bsi.

...making excellence a habit.™

Modern Corporate GOVERNANCE

Introducing optimal business governance through standards

Introduction

Strong and dynamic governance is essential in today's connected and rapidly changing world. Making the most of new opportunities, minimizing risk and reacting appropriately to the unexpected requires defined leadership responsibilities and procedures.

Corporations can use standards to enhance and shape fundamental strategies for governance, operations, security and reputation management – as well as optimize those already in existence. The modern operational landscape demands agility and swift, decisive action – regardless of whether the situation or issue at hand is positive or negative for a business.

Consumers, stakeholders, partners and government expect modern companies to behave ethically, sustainably and safely. Leadership teams taking a standards-based approach to governance are more likely to maintain integrity and reputation when it matters most.

This report examines three business-critical issues for consideration, highlighting the standards that are most important and useful when it comes to building long-term organizational resilience and high performance.

1 Cybersecurity

Understanding your cybersecurity risk • Bring your own device
Mitigating the risk from human error

2 Occupational health and safety

Improving organizational resilience with OH&S management • Psychological health in the workplace • Reaping the benefits of global OH&S standards

3 Sustainability

Environmental challenges in businesses: standards as a solution
Sustainable energy management: a framework for responsible businesses

1 Cybersecurity

Understanding Your Cybersecurity Risk • Bring Your Own Device • Mitigating the Risk from Human Error

Corporations simply can't be too careful when it comes to information security. Protecting personal records and commercially sensitive information is critical. Getting it wrong in the post-GDPR landscape means significant fines and serious reputation damage.

"The concept of cybersecurity has gone from a relatively obscure conversation to a mainstream international priority. From an organizational standpoint, cybersecurity has long ceased to be the sole responsibility of the IT department.

The right awareness and knowledge must inform and guide the daily activities of everyone in the workplace. Using internationally recognized standards in cybersecurity system design, and employee training, helps improve data protection and legislative compliance."

John DiMaria

Former Global Product Champion for Information Security and Business Continuity, BSI Group

Understanding your cybersecurity risk

Cybersecurity is an issue for every organization across the world, regardless of size or focus. Over the past decade it has moved from a technical specialism to a mainstream concern for individuals, businesses and government.

Despite this, many organizations are still not doing enough to protect themselves. According to a 2019 cybersecurity study conducted by IBM, which surveyed more than 3,600 security and IT professionals from around the world, three-quarters of businesses do not have a plan in place to respond to a cybersecurity incident.

Also, a significant proportion (45%) of companies that do have such a process in place don't test it regularly, or even at all, making it impossible to keep up to date and exposing vulnerabilities in a fast-moving environment.

This is no longer just an issue for IT professionals – in today's world, all organizations and their employees must take responsibility for digital security. From the biggest government department shielding critical infrastructure 24 hours a day, to a microbusiness looking after its customer data, the right awareness and knowledge is needed to guide everyone in the workplace.

The most effective way to improve cybersecurity is by using internationally recognized standards to introduce processes which protect against both deliberate and chance incidents.

Standards help companies improve their cybersecurity levels in several ways. From informing new protective processes to delivering more effective employee training, as well as introducing better data protection and assisting with legislative compliance ●

