Infosecurity Magazine

bsi.

HOW TO ENHANCE INFORMATION SECURITY RESILIENCE WITH THE NEW ISO/IEC 27001 STANDARD

AN INFOSECURITY MAGAZINE WEBINAR REVIEW

OVERVIEW

The ISO/IEC 27001 international information security standard was updated in 2022, reflecting major changes to business practices and the wider cybersecurity sector. These include the shift to remote working, increased reliance on digital services and the maturing of the cyber industry.

This recent Infosecurity Magazine webinar highlighted the revisions to the standard and outlined best practices for organizations to implement these effectively, at whichever stage of the compliance journey they are on. May 1, 2024, is the date at which every new certification or recertification will be audited against the 2022 version. It is vital for organizations to understand now the changes now.

OPENING PRESENTATION

The session began by outlining the most significant changes made in the 2022 version of ISO/IEC 27001.

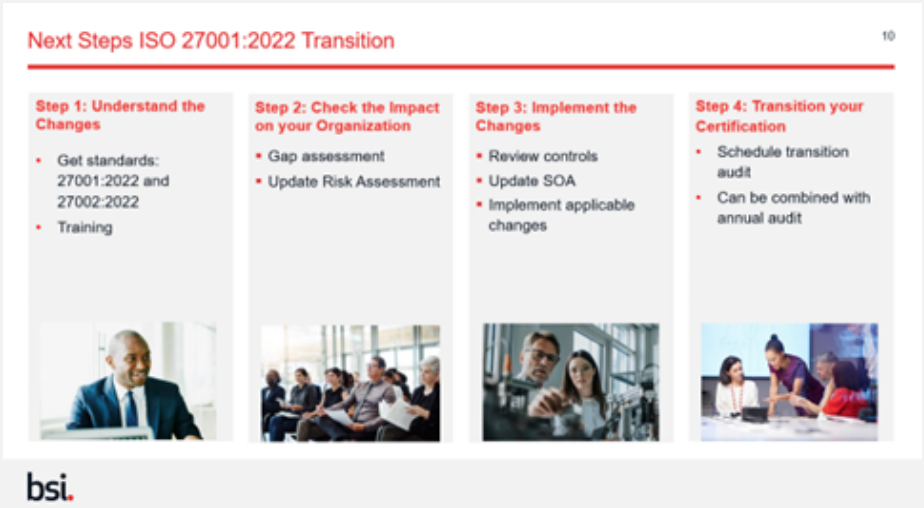
David Mudd, Global Head of Digital Trust Assurance at BSI Group, the national standards body of the UK, said the new variation of the standard aims to be more relevant, flexible and streamlined.
The update, the first since 2013, reflects seismic changes in how we live and work, like the ongoing digital transformation within orgnaizations and the move to remote working.

Additionally, Mudd noted that the updated version incorporates new cybersecurity principles that have gained prominence – in particular, acknowledging the importance of strong response and recovery processes.

He divided the most significant changes into three areas:

- **Processes:** The 2022 update of ISO/IEC 27001 requires not just the definition of an Information Security Management System (ISMS), but the processes and interactions needed to create and maintain it. Organizations also need to have criteria for their processes and implement them using those criteria.
- **Annex A Controls:** The new standards have rationalized and merged the controls in the standard. Where there were previously 114 controls in 14 groups, there are now 93 in four, which are “easier to comprehend.” There are 11 new controls, while 24 now comprise two or more of the previous control set. Document 27002/2022, the reference control set guidance, has been completely updated in light of these amendments.
- **Editorial amendments:** Mudd emphasized the importance of recognizing wording changes throughout the standards, as these can impact how the requirements are implemented within an individual organization.

Mudd concluded by urging organizations “to engage with this standard if you’ve not already and understand the issues and potential impact on your business.”



THE JOURNEY TO RECERTIFICATION

Beginning the panel discussion, Gary Hibberd, Co-Founder of Consultants Like Us who specialize in ISO 270001, outlined advice he is currently giving to clients about compliance with the updated standards.

“This is evolutionary rather than revolutionary,” he emphasized, urging organizations to properly read and understand the changes before acting.

An important step is to undertake a gap analysis on the 11 new controls introduced in Annex A, and update risk registers based on that. Additionally, he echoed Mudd’s point about the importance of wording changes in the standards. For example, the language changing from ‘what is relevant to information security’ to simply ‘what is relevant’ can have major implications.

Lee Williamson, CISO at EIP, a company that provides cloud-based software for firms that offer insurance, said his organization has already started the journey to recertifying to the 2022 update and is undertaking a “wider approach” than gap analysis and risk assessment. This encompasses the same processes as achieving compliance with the 2013 version of ISO/IEC 27001 and considering if what they are currently doing is still relevant.

“Not just in terms of the standard but with threats and things that are going on business wise that are changing the environment,” he explained.

