Standards: supporting risk management and adding business value

INTRODUCTION

Julia Graham, deputy CEO and technical director, Airmic

When I started my risk management professional journey, I searched for tools and techniques to help me design a risk management system for my organisation. There was very little practical help available. Then I discovered the world of standards. Now having been involved in the development of risk management standards for almost 20 years, I remain convinced that when they are used wisely, there is and continues to be a place for standards in the management activities of organisations - including the activities associated with managing risk and insurance.

The international risk management standard *ISO 31000: 2009* was replaced earlier this year by *ISO 31000: 2018 Risk management – Guidelines*. This encouraged Airmic to step back and reflect on how standards can help organisations to excel and how they can support risk managers - because there seems to be a fear that standards add bureaucracy and not value. We believe that, consistently applied, the consensus among stakeholders on good practice represented by standards is likely to streamline systems.

Standards are an important means of communicating to trading partners that our products and processes follow recognised good practices that they can trust in a competitive world, and that the quality of our risk management makes us a desirable partner.

Independent research on the economic contribution of standards to the UK economy and businesses found that standards boost productivity and improve performance, kick-start innovation, and support domestic and international trade.

HOW STANDARDS HELP THE RISK MANAGER: ACHIEVING OBJECTIVES

Howard Kerr, CEO, BSI Group

Business standards are essentially agreements to apply best practice and knowledge that has been developed by users and practitioners for their own use. They contain the distilled wisdom of people with expertise or an interest in the subject matter: manufacturers, service providers, distributors, trade associations, academics, regulators and consumers. They enable real world, peer to peer engagement and ensure consistency of output.

We know from research that we conducted with the Centre for Economics and Business Research (Cebr), that standards make a significant, positive contribution to the success of UK companies, for example increasing productivity, enhancing the quality of products and efficiency of processes, and promoting international trade. The full report can be found here: https://www.bsigroup.com/LocalFiles/en-GB/standards/BSI-The-Economic-Contribution-of-Standards-to-the-UK-Economy-UK-EN.pdf

The UK has led the evolution of consensus standards for more than a century. We have developed from technical product standards and process standards to consensus on principles of good business practice for leadership, governance and risk.

Standards help organisations:

- **Remove technical barriers to trade**
- **Improve supply chains and create fair and equal competition**
- **Provide business credentials**
- **Increase consumer protection**
- **Give regulatory support**
- **Stimulate innovation**
- **Manage organisation risk**

HOW STANDARDS SUPPORT RISK MANAGEMENT

A key aspect of risk is that it is integral to all activities within an organisation that impact its sustainability, resilience and business excellence. Without an effective analysis of risk, it is impossible for an organisation to develop a realistic strategy or achievable objectives. How can an organisation implement effective information management systems or quality systems or plan for organisational change without analysing risk?

As a discipline, risk management benefits from the rigour of the agreed terminology that was developed in the international risk management standard ISO 31000 and the associated ISO Guide 73. The definition of risk in this guide and the standard is that it is "the effect of uncertainty on objectives" – outcomes can be positive or negative. This is the definition that wide swathes of the business community acknowledge when speaking about risk.

Standards do not function in isolation but are intended to work together. This is why the risk management standard and related management system standards are so important to ensure effective enterprise governance and operation of organisations. Some standards that relate closely to risk management – quality, health and safety, environment, business continuity and information management – are measurable and auditable and can therefore form the basis of certifiable schemes.

So, while it is not necessary to achieve third party certification to demonstrate implementation of the systems outlined by a standard, there is an option for organisations to do so, if they think it will benefit their business. It does this by communicating best practice to stakeholders and supply chains and may also help to reduce insurance premiums, since they reflect the organisation's attitude and exposure to risks.

However, within all of this, the risk management standard retains its status as an independent and fundamentally flexible tool that can be used in ways that best suit the organisation – either as the basis of knowledge, or of systems, or as a demonstrably achieved benchmark.

The principles of risk management in ISO 31000 are the foundation of the management and operational systems that all organisations can use to help achieve sustained success.

ISO: The International Standardization Organisation: www.iso.org

ISO is an independent, non-governmental international organisation with a membership of 161 national standards bodies.