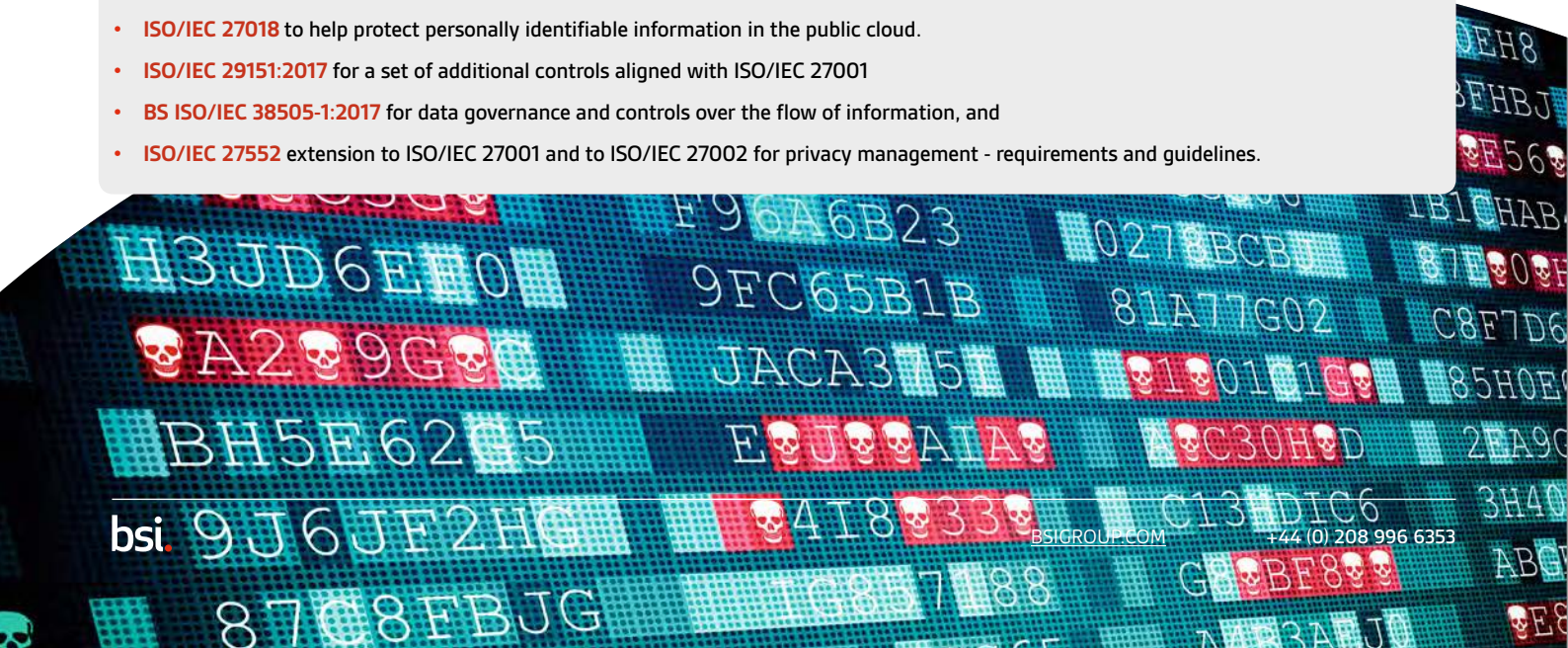
The five W's of data

BS 10012 helps companies manage the five Ws of data, namely:

1. Whose data is it?
2. Why are we processing it?
3. Where is it kept or transferred to?
4. When are we keeping it until?
5. What safeguarding mechanisms do we have in place?

Other relevant standards include:

- **ISO/IEC 27018** to help protect personally identifiable information in the public cloud.
- **ISO/IEC 29151:2017** for a set of additional controls aligned with ISO/IEC 27001
- **BS ISO/IEC 38505-1:2017** for data governance and controls over the flow of information, and
- **ISO/IEC 27552** extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy management - requirements and guidelines.



Relevant Cybersecurity Standards

PROTECTING INFORMATION & RESILIENCE AGAINST CYBERASSAULTS

ISO/IEC 27001

Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002

Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27003

Information technology – Security techniques – Information security management system implementation guidance

BS 7799-3

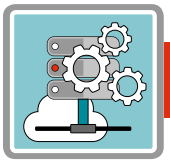
Information security management systems. Guidelines for information security risk management

ISO/IEC 27032

Information technology – Security techniques – Guidelines for cybersecurity

ISO/IEC 27017

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services



DATA MANAGEMENT AND CLOUD STORAGE

ISO/IEC 27018

Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

BS ISO/IEC 19944

Information technology – Cloud computing – Cloud services and devices Data flow, data categories and data use

ISO/IEC 27701

Privacy Information Management – Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002. Requirements

BS 10012:2017+A1:2018

Data protection. Specification for a personal information management system

BS 10008

Evidential weight and legal admissibility of electronically stored information (ESI). Part 1: Specification

BS 10010

Information classification, marking and handling. Specification

Bring Your Own Device (BYOD) arrangements and controls:

A standards-based approach

Increasingly popular, BYOD sees employees using personal devices such as laptops, tablets and smartphones for work activities, connecting to corporate networks and generating or storing data. A standards-based approach helps organizations mitigate security risks associated with BYOD arrangements.

According to a report by MarketsandMarkets, the BYOD and enterprise mobility market is estimated to grow to $73.3 billion by 2021[1]. However, BYOD still divides opinion – some see productivity gains and cost-saving potential, while others are more mindful of possible data breaches.

Having a specific BYOD policy, created in accordance with the ISO/IEC 27001 Information Security Management and ISO/IEC 38500:2015 (IT Governance) standards, should now be considered a minimum level of corporate protection.

Employee awareness and understanding of BYOD security responsibilities are critical to organizational risk. Regular communication of best practice in this area is important for people in all areas and at all levels of the organization. It's not enough to assume all staff will educate themselves to the required standard.

Consider how common it is to skip to the end of a terms and conditions form and just accept, without reading or engaging with the copy. Everybody must be invested in the process and given the chance to provide feedback and make suggestions. Individual responsibilities must be communicated to staff on a regular basis. The aspirational scenario is to have well-trained, proactive employees looking out for each other and the organization, providing coaching and interventions as required.

