WORLD TRADE ORGANIZATION

G/TBT/GEN/226

19 June 2017

(17-3252)

Committee on Technical Barriers to Trade

THEMATIC SESSION ON RISK ASSESSMENT[1]

MODERATOR'S REPORT[2]

This Report was delivered by the Moderator of this Thematic Session of the WTO TBT Committee at the meeting of 14-15 June 2017.

At the Seventh Triennial Review, Members agreed to continue to hold thematic sessions in conjunction with regular meetings of the Committee[3], and agreed to dedicate the 13 June 2017 thematic session to the topic of risk assessment. The presentations summarized below will be made available through the WTO website.[4]

1. **Mr. Pablo Neira** (European Union) explained how risk assessment features in the EU's regulatory process. The basic principles underpinning risk assessment are proportionality and the precautionary principle, and the Commission takes as a base a high level of protection of health, safety, environmental and consumer protection when proposing legislation, as per Art.114(3) of the Treaty on the Functioning of the European Union. While the EU Treaty did not provide any guidance on how to conduct risk assessment, the Case T-70/99- Alpharma suggested two elements for conducting risk assessments: (i) determining what level of risk is deemed unacceptable, which entailed a political decision; and (ii) scientific assessment of the risk. According to this case, the scientific risk assessment must enable the competent authority: (i) to ascertain whether matters have gone beyond the level of risk that it deems acceptable for society; and (ii) to decide which measures appear to be appropriate and necessary to prevent the risk from materializing. With respect to impact assessments in the EU, they are carried out for Commission initiatives that are likely to have significant economic, environmental or social impacts and should answer a number of questions: (i) what is the problem and why is it a problem?; (ii) why should the EU act?; (iii) what should be achieved?; (iv) what are the various options to achieve the objectives?; (v) what are their economic, social and environmental impacts and who will be affected?; (vi) how do the different options compare in terms of their effectiveness and efficiency (benefits and costs)?; and (vii) how will monitoring and subsequent retrospective evaluation be organised? With respect to conformity assessment procedures, he explained that Decision 768/2008 sets out criteria for selecting procedures in proportion to the level of risk and safety required. These criteria include the type and size of companies, the complexity of product technology, the type and importance of production, the appropriateness for the type of product, and the nature of risk involved and correlation of the procedure to the type and degree of risk. To conclude, he noted that the EU experience showed that: (i) it is possible to attain a high level of protection while ensuring a fair balance between pre-market and post-market controls; (ii) the use of good regulatory practices and tools allowed to determine both the need for regulation and the choice of conformity assessment procedures; (iii) any type of conformity assessment procedure requires an adequate level of post-market surveillance; and (iv) the aim should be an efficient allocation of both private and public resources.[5]

---

[1] The list of speakers is contained in JOB/TBT/232/Rev.1.
[2] Mr. José Manuel Campos (Chile). This Report is provided on the Moderator's own responsibility.
[3] G/TBT/37, para. 8.3.
[4] https://www.wto.org/english/tratop_e/tbt_e/tbt_e.htm
[5] The full presentation is contained in document RD/TBT/222.

2. **Mr. Chien-Lun Hou** (Chinese Taipei) explained that the Commodity Inspection Act set out how risk assessments feature in the inspection system of the Bureau of Standards, Metrology and Inspection (BSMI). The Act applies to four categories of products: consumer, electrical, mechanical and electronic. BSMI carries out pre-market inspections, border and customs checks and market surveillance. Different conformity assessment procedures are used depending on the risk of the product: batch-by-batch inspection; type approval batch inspection; monitoring inspection; registration of product certification; and declaration of conformity. While batch-by-batch inspection is used for products of high risk, declaration of conformity is used for products of low risk. For medium risk products, the manufacturer has the choice of different alternatives. Under the BSMI Product Safety Framework, risk assessment involves a number of different stages: (i) regulating and setting standards; (ii) pre-market controls; (iii) border and customs checks; (iv) market surveillance; and (v) enforcement. In the regulating stage, BSMI has an internal procedure for implementing and rescinding technical regulations: (i) the zero-order assessment table for deciding whether a new product should be regulated; and (ii) the first order assessment table for deciding the conformity assessment procedure that should be selected for a regulated product. In the zero-order Assessment Table, potential risk factors are identified by consultation with a BSMI group of experts and an analytic hierarchy process is used to weight each risk factor through a comparative survey. An additional survey is conducted to determine whether a regulation scores above a certain threshold, which indicates that the regulation is required. As an example, he shared how this process was carried out for electric scooter chargers, which were designated as a regulated product subject to registration of product certification. He observed that the results of risk assessment may change overtime due to different perceptions of risk factors when different social issues evolve, and that it is therefore crucial to identify the key factors that contribute to risks and to incorporate them into the assessment.[6]

3. **Mr. I Nyoman Supriyatna** (Indonesia) described risk assessment of electrical and electronic products in Indonesia. He explained that Ministry of Industry Regulation No. 86 of 2009 established the Procedure for the Implementation of Indonesia National Standards. Each proposal had to follow several steps of analysis, including: (i) a benefits and risk analysis; (ii) the readiness of producers and conformity assessment bodies to comply; (iii) the determination of the conformity assessment scheme and factory surveillance; and (iv) the determination of the market surveillance scheme. Once the Ministry issues the Regulation's Concept, the draft is then notified to the WTO. Currently, there are 14 standards and regulations from Ministry of Industry on electrical and electronic products that are mandatory for both domestic and foreign producers. Indonesia has assigned risk assessment scores to a number of different electrical and electronic products, ranging from medium to high. He noted that other Members sometimes assess the risk of the same products differently; and that some Members view electrical and electronic products as low risk. In this respect, Indonesia suggested that the Committee explore an internationally accepted definition on high and low-risk products.[7]