BSI: The British Standards Institution: www.bsigroup.com

BSI is the UK's national standards body, recognised by the UK government. It provides UK interests with a route into formal, consensus standards development. Aims and objectives include: promoting trade by developing common industry standards and encouraging their use, showing businesses how to improve performance, reduce risk and achieve sustainable growth

TYPES OF STANDARDS

International standards provide a framework of consistent rules, guidelines or characteristics to help those using them achieve best practice outcomes. National standards bodies, with input from professional bodies and other experts, facilitate standards development for all interested parties to a subject (in International Standards Organisation (ISO), for example). A standard developed nationally may be considered appropriate as the basis of an international standard and an industry sector may decide that specifics of that sector demand something more bespoke and tailored.

A PAS is a publicly available specification

A PAS is a solution that can be sponsored by industry leaders, trade bodies, governments or academia to bring innovation or new concepts to markets as quickly as possible. They are often intended for global markets from their inception. A PAS may also progress to become the basis for a national or international standard. PAS 56 sponsored by the Business Continuity Institute helped contribute to British Standard BS25999 which in turn formed a foundation for International Standard ISO22301

Figure 1: The family tree of standards

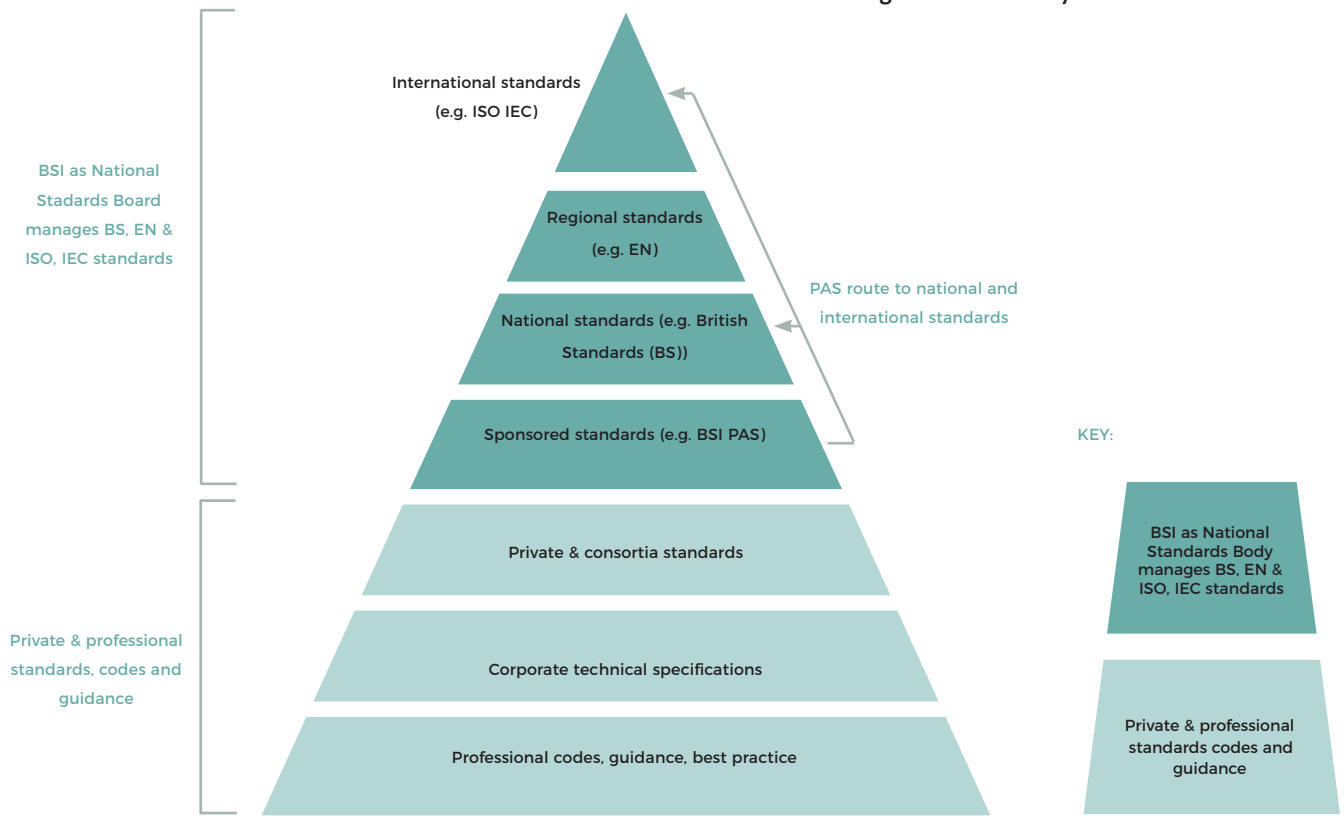


Figure 2: Three main types of standard
Source: BSI

Type 1	Type 2	Type 3
Products	**Processes**	**Principles**
Technical specifications	Management systems	Set out values and principles
Better products	Better business processes	Better business potential