> **“Employee awareness and understanding of BYOD security responsibilities are critical to organizational risk.”**

As well as getting new employees on board, a standards-based BYOD policy must include detail on procedures for when staff leave an organization. This is particularly important when employees are not leaving of their own free will. Organizations can request certain actions when an employee leaves, for example file deletion, but a BYOD policy should outline how this will occur.

It should also clarify whether the individual is trusted to carry out the actions themselves, or if the IT department must undertake them. It's important to follow the policy as quickly as possible once it's confirmed that an employee is leaving. There's a strong likelihood they'll use their mobile devices in their new workplace, in which case the difficulty in obtaining any required data is multiplied.

Legislative changes, such as the General Data Protection Regulation (GDPR), must also be considered when designing or updating a BYOD policy[2]. In strengthening personal data protection for EU residents and citizens, GDPR changes the way every organization collects, holds, processes and shares an individual's data.

Mobile device and BYOD policies must reflect GDPR requirements, particularly around subject access, data discoverability and data collection. The GDPR places responsibility firmly with the organization to produce the required data or files, rather than the individual.

The BS 10012 Personal Information Management System standard helps organizations demonstrate the required level of competence in GDPR-critical areas. The risk of data breaches from mobile devices can also be reduced by using well-maintained management applications to separate a user's personal and professional files, however BYOD policies based on established standards are the best protection possible.

Employee behaviour must also be accounted for outside the usual workplace. For example, when mobile device users are away from their usual working environment, their susceptibility to threats such as phishing tends to increase (employees are more likely to neglect security responsibilities if accessing non-work related content).

Wombat Security's 'Beyond the Phish 2017' report found that almost a quarter of people surveyed answered questions on protecting mobile devices and information incorrectly[3]. It also found that 14 per cent of UK workers have no locking mechanism on their mobile devices.

Finally, when mistakes are made, education is essential, whether delivered in person or through a specific software application. Having an up-to-date incident response plan clarifies immediate responsibilities and ensures the correct action is taken to contain and control the situation in the event of a breach. The emphasis must be on continuous risk assessment and testing to ensure security and BYOD policies remain effective ●

References

1. www.marketsandmarkets.com/Market-Reports/enterprise-mobility-334.html
2. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr
3. Beyond the Phish Report 2017, published by Wombat Security: www.wombatsecurity.com/beyond-the-phish

Mitigating the risk from human error

David Maher, International Marketing Director, BSI Cybersecurity and Information Resilience, outlines the challenges that companies face in today's cloud-based landscape.

Human error will always be part of an organization's cybersecurity risk profile, and is often seen only as a possible weakness. However, standards-based training has the potential to transform it into an area of strength.

People are often described as the weakest cybersecurity link, given that human error is responsible for a high percentage of security and data breaches each year. With this in mind, the importance of standards-based awareness training, and education, cannot be overstated.

Criminals routinely seek to exploit individuals, rather than systems, because they understand just how effective social engineering techniques are on busy, distracted people who might not have cybersecurity front of mind. Wombat Security's 'Beyond the Phish 2017' report revealed that almost a quarter (24 per cent) of respondents answered questions relating to identifying phishing threats incorrectly. This highlights the significant opportunity for those looking to steal data and identities by manipulating a lack of awareness[1].

Rather than take a reactive mind-set, companies should work to make their employees a stronger link in the cybersecurity chain – empowering them to become a 'human firewall'. This is particularly important given the rise of home working and the popularity of employees using personal devices for work. Cybersecurity awareness must extend beyond an employee's regular workspace.

Using phishing simulations and knowledge assessment, organizations can accurately assess specific training requirements, and current risk – ideally at the individual user level. Using this as a baseline, companies should then tailor plans to an employee's needs. The information security standard ISO/IEC 27001 helps companies create and structure training in accordance with international best practices.

Wombat Security's research found that the average employee also lacks awareness when it comes to supposedly simple safeguards. For example, over half of US workers believe they can trust open WiFi networks in trusted locations, 40 per cent of UK workers who installed a VPN said they rarely or never use it and more than half of US and UK workers would leave a corporate laptop in their car rather than take it into a restaurant with them. The study also highlighted common training needs around physical security, such as protecting items like ID badges, printed information and files that provide details about suppliers[1].

Consideration should also be given to how cybersecurity training content will be delivered. Taking an annual approach to training will not provide the desired results, or engage staff. We recommend short, but frequent, training, as well as targeting employees with consistent content. To make a real change in behaviour, it's also important to create a culture of involvement, as giving staff the chance to provide feedback and make suggestions increases their engagement.

Standards-based cybersecurity training can help foster genuine awareness amongst employees and embed individual and collective responsibilities within staff at all levels. With improved understanding of the risks, employees are much more likely to report anything suspicious, becoming a highly effective first line of defence.

It's also important to introduce quick and easy reporting mechanisms for anything suspicious. Even with an optimal cybersecurity system in place, errors will still occur, although their significance and severity should be significantly reduced.

