Risk Management and ISO 31000 in Brazil

Interview conducted for isotc262 with

Alberto Bastos, member of the Brazilian mirror committee to TC 262

Alberto Bastos is the Founder and CEO of Modulo Security, a leading global enterprise provider of comprehensive Governance, Risk and Compliance (GRC) management solutions. Mr. Bastos has an undergraduate degree in computer science from the Federal University of Rio de Janeiro, an Executive MBA from COPPEAD/UFRJ and certifications of CISSP, CGEIT, CRISC, PMI-ACP and MCSO. He is the head of the Brazilian delegation to ISO/TC262 and Coordinator of Brazilian National Risk Management Committee responsible for standardization in risk management and business continuity. Mr. Bastos is also a Member of the CCE Working Group from MITRE and coordinated various large security and risk management projects.

isotc262.org: *Alberto, you are the coordinator of the Brazilian mirror committee to ISO/TC 262. Can you briefly introduce ABNT the Associação Brasileira de Normas Técnicas, your national standardization organization, please?*

Alberto: The Associação Brasileira de Normas Técnicas (ABNT) is the National Forum for Standardization in Brazil and a founding member of the International Organization for Standardization (ISO). ABNT is also a member of the International Electrotechnical Commission (IEC), Global Ecolabelling Network (GEN) and has contributed to the foundation of the Pan-American Standards Commission (COPANT) and the MERCOSUL Association for Standardization (AMN), being responsible for its Executive Secretariat.

ABNT has been active in product certification since 1950, and has developed different programmes aiming at meeting the needs of Brazilian companies. ABNT is an accredited registration body certifying quality systems, environmental management systems and several other products.

isotc262.org: *You have been a »regular« at TC 262 meetings in the past but were prevented from coming to Amman – will you be back at the next meeting and what is Brazil's principle message regarding the last drafts of ISO 31000?*

Alberto: I´m the head of Brazilian delegation and unfortunately could not participate in the Amman meeting last year. Nonetheless, I have participated in almost all the meetings since the beginning of the work to develop ISO 31000 and will be present in San Francisco this July, for the next meeting representing Brazil and our national committee.

I could say that Brazil´s main message regarding the latest drafts of ISO 31000 is that we did a good job not changing the original standard too much as the current version is used by many companies in all countries. On the other hand, some revision was necessary in order to simplify and better explain or adjust some text based on the experiences and feedback of the companies that are applying ISO 31000.

isotc262.org: *What is risk management based on in Brazil (e.g: are there any laws, regulations, national standards or other rules)?*

Alberto: Brazil has been actively participating in the development of risk management standards such as ISO 31000, ISO Guide 73, ISO 31010 and ISO/IEC 27005 and as soon these standards were issued internationally, we have published almost simultaneously the equivalent national standards in Portuguese. (ABNT NBR ISO 31000, ABNT ISO Guia 73, ABNT NBR ISO/IEC 31010, ABNT NBR ISO/IEC 27005).

Our Brazilian national committee is also responsible for the development of business continuity management standards and published in Portuguese the national version of ISO 22301 - Business Continuity Management Systems - Requirements and ISO 22313 – BCMS - Guidance.

At the moment, Brazil is working on a new technical standard for risk management in regulatory structures.

In terms of law and regulations, INC01 - Instrução Normativa Conjunta (Joint Normative Instruction) for federal government was recently published in Brazil requiring the implementation of a risk management and internal control framework based on ISO 31000.

isotc262.org: *What is the impact of risk management and in particular ISO 31000 in Brazil?*

Alberto: We are facing a new global trend in organizations with their management systems using a risk-based approach to support their governance and decision making processes. This is also reflected in ISO´s publication of some new standards such as ISO 19600 for compliance systems, ISO 37001 for anti-bribery systems, both of which use risk management concepts and terminology. In addition, new versions of ISO 9000 and ISO 14000 are also using this approach that they call risk-based thinking.

ISO 31000 has an important role in establishing common language across sectors and domains, breaking silos and integrating areas within organizations.

isotc262.org: *Who are the key stakeholders of risk management in Brazil?*

Alberto: In Brazil, large organizations are implementing risk management structures and processes based on ISO 31000. Our national risk management committee with more than 500 member organizations has promoted and supported the use of ISO 31000 as a common language to manage risks in organizations aligning and integrating all stakeholders, not only for technical people but also executives and top management.

Regulatory agencies are also important key players in this scenario requiring some sectors to implement a risk management framework based on best practices and technical standards.

Some industries are more mature in this implementation, as are some sectors such as security, reliability, defense, and project management.

isotc262.org: *What are the biggest obstacles for integrating risk management in all organizational activities for managers in Brazil?*

Alberto: One of the major obstacles to the integration of risk management in all organizational activities is the lack of a common language. For example, in the definition of risk of ISO 31000 ("effect of uncertainty on objectives"), the term objective must be understood in a general way as a result to be achieved, meaning not only strategic or corporate objectives but also, in the context of the organization, related to different disciplines (such as financial, health, safety or environmental) and applicable at different levels (such as strategic, organization-wide, project, product or process).

Another obstacle is the lack of automated systems to enable organizations to apply risk management in a broad scope with an effective process instead of the use of Excel spreadsheets to collect and process information that are problematic to consolidate, share and provide information to the right people. The use of some automation system seems to be needed to achieve scalability and effectiveness in risk management activities.

isotc262.org: *ISO 31000 quickly became one of the bestselling and most well recognized standards in ISO. What do you think about the future of the standard and how will it change to adapt to new challenges?*

Alberto: Business today requires decision makers to analyze and act in near real-time. Technology helps them with tools and applications that allow them to collect and analyze big data to support decision-making. Dashboards and automatic alerts about threats and opportunities, bots (robots) using Artificial Intelligence is beginning to help people with

their repetitive activities and improve their ability to act and make decisions. All this is possible only if we establish standards and common rules. Risk management can be the common basis for all this work together. ISO 31000 is the first step, with the alignment of terminology and concepts, but we need more.

Some specific standards need to be developed such as ISO 27005 – an international standard for information security risk management that details and deepens issues related to the information security domain, aligned and based on ISO 31000.

isotc262.org: *Is there a message that you want to give to the risk management community?*

Alberto: It is time for all risk management professionals and experts to join forces to create this common language. Not just about terminology and definitions, but mainly about methods and tools to promote this alignment with all stakeholders.

At the end of the day, the CEO or top management needs to consider the big picture of the organization to make the best decisions, so breaking the silos is critical to promoting integration in organizations. We have to wonder if we are part of the problem or part of the solution!

isotc262.org: *What advice can you give to interested parties in Brazil who want to offer their input to the work of ISO/TC 262 and who should they address?*

Alberto: In Brazil, I am the coordinator of the ABNT risk management committee which is the official group responsible for developing standards in this area, nationally or internationally. We are also participating in the revision of ISO 31000 and other initiatives related to risk management in Brazil.

People interested in participating, can contact ABNT or me via email abastos@modulo.com.br.

isotc262.org: **Thank you very much!**

Alberto: Thank you for the opportunity to share Brazilian experience and reality. We hope that we can soon launch a Portuguese website with some of these materials translated to promote and support risk management professionals and organizations.