Products: quality marks (such as the Kitemark) can confirm that a product or service has been thoroughly tested and checked and is proven to meet a recognised industry standard or need. It is a voluntary mark that manufacturers and service industries can obtain to demonstrate safety, reliability and quality – for example, for secure digital transactions or financial products.
Processes: a management system is the way in which an organisation manages the inter-related parts of its business in order to achieve its objectives. These objectives can relate, for example, to product or service quality, operational efficiency, environmental performance and health and safety in the workplace. Organisations do not have to seek third party certification and can do so for business benefits such as described in this report by Jon Murthy of UKAS and Marcus Long of IIOC ("How standards help the risk manager: insurance"). ISO 9001 (quality), ISO 14001 (environmental, ISO 27001 (information security and ISO 22301 (business continuity) are examples of standards against which certifiable schemes have been developed.
Principles: provide frameworks for best practice and guidance ISO 31000 is an example of this type of standard.

Many ISO management system standards have the same structure and contain many of the same terms and definitions. This is useful for those organisations that choose to operate a single (sometimes called "integrated") management system that can meet the requirements of two or more management system standards simultaneously.

DEVELOPING STANDARDS

Like a symphony, it takes a lot of people working together to develop a standard.

Anyone can get involved in standards development: all you need is a relevant interest and expertise in a particular field. Also, you must satisfy the need for balance of representation on the committee which develops a standard through an independently managed process of consensus. Key stakeholders on a committee will typically come from industry, government and civil society.

The committee begins the process with the development of a draft that meets a specific market need. This is then shared for public comment and further discussion until the consensus of the committee (based on receipt of comments and canvassing of their own constituents) is that the document satisfies current market conditions. The standard is monitored and reviewed regularly to ensure it remains fit for purpose.

HOW STANDARDS HELP THE RISK MANAGER

Russell Price, chair of the BSI risk management working group RM/1

The latest version of the guidance provided by the International Standard BS ISO 31000:2018, *Risk management - Guidelines* aims to help organisations realise the opportunities provided by its framework by simplifying and clarifying the guidance originally published in 2009. It is suitable for organisations of all types and sizes. The revised standard is more easily integrated into management processes to support decision-making at all levels of operation, and it helps develop the understanding of risk across the organisation.

Jason Brown, Chair of technical committee ISO/TC 262 on risk management that developed the standard, says: "The revised version of ISO 31000 focuses on the integration with the organization and the role of leaders and their responsibility. Risk practitioners are often at the margins of organizational management and this emphasis will help them demonstrate that risk management is an integral part of business."
Each section of the standard was reviewed in the spirit of clarity, using simpler language to facilitate understanding and make it accessible to all stakeholders. The 2018 version places a greater focus on creating and protecting value as the key driver of risk management and features other related principles such as continual improvement, the inclusion of stakeholders, being customized to the organization and consideration of human and cultural factors.

BS ISO 31000:2018 presents management with the ability to build a good practice framework for risk management that can be embedded across the organisation to better understand and manage how threats and opportunities affect performance. It can be integrated into processes of all types, including other management systems. By integrating and embedding the risk management framework, the organisation can target and prioritise activities that focus on the achievement of its objectives.

The work involved in producing BS ISO 31000:2108 built on the strengths of the original publication, but importantly recognises how the world has changed since then. There was a focus on ensuring that any changes improved accessibility and practicality, and that it was adaptive and agile. This flexibility is an essential ingredient in the way BS ISO 31000 operates. It not only helps the organisation develop better risk management across its internal operations, but also to deal with risks that arise from the more connected and extended modern business practices, such as outsourcing and shared or embedded services.

When appropriately applied, BS ISO 31000 can also support the integration and performance of other standards across the ISO family, as most ISO standards include references to risk and its management. This latest revision of BS ISO 31000 stresses the importance of consistency, communication and information sharing across the range of activities of the organisation. This capability can transform how risk is managed and potentially improve how management prioritises decisions. By focusing on the needs and objectives of the organisation and its stakeholders, the standard provides a framework that is completely scalable. The processes and activities described can be applied at the macro level, addressing key strategic market issues, as well as at operational levels where management must ensure appropriate risk controls are in place.