Maintaining an up-to-date incident response plan will clarify immediate responsibilities and ensure correct action is taken to contain and control the situation. Event details should be recorded to guide ongoing learnings and continuous risk assessment. Specific post-event training and education may also be necessary.

Finally, proving that an organization is certified to (or uses and follows) recognized standards in its cybersecurity training and processes is important. In the event of any data breach, it helps demonstrate that a company has the necessary controls in place to reasonably and responsibly fulfill its duty of care ●

> **Criminals routinely seek to exploit individuals, rather than systems, because they understand just how effective social engineering techniques are on busy, distracted people who might not have cybersecurity front of mind.**

References

1. Beyond the Phish Report 2017, published by Wombat Security: www.wombatsecurity.com/beyond-the-phish
2. PhishMe, 2016: www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

2 Occupational health and safety

An effective occupational health and safety management system will help you to protect and enhance your most important asset, your people.

“New job roles and tasks have caused a sharp rise in conditions that previously received little attention. Stress-related complaints cost economies millions each year; musculoskeletal conditions, repetitive strain injury (RSI), eye strain and other chronic health issues are also widespread.

New questions must be raised in line with changing employment patterns and practices… [and] emerging technologies and industries have, in many ways, increased the complexity of occupational health and safety. However, the primary responsibility of every organization remains the same: to provide an environment that minimizes risk and protects its workers.”

Dr Scott Steedman
Director of Standards at BSI and ISO Vice-President (Policy)

Improving organizational resilience with OH&S management

Sally Swingewood, Lead Standards Development Manager at BSI and Committee Manager for ISO/TC283, outlines how ISO 45001 will provide practical solutions for workplace health and safety.

Over 7,600 people die each day from occupational accidents or work-related diseases. That's over 2.78 million deaths worldwide, every year. On top of this, around 374 million non-fatal injuries occur annually in the workplace, leading to extended absences from work, rising insurance premiums and also early retirement.[1]

The devastating impact such workplace incidents can have on people is palpable – and on top of this comes a wider economic cost. Poor management of OH&S results in business interruption and reduced productivity, leading to losses that could have a significantly large and long-term impact on an organization. Depending on who is at fault, work-related injuries and ill health can also cause severe reputational damage, perhaps leading to legal action.

It is crucial that businesses of all sizes manage occupational risks to protect their workers and create better, safer working conditions across the globe. Proper management of OH&S is key for employers, enabling them to increase organizational resilience through proactive risk prevention. This is where ISO 45001 Occupational health and safety management systems – Requirements with guidance for use comes into play.

ISO 45001 is the world's first formal international standard dealing with health and safety management at work. It was designed to transform workplace practices, providing employers and workers with a clear framework to better their OH&S performance and lay the ground for continuous improvement.

The standard draws on OHSAS 18001, a former benchmark for OH&S. However, it contains new and distinct guidance and is not a revision or update. ISO 45001 places far more emphasis on those at the top of the organization taking responsibility for OH&S performance and for including workers in deciding how to identify and manage risks that can affect them. It promotes a holistic and decentralized approach, with OH&S fully integrated into senior management processes, and workers at all levels playing a significant role in decision making and implementation.

OH&S is no longer a standalone issue with responsibility laid on the shoulders of specialists alone, it's an integral element in running a healthy and sustainable organization. The focus of ISO 45001 is on the workers, what they do, where they need to go to work and the hazards they face. It starts with context – what the organization looks like, what its activities are and who can affect, or be affected by, the OH&S management system. It advocates a preventative approach to identify, anticipate and ideally eliminate hazards long before harm is caused. This requires comprehensive planning and commitment from top management to improve health and safety within their organization.

If this happens, the performance improvements can be extended to everyone who works for, or on behalf of, the organization. The context driven risk-based approach is adaptable for companies of all sizes, including the very smallest. The standard sets out what needs to be done, not how it should be done, and this is important. How any organization meets ISO 45001 requirements should be determined by what is useful and necessary for their own situation.

The benefits of ISO 45001 are endless when implemented correctly. Implementation helps improve the physical and psychological health and safety of workers, and brings commercial and reputational benefits: less time lost, better employee retention, easier regulatory compliance and an awareness that can lead to better change management.

Ultimately, implementing a robust and adaptable OH&S management system allows organizations to better protect themselves and everyone who works for them, leading us closer to a world where everyone can expect to return safely home from work each day without injury or work-related ill health ●

> **It is crucial that businesses of all sizes manage occupational risks to protect their workers and create better, safer working conditions across the globe.**

References

1. https://www.ilo.org/global/topics/safety-and-health-at-work/lang--en/index.htm

Psychological health in the workplace

Mental health has benefitted from increased mainstream attention in recent years. As a result, the subject of psychological health in the workplace has also gained greater prominence. We spoke to Norma McCormick, from Corporate Health Works, Inc. and Stavroula Leka, Professor of Work Organization and Well-being at the University of Cork, about how standards can be used to address this important issue.