4. **Mr. Daniel Reese** (United States) stated that the Food and Drug Administration (FDA) has the mission of protecting public health from various risks, covering both food safety (SPS) and nutrition policy and labelling (TBT). The FDA actively assists consumers in maintaining healthy dietary practices and combating obesity, including through food labelling requirements which may lead to the reformulation of food products. There was ample scientific evidence about the association between the risk of coronary heart disease and trans fats consumption, and FDA therefore mandated trans fats labelling in 2003; and, in 2015 the agency revoked the "generally recognized as safe" (GRAS) status of partially hydrogenated oils. He said that overall sodium content of the food supply remains high, despite industry efforts and that sodium is associated with hypertension and strokes. The FDA issued a Draft Voluntary Guidance on Sodium Reduction Targets, and is currently considering comments received on the draft targets. In line with its strategic priority of ensuring that consumers have information to make healthy choices, the FDA updated the Nutrition Facts Label in order to: (i) emphasize the number of calories; (ii) more realistically reflect the current serving sizes; (iii) require the declaration of added sugars in addition to total sugars; and (iv) require calories and nutrients to be declared for single serving packages.[8]

[6] The full presentation is contained in document RD/TBT/227.
[7] The full presentation is contained in document RD/TBT/228.
[8] The full presentation is contained in document RD/TBT/221.

5. **Dr. Xiao Junfang** (China) highlighted the serious and growing cybersecurity risks of industrial control systems (ICS), which are widely used in the key information infrastructure such as energy, electricity, water, key manufacturing and communication infrastructure. ICS face a high number of information security vulnerabilities, and it is becoming less difficult to launch cyber-attacks on ICS, since hackers can easily identify ICS and exploit vulnerabilities in them with information shared through online open source communities. There is an upward trend in cybersecurity incidents affecting ICS, and she gave several examples of attacks on critical energy, electrical and communications infrastructure worldwide. In addition, ransomware attacks against ICS were an emerging risk. Against this backdrop, she explained that the traditional IT security paradigm was not sufficient to ensure the security of ICS in an increasingly interconnected world, especially given the high performance requirements of ICS and the major risks posed by shutdown of critical infrastructure. Enterprises often underestimate ICS security needs, and are not doing enough to address security hazards. The Electronic Technology Information Research Institute (of the Ministry of Industry and Information) was therefore engaged in risk assessment for ICS, simulation testing, threat monitoring and technical research, and also sought to increase cooperation with other Members in the areas of standards development, and information and technical exchange.[9]

6. **Mr. Timothy Wineland** (United States) presented the United States Cybersecurity Framework, developed by the National Institute of Standards and Technology (NIST), in collaboration with the private sector, technology experts and government agencies. The Cybersecurity Framework originated from a 2013 Executive Order, and was later enacted in the 2014 "Cyber Security Enhancement Act". The Cybersecurity Framework is a voluntary and flexible tool to help organizations of all types to develop plans for reducing cyber security risks, with particular focus on 16 critical infrastructure sectors. The Cybersecurity Framework recognizes that cyber security is a shared responsibility that neither government nor business can address alone. The expertise and knowledge-base of how to address cyber security lies within businesses impacted by cyber security threats, as well as technology experts, and therefore the framework is driven and designed in close collaboration with industry. The framework was developed in an iterative fashion, and was subject to extensive stakeholder consultation, with more than 3,000 experts from industry, academia and government participating in its development. The framework is not a particular set of standards or regulatory requirements, but rather a living document that incorporates effective standards that are being applied by industry, with an emphasis on the use of international standards. The framework helps organizations identify dependencies with partners, vendors, suppliers, and it allows organizations to communicate and coordinate cyber risk management within an industry or sector. The intent behind the framework is to identify best practices for cyber security risk management, and transform these into common practices that are widely applicable across industry sectors. The framework includes five functions in cyber security risk management: identification; detection; protection; response; and recovery. He explained that the Cybersecurity Framework is not a regulatory regime, but instead provides regulators with a standardized language and foundation for expressing any necessary regulation. The voluntary nature of the framework, as opposed to a regulatory regime, is intended to address the fact that regulations take time to prepare and may not be able to keep up with technology and threats, and that voluntary guidance and private sector expertise can more quickly respond to challenges and changes in technology.

7. On a personal note, the **Moderator** observed that risk assessment was a multi-faceted topic, with relevance to different aspects of the work of the TBT Committee. The use of risk assessment in support of the choice and design of conformity assessment procedures was one theme that emerged from discussions. In this respect, presentations highlighted the importance of aligning conformity assessment procedures with the nature and level of risk posed by products. Members shared examples of different ways to assess such risks, including quantitative and qualitative approaches to scoring the level of risk. One interesting suggestion was that Members further explore international definitions of the level of risk of products, from low to high risk. The session also usefully shared experiences on how Members applied risk assessment to specific policy challenges, such as with respect to food labelling and cybersecurity. I believe that risk assessment is a topic that the Committee should continue to reflect upon, given its close link to our work.

[9] The full presentation is contained in document RD/TBT/220.