HOW STANDARDS HELP THE INSURANCE MANAGER

Jon Murthy, marketing manager, United Kingdom Accreditation Service (UKAS) and Marcus Long, CEO, International Independent Organisation for Certification (IIOC)

The insurance sector strives continuously to improve its management of risk. A significant number of existing standards, such as management systems, product certification, testing and inspection standards, provide insurers with reliable evidence of aspects of the quality of the risks that they are asked to underwrite. Combined with the insurers' own due diligence, compliance with such standards can reduce premiums or increase the capacity that insurers are prepared to offer.

When underwriting cyber risk, standards like the UK Government backed scheme Cyber Essentials Plus (Cyber Essentials with verification of cyber security by an assured Certification Body) and NIST (National Institute of Standards and Technology, part of the US Department of Commerce) can be effective risk controls. Cyber Essentials Plus is a good place to start for SMEs and NIST is especially relevant when you have high network dependency and resiliency requirements.

James Tuplin
Head of cyber and TMT – International Financial Lines, XL Catlin

These standards may be statutory, regulatory or voluntary, and they may be self-regulated or have third-party independent verification and certification. Virtually every sector relies on certification, inspection, testing or measurement services to demonstrate its proficiency on a wide range of issues, such as quality or health and safety.

Insurers are interested in the overall management of risk in the business they are insuring. There is research, for example, to show that companies that conform to ISO 9001 on quality management are likely to perform better. ISO standard 31000 shows that an organisation has a methodical approach to its risk management. Technical standards are already widely used to manage risk in areas such as electrical safety, fire safety and storm water management.

Insurers, such as Allianz Engineering and Zurich Engineering, have gained UKAS accreditation to ISO/IEC 17020, which sets out requirements for the competence of bodies performing inspections, to ensure that their engineering surveyors can carry out dynamic and robust risk assessments for any client location. Accreditation requires that the continual training and competency of their surveyors is maintained and improved, and ensures that the insurer has access to reliable information on which to manage its risk.

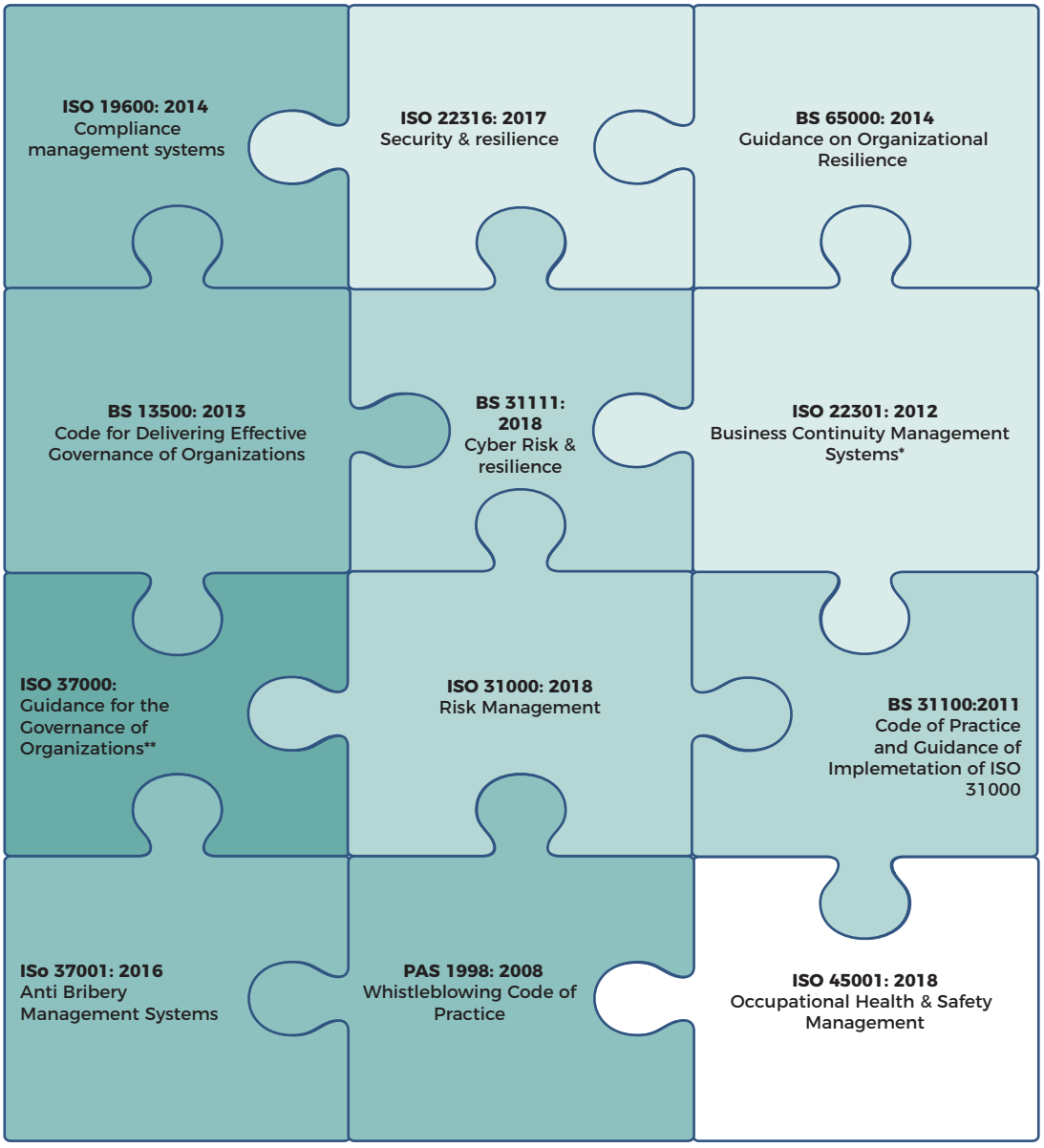
Accreditation is internationally recognised as a robust, independent declaration of an organisation's competence, the validity and suitability of its methods, the appropriateness of its equipment and facilities, and ongoing assurance through its internal quality control.