Q Why do you think the focus on psychological health and safety in the workplace has increased in recent years?

NORMA: The recent transformation in how we talk about mental health means there's much less stigma attached to it – it's no longer something that people feel must be hidden or denied. At the same time, understanding of how psychological health directly influences all aspects of our lives has also increased.

STAVROULA: I think that socioeconomic context has played a big role, especially since the last financial crisis. As job security has deteriorated and work has become more intense, poor mental health has increased. We have also seen the rise of new forms of employment relationships such as zero-hour contracts in the UK and the flexisecurity model in Europe, both of which reduce the power employees have over their working conditions.

Q What are the key factors that influence psychological health in the modern workplace?

STAVROULA: Researchers refer to the 'psychosocial' dimensions of a workplace. This can cover anything from work schedule, timescales and how tasks are organized to flexibility and work-life balance, as well as the human relationships involved. A healthy workplace covers all these dimensions in a way that promotes both sustainable staff health and wellbeing and sustainable organizations.

Q Aside from any ethical considerations, why should businesses pay attention to psychological health at work?

NORMA: Poor psychological health presents a significant threat to long-term economic prospects. According to a recent study, mental health disorders could cost the global economy up to US$16 trillion between 2010 and 2030 unless significant action is taken.[1]

STAVROULA: I think employers have become increasingly aware of the impact of mental health on the bottom line in recent years. Stress causes higher workplace absence, as well as sub-optimal performance and lower productivity – so you can quickly see how it influences long-term organizational success. On the other hand, promoting wellbeing at work means promoting engagement, fulfilment and performance.

References

1. https://www.mentalhealthcommission.ca/English/what-we-do/workplace/national-standard

Q What are the main challenges for businesses when it comes to improving psychological health in the workplace?

NORMA: Each organization has its own set of circumstances regarding workplace demands and the psychological health of employees. Generally speaking, larger companies already have dedicated HR experts to focus on these challenges, while smaller ones are more time and resource-poor when it comes to health and wellbeing management.

However, the process by which both large and small organizations can begin to manage workplace psychological health is the same – by identifying primary risk factors and then assessing what can be done to change the working environment. The first part is often most difficult for business owners because it involves making an open and honest appraisal of their operations and approach.

Standards can have a significant influence on the way that businesses approach psychological health in the workplace.

STAVROULA: Sometimes the terminology and language used to discuss these issues presents a major practical barrier to progress. Although there is increasing awareness, in workplaces where there's still some sensitivity attached to mental health, it may be easier for managers to focus conversations on the contributing issues – like work organization – rather than use terms which might still trigger unease, like "work-related stress" or "mental illness". Targeting the sources of mental ill health should represent a priority.

Q How can standards play a role in promoting psychological health at work?

NORMA: Standards can have a significant influence on the way that businesses approach psychological health in the workplace. The National Standard of Canada for Psychological Health and Safety in the Workplace CAN/CSA-Z1003-13/BNQ 9700-803/2013, published in January 2013, was the first of its kind in the world.[2] Many large Canadian organizations are now using the standard to create preventative processes which sit at the heart of their operations.[3]

STAVROULA: Momentum has been growing over the last decade to create standards in this area. Australia has developed and promoted the importance of psychological health as part of its model Work Health and Safety Act, as have other countries. BSI published a guidance standard on managing psychosocial risks at work in PAS 1010 in 2011, while other countries, like Italy, Japan, Sweden, Spain and Ireland also have their own frameworks and tools.

NORMA: Internationally, we have the upcoming ISO 45003 which will focus solely on psychological health and safety in the workplace, expected by mid-2021. Designed to supplement ISO 45001, ISO 45003 will help organizations clarify responsibilities within their specific operational context and honestly appraise issues which might negatively impact psychological health, as well as any current barriers to addressing them. From here it will provide guidance around implementing preventative management structures, to improve psychological health in the workplace.

STAVROULA: The standard also requires organizations to monitor the impact of the initiatives they introduce, gathering ongoing input from staff. This will highlight 'leading indicators' where good progress is being made, as well as 'lagging indicators' where more attention is needed. These indicators could include the volume and type of sickness absence days, for example.

Q Looking ahead, what would be your goal for ISO 45003?

NORMA: Although there have been several national standards and toolkits introduced over last decade, ISO 45003 will be the first international standard to tackle psychological health in the workplace. I'm confident that the broader reach and extra credibility of a global standard will help many more organizations address this critical issue.

