wp6/documents/2009/ConfRisk_Finaloutcome.pdf

14. Paul Hunter and Lorna Fewtrell, Water Quality: Guildelines, Standards and Health (2001)