Accredited certification, inspection, testing or measurement services based on standards support brokers and underwriters in their management and assessment of risk, as well as giving consumers the assurance that the product or service delivered meets a certain level of quality and satisfies the legal requirement. Conformity assessment bodies, which provide services such as testing laboratories and inspection facilities, can provide further assurance that a product, service or system meets the relevant requirements.

In the UK, Howden, an independent Lloyd's broker, created a professional indemnity scheme for clients operating under accreditation, which helped it gain a full understanding of the client's risk profile and so obtain more accurate pricing for the cover required. This scheme also provides insurers with access to new, potentially profitable, lines of revenue. Those with less long-tail exposure tend to be more willing to look at the riskier lines of business, but they are unlikely to proceed unless there is some tangible evidence that the sector under consideration has recognised quality standards. Accreditation provides this evidence.

There is a family of standards designed to support the management of risk. Figure 3 illustrates how these fit together. The figure also describes standards under development that will further add to the family.

Figure 2: Key standards for risk management



ISO TC 309 Governance of Organizations
New areas:
- ISO/NP 37002 whistleblowing management systems: guidelines

ISO TC 262 Risk management
New areas:
- Legal risks
- ISO 31000 Managing travel risks
- Product safety risks [NB PAS 7100 on product recall just released]
- Emerging risks
- Supply chain risk management

ISO TC 292 Security & resilience
New areas:
- BS 67000 on City Resilience
- ISO TS 18091 Crisis Management - Strategic issue resolution

*ISO/TS 22317: 2015 - Guidelines for business impact analysis (BIA). Also standards on Emergency Management & Community Resilience
**Under development

HOW STANDARDS HELP THE RISK PROFESSIONAL

Risk professionals in conversation

Airmic Deputy CEO and Technical Director Julia Graham and Wellcome Foundation Enterprise Risk Manager Fiona Davidge talk about the value of standards to business generally and ISO 31000 2018.

Julia: Airmic is producing a paper to promote the thesis that the use of standards can add value to business. The launch of ISO 31000: 2018 seems a good time to do this because I hear comments that standards just add bureaucracy. British Standards did research with the consultancy Cebr (now part of Gartner) and they found that organisations that follow standards, create greater value than those organisations that don't. Standards helped to give organisations a system and a framework.

Fiona: There are different types of standards, and some people believe they are all prescriptive. If they hear the word standard, they think it means a formulaic, complicated approach and that using a standard will involve a tick box exercise. However, they vary. ISO 31000 provides a set of principles, a framework and a process; it's not about ticking boxes.

Julia: There is a hierarchy of standards and they exist at international, regional, country, location, sector, profession and individual organisation levels. ISO 31000: 2018 is strategically positioned and it's shorter and sharper than its predecessor. It is not designed to be certifiable because it's meant to provide a generic guide that is helpful for organisations of all shapes and sizes and to be used in a way that suits each business. The principles in 31000: 2018 are strategically positioned and useful when communicating an organisation's approach to risk at a board and c-suite level.