STAVROULA: I'm keen to see ISO 45003 used as a guidance standard to supplement ISO 45001, which covers more generic occupational health and safety. It's important that psychological health is no longer addressed simply as an individual issue to be dealt with through rehabilitation efforts: developing a healthy psychosocial work environment is key to creating positive change. ISO 45003 heralds the move towards this prevention-focused approach •

1. https://www.mentalhealthcommission.ca/sites/default/files/2017-03/case_study_research_project_findings_2017_eng.pdf
2. https://www.reuters.com/article/us-health-mental-global/mental-health-crisis-could-cost-the-world-16-trillion-by-2030-idUSKCN1MJ2QN

Reaping the benefits of global OH&S standards

How can OH&S standards like ISO 45001 drive societal benefit on a global scale? We spoke to experts from different regions to get their perspective on the role of OH&S standards, as well as more general health and wellbeing standards – and to share key learnings.

Martin Cottam, Group Technical Assurance & Quality Director at Lloyd's Register and ISO Committee TC 283 (Occupational Health & Safety Management) Chair:

"Rather than regulation prescribing exactly how every issue is managed, I believe the company itself is best placed to understand and manage their health and safety. This really sits at the heart of the framework for OH&S management in the UK, and through the guidance of standards, it can be mirrored on a global scale.

Communication around OH&S needs a structured approach to be effective. Standards like ISO 45001 present an opportunity for business owners and workers to encapsulate good practice, to be used as a common currency and toolset – whether that's for one office or across different time zones and cultures.

The committee responsible for ISO 45001 represents approximately 70 countries and includes delegates from mirror committees, some numbering over 100 individuals. The contributions from this extensive network provide a lot of intelligence when scoping out what new and existing standards must encompass for a world-wide user-base. This process allows for continual improvement, ensuring our guidance clearly addresses all potential issues across the world. A good example of this is the standard currently being developed to protect psychological health in the workplace."

Dr Stella Tawana, Director in the Department of Health Services at the University of Botswana:

"Most countries in the African region face several complex OH&S challenges, such as inadequate infrastructure to capture data, lack of funds to acquire and implement guidelines and no external players pushing for adoption of international laws. What's more, while our construction and mining industries are thriving, there are few safety controls in place. In many cases, organizations only adhere if it's a necessity, for example when it is required by international parent companies or related to exportation quality management.

There are inadequate penalties in place for safety breaches, with employers being more willing to pay for a breach than to invest in OH&S. And, while there has certainly been more interest in OH&S in recent years, this can have a negative impact unless it's based on recognized certification and training.

Botswana does not have specific OHS legislation and will immensely benefit from internationally recognized standards like ISO 45001; it is therefore vital that more is done to demonstrate their wider-reaching benefits. Identification and reduction of risk and injury is just one aspect; OH&S standards and certification play a fundamental role in helping organizations move towards improved economic and social impact."

David Solomon, FISQEM, CMSS, ISO45001 Master, OH&S Master, QMS, EMS and Head of Delegation – Standards Australia, ISO TC283 (Occupational Health and Safety Management Systems)

"Safety is in everything we do, be that procurement, outsourcing or design. Everyone in an organization is accountable, no matter the size or location of that enterprise. Individuals must take responsibility for their own actions, because safety is everyone's responsibility.

ISO 45001 aligns very much with our own Work Health and Safety laws in parts of Australia, meaning that at least in those locations we already do much of what the standard requires. The real challenge is integration across all operational areas – from finance to production to HR. Senior management must lead by example to ensure staff at all levels are engaged. Once this happens, personnel will be more likely to use the same system as guidance, regardless of their location, in safeguarding their health and wellbeing."

Dr. Yoshiaki Ichikawa, Senior Chief Engineer at Hitachi and ISO TC 268/SC 1 (Smart Community Infrastructures) Chair:

"For businesses that operate globally, health and wellbeing standards (which are more relevant to overall lifestyle than just occupational risk and are complimentary to OH&S standards) are essential – especially considering that many countries receive limited state guidance on these matters. Right now, we are expanding operations to Sri Lanka, and will share how we prioritize optimal employee wellbeing.

Of course, our various strategic partners won't all follow the same health and well-being policies that we have in Japan. Instead, through the provision of standards, like PAS 3002, we will provide them with the framework to improve health and wellbeing within their own cultural context. This helps us ensure employees in neighbouring sites have the appropriate support to create fulfilling work-life balance."

3 Sustainability

Environmental challenges in businesses: standards as a solution
Sustainable energy management: a framework for responsible businesses

Increased sustainability reduces cost, improves reputation, engages stakeholders and employees, while building adaptability and resilience against uncertainty.

“Without a doubt, the natural environment is our most precious asset. Recognizing its value is more crucial now than ever before: the stress that humans have placed upon the biosphere through excessive demand and exploitation of natural resource is significant, and in some cases, irreversible...

It is our responsibility to protect and restore our natural environment, leaving it in a better state for future generations. We can harness the value of nature and the natural environment for people and the economy, whilst ensuring that development creates a positive environmental legacy. Standards will play a key role in helping to realize that ambition.”

Dr Nick White
Principal Advisor at Natural England

Environmental challenges in business:

Standards as solutions

Nick Blyth, Policy and Practice Lead on Climate Change, Corporate Sustainability and Natural Environment at the Institute of Environmental Management and Assessment (IEMA), outlines how organizations can address key impacts and dependencies on the climate with a standards-based approach.

The Paris Agreement was adopted on 12 December 2015 at the annual Conferences of the Parties (COP) summit. Signatory countries came together to assess global progress in dealing with climate change and establish legally binding obligations for developed countries to drastically reduce their greenhouse gas (GHG) emissions. Civic society, business and a host of NGOs have all played important roles, contributing to the new international consensus.

COP21 in December 2015 famously led to the signing of the Paris Agreement, which sets out a global plan to limit global warming to well below 2°C. Such global plans are badly needed, and International Standards are an integral part of the solution – crucial in supporting the climate change framework.

All countries in the world signed the Paris Agreement, making commitments not just for governments but also reflecting an unprecedented momentum for action from cities, companies and communities (the so called non-state actors). For these important contributors and for their governments, international standards have a unique role to play. They offer a route for building effective frameworks and tools, all developed through international consensus, and are vital in underpinning the growth of new technologies, new markets and economic transformation.

GHG emissions quantification, monitoring and reporting, and promoting good practice in environmental management and design, are just some of the ways in which ISO international standards help organizations address climate change. ISO has produced more than 600 environment-related standards, including those that help to open world markets to clean energy and energy-efficient technologies and support climate change adaptation and mitigation schemes.

ISO standards are already well developed in climate change mitigation, providing credible, accepted approaches that measure and account for GHG emissions. Along with management system standards, they help organizations to plan and take effective actions to reduce GHG emissions.

However, in addition to addressing the causes of climate change (mitigation) ISO international standards are now supporting actors in addressing and responding to the impacts of climate change (adaptation). A UK-led adaptation principles and framework standard (ISO 14090) is near completion, along with developments assessing vulnerability and risk and a framework for climate actions.

Opportunities, however, are not limited to these climate change specific international standards. A wide range of mainstream standards are in development and, with new developing guidance, these too can be future-proofed to make their own contribution to climate change adaptation and carbon reduction.

As we move towards a low-carbon and climate-resilient society, these new standards will help organizations to adapt, transform, communicate sustainability performance and better allocate resources. Climate change is fast becoming a business reality through carbon taxes, procurement practice, supply chain risks and extreme weather events.

Significant governmental and private sector collaboration is needed to increase the impact of all climate programmes, and a standards-based approach is important to enable and support coordinated international response ●

.

> **...standards will help organizations to adapt, transform, communicate sustainability performance and better allocate resources.**

Sustainable energy management:
A framework for responsible businesses

Global energy consumption has risen steadily over the past century, driven by strong economic growth and an ever-increasing population. This demand puts increasing pressure on our natural resources, whilst continued use of fossil fuels contributes directly to pollution and global greenhouse emissions. And, despite mounting environmental concerns, it continues to rise.

In its 2016 International Energy Outlook report, the US Energy Information Administration (EIA) projected a 48 per cent increase in world energy consumption from 2012 to 2040.[1] A significant change in direction is required to ensure adequate energy supply for all. To minimize environmental impact, and achieve long-term sustainable economic growth, organizations worldwide must take the necessary measures to offset their consumption of energy resources.

Standards, like ISO 50001, can help businesses to implement energy management solutions, increasing their energy saving as they become more climate neutral. A standards-based approach to sustainable energy management enables businesses to measure and monitor their energy use, identify and manage risks, and improve performance through cutting consumption and energy bills. It also promotes corporate social responsibility (CSR), enhancing a company's image and offering a competitive advantage, along with a greater return.

As it stands today, effective energy management isn't just good for business; it's also becoming a requirement. Regulation, such as the UK Government's Energy Savings Opportunity Scheme (ESOS), has put energy use high on the corporate agenda.[2] As such, many businesses have started to invest time and budget into reviewing their current consumption, identifying cost-saving opportunities that will safeguard their business and protect the planet (and its populations) – now and for the future.

To commit to sustainable energy management and comply with legislation where required, organizations must take an integrated approach, embedding the sustainability agenda into their core business strategy. As part of this strategy, a structured energy management system is required.

The ISO 50001 standard can help all businesses deliver this, regardless of size, location or industry. Even smaller companies, with limited financial and technical resources, will feel the practical benefits of introducing organizational change. In fact, The Carbon Trust has found that low and no-cost actions can reduce an organization's energy costs by at least 10 per cent, producing quick returns on investment.[3]

The worldwide application of an international standard like ISO 50001 also contributes to more efficient use of available energy sources, and to reducing greenhouse gas emissions and other related environmental impacts – including waste and pollution. As such, it is inextricably linked to the 17 SDGs.