Fiona: But the principles are not unique to risk. They represent good management.

Julia: A big message, however, is that standards are not a substitute for good risk management. They are complementary. In my experience they are often what your customers and other stakeholders are also following and may demand that you adopt too in contract terms. They give you a common language and common approaches into which you can adopt, according to the nature, scale and risk maturity of your business.

Fiona: When it comes to IT security and the General Data Protection Regulation (GDPR), at Wellcome we have said to suppliers that unless you adopt ISO 27001, and are certified for information security, we won't enter a contract with you if that contract involves data. For us, it provides an independent view of this organisation.

We recently didn't renew a contract for a very large organisation because they had not certified themselves to that standard. We asked this organisation, which is global and deals with a lot of data, why it didn't have this certification. They said their standards were higher than that. We said – why are you making life difficult for yourself by not being certified? We had set this criterion that we expected from a supplier with sensitive data. We terminated the contract at renewal and they were so shocked. We said – if you're so good, how do you prove it?

Julia: We should never under-estimate the value of language that standards offer. One of the challenges in cyber at the moment is the lack of common language. A standard can offer a taxonomy and give a convention, but it doesn't put you in a straightjacket. You decide how to use it and to apply it consistently in a way that is meaningful to your organisation.

Fiona: I've had external auditors asking if we have based our risk management policy and approach on 31000. If I can say, yes, it makes things easy, because we have a common understanding. It's not as clear cut as if it were certified, but people should understand the approach.

Julia: But I don't think a standard has to be certifiable to be auditable. Audit and certification are not interchangeable.

Fiona: Exactly. If you're doing a preliminary debrief with an auditor, the fact that you say – my risk management process is aligned to ISO 31000 - conveys to the auditor that you know the subject. It doesn't matter that you haven't got a piece of paper to say that it has been certified.

Julia: However, if you want a supplier who is certified to an ISO standard, you want the standard and scope of certification to match what you're looking for. When I was in the law firm, it was very common to have ISO 27001 in our client agreements, but the clients who really got the value out of this were the ones who were careful in what they specified of us as a supplier and then embedded this scope in their terms of business.

Fiona: Standards have to be used and relied on with care and intelligence.

Julia: I like that, 'with care and intelligence'. As we've agreed, standards do not replace risk management. They are complementary and they can contribute to good enterprise risk management (ERM) and ultimately to the success of the business.

Julia Graham, deputy CEO and technical director, Airmic

Fiona Davidge, enterprise risk manager, Wellcome Foundation

ABOUT AIRMIC

Airmic is the not-for-profit UK association for risk and insurance professionals, dedicated to shaping the future of the profession and supporting members in their roles. Airmic is the largest network of corporate risk and insurance professionals in the UK, who benefit from industry-shaping thought leadership, CPD-accredited events and peer-support networking groups. We support our members in a range of ways: through training and research; sharing information; through our diverse special programme of events; by encouraging best practice; and by lobbying on subjects that directly affect risk managers and insurance buyers. We provide a platform for professionals to stay in touch, to communicate with each other and share ideas and information. The more people who take part in our activities, the more valuable we become.

airmic.com

ABOUT BSI

BSI is the business standards company that enables organisations to turn standards of best practice into habits of excellence. For over a century BSI has championed what good looks like and driven best practice in organisations around the world. Working with more than 86,000 clients across 193 countries, it is a truly international business with skills and experience across a number of sectors including aerospace, automotive, built environment, food and healthcare. Through its expertise in standards development and knowledge solutions, assurance and professional services, BSI improves business performance to help clients grow sustainably, manage risk and ultimately be more resilient.

bsigroup.com

ABOUT IIOC

The Independent International Organisation for Certification (IIOC) is a trade body for international certification bodies and national and regional certification associations. It represents their views on management system certification issues and provides technical input to influence decision-making in this field. IIOC also supports the regulatory framework and development of industry-led schemes to ensure that management systems deliver improvements in performance expected from third-party certification.

iioc.org

ABOUT UKAS

The United Kingdom Accreditation Service (UKAS) is the national accreditation body for the United Kingdom. It is recognised by the UK Government to assess against internationally agreed standards, organisations that provide certification, testing, and inspection and calibration services. Accreditation by UKAS demonstrates the competence, impartiality and performance capability of these evaluators.

ukas.com