Efficient energy use relates directly to SDG 7, which aims to ensure universal access to "affordable, reliable, sustainable and modern energy".[4] This is essential in reaching overall climate change mitigation goals (SDG 13). It also:

- Contributes to furthering long-term economic growth (SDG 8)
- Aids in the transition to smart, sustainable cities (SDG 11)
- Ensures responsible consumption of natural resources (SDG 12)

> **A significant change in direction is required to ensure adequate energy supply for all.**

Analysis by Williams Sale Partnership (WSP) Sweden shows that in truth, SDG 7 is linked, directly or indirectly, to all of the SDGs.[5] This means that by proactively taking steps to manage energy more efficiently, organizations will help facilitate the achievement of all 17 goals.

In addition to ISO 50001, the ISO 14000 family of standards, such as ISO 14001 and 14006, provide practical tools that enable organizations to set up an effective environmental management system. These standards help firms introduce targeted initiatives for reducing raw material use, energy consumption and disposal costs.

It is clear that such guidance will become increasingly valuable as the environmental context in which businesses operate changes. Organizations that take responsibility to address energy efficiency will reap the rewards and contribute to the behavioural changes that are critical for future generations ●

References

1. https://www.eia.gov/todayinenergy/detail.php?id=26212
2. https://esosregister.com
3. https://www.carbontrust.com/resources/guides/energy-efficiency/better-business-guide-to-energy-saving/
4. https://sustainabledevelopment.un.org/sdg7
5. https://www.eceee.org/all-news/columns/energy-efficiency-required-for-all-agenda-2030-sustainable-development-goals/

Business governance essentials

C-level Management

BS ISO 31000
Risk management

ISO 22301
Business continuity

BS EN ISO 9001
Quality management

BS ISO 56002
Innovation management

BS ISO 44001
Collaborative business relationship management

BS ISO 45001
Occupational health and safety management

BS EN ISO 14001
Environmental management

BS EN ISO 50001
Energy management systems

BS EN ISO/IEC 27001
Information security management systems

Legal

BS ISO 37001
Anti-bribery management.

PD CEN/TS 16555-4
Innovation management. Intellectual property management

BS 10012
Data protection

Finance

PAS 1919
Guide to management accounting principles

Marketing

BS ISO 10668
Brand valuation

Human Resources

BS ISO 30414
Human capital reporting

PAS 1010
Management of psychosocial risks in the workplace

BS ISO 30405
Guidelines on recruitment

BS 76005
Valuing people through diversity and inclusion

PAS 3000
Smart working

Facilities

BS EN ISO 41001
Facility management systems

Customer Services

BS 8477
Customer services code of practice

BS ISO 10002
Quality management. Complaints handling

BS 18477
Inclusive service provision

Information Technology

BS ISO/IEC 20000-1
Service management

BS EN ISO/IEC 27002
Information security controls

BS ISO/IEC 27032:2012
Guidelines for cybersecurity

BS ISO/IEC 27017 / 27018
Cloud services and personally identifiable information

BS ISO/IEC 27701
Privacy information management

BS ISO/IEC 19944
Cloud services and devices

bsi. BSOL
Standards Online

Improve your organization's performance

The standards you need for best practice, all managed with one simple tool

Misunderstandings and mix-ups are expensive in business. They cost money, they waste people's time, and they damage trust. That's why standards are so powerful.

Standards boost your business

Gain a competitive advantage

Customers are always looking for reassurance. Demonstrating that you conform to internationally-recognised standards is a clear way to set yourself apart from less-professional competitors.

Trade internationally

BSOL contains internationally recognised standards, providing a passport to trade across national boundaries.

Reduce technical barriers

Standards give business partners like you and your customers the confidence that products or services will meet technical criteria.

Embed excellence in your company

As the world's oldest standards body, BSI is trusted by organizations across the world to drive quality and performance.

Protect your bottom line

With the latest standards on risk areas from cyber security to health and safety, you can put best-practice policies in place and keep your company safe.

Standards help you work smarter

Save money

BSOL's standards give you a framework for getting things right first time, so that you can achieve economies and efficiencies.

Deliver best practice

Standards shape and support your policies, educating your staff and making your business more resilient.

Encourage co-operation

Standards help different teams and organisations to work together smoothly and more effectively. Everyone knows what to expect and understands exactly what to do.

Build in quality

Once you've started using standards, BSOL is the simplest way to manage your workflows. It's easy to find standards, share them and get notified about updates.

Deliver excellence with BSOL.

Get a quote or find out more:
E: BSOLSales@bsigroup.com
T: +44 (0) 208 996 6353
W: bsigroup.com/BSOL

bsi.

...making excellence a habit.™