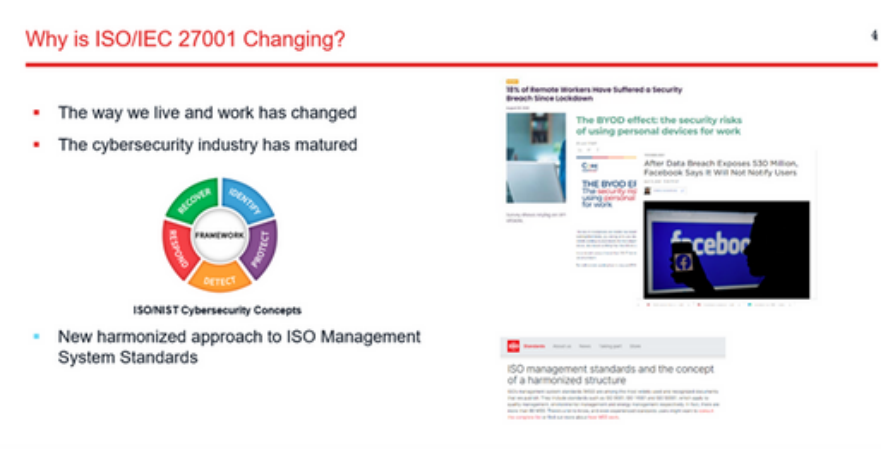
Williamson also expressed his support for the emphasis on cyber threat intelligence in the new standards, which provides a framework for organizations to obtain relevant and contextual data. Hibberd observed that cyber threat intelligence often appears daunting to organizations. However, when he translates what it means in business terms, “most people realize they’ve been doing it.”

His clients have networks in place to find out about the latest vulnerabilities, with business leaders connecting to organizations that provide information about the latest threats and events.

SECURING CLOUD SERVICES

There is a lack of awareness around securing cloud services, Hibberd said, with many organizations believing they don't need to act because they use major cloud providers like Amazon and Microsoft.

Cyber-criminals have recognized the opportunities to target such cloud services and hit multiple organizations in one go, according to Mudd, who noted that the cloud is becoming a primary attack vector.



He welcomed ISO 27001:2022 in its underlining of cloud services as a business risk rather than simply an IT issue.

"You need to make sure your board understands the risk you're holding by using these services," said Mudd.

Understanding the terms and conditions of contracts with cloud providers is also crucial to enhancing information security practices, the panel agreed. Williamson noted that many businesses will go with such services because they are cost-effective and not consider other factors. However, the contracts often contain clauses that absolve the cloud provider of responsibility when issues do occur.

For example, some contracts will state that backups are provided when the service fails, but not for accidental deletion.

Mudd urged organizations to review all the cloud services they are using and the contractual agreements in place to identify potential business risks.

"Whatever policies you're trying to manage, if they're not aligned with your cloud provider, that's going to cause a problem," he noted.

Hibberd also emphasized "you can't protect what you don't understand." He noted that it is vital to understand how data stored in the cloud is transferred and stored.

COMBINING ISO/IEC 27001 WITH OTHER REGULATIONS

With a growing range of information security guidelines and regulations, compliance is becoming more challenging, particularly for large global organizations.

Williamson said that EIP has introduced software to help this process, enabling them to quickly see what controls they are missing with any new standard. “That’s one of the best ways to manage it, otherwise you can bury yourself in effort,” he advised.

Encouragingly, Mudd noted that the updated ISO/IEC 27001 provisions are becoming increasingly aligned with other major standards, such as the US National Institute of Standards and Technology (NIST) Cybersecurity Framework.

However, privacy regulations, including the General Data Protection Regulation (GDPR), are very different. Mudd warned that complying with standards like ISO/IEC 27001 will never mean you are showing compliance with laws like GDPR. Instead, these regulations require the support of legal teams, ensuring privacy is not solely the responsibility of IT.

BUILDING A CULTURE OF SECURITY

Mudd lauded the fact that the new version of 27001 insists security policies must be signed by the company’s CEO, as it ensures board responsibility and input in this area.

This is a concept practiced at EIC, Williamson explained that the firm has a monthly management forum, where the C-suite and board members discuss and learn about data security and risk in the organization.

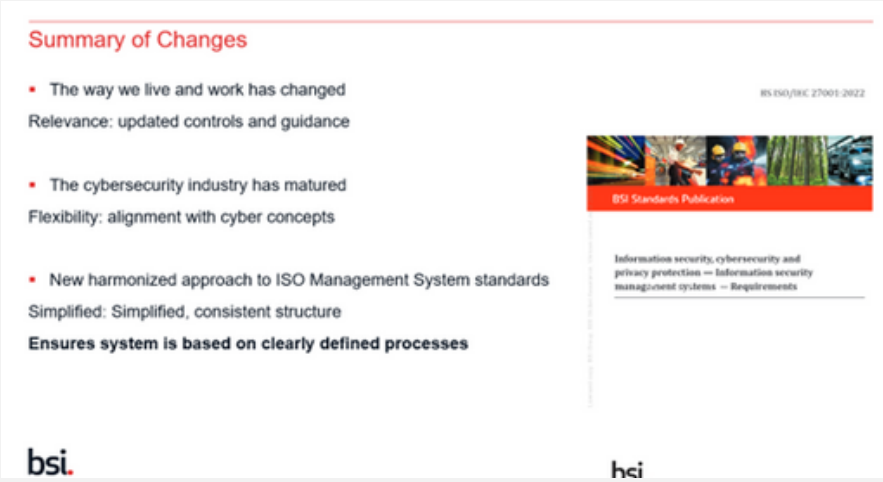
Putting this issue on the board’s agenda has driven cultural change in the organization, moving information security away from being just an IT issue to one everyone has responsibility for, said Williamson.

Hibberd emphasized this cultural change must start at the top, and this can be achieved by making the business case for having strong information security measures in place. This includes improving staff morale and retention, as “nobody wants to work for a company that’s constantly having outages and incidents.”

Additionally, showing compliance with standards like ISO/IEC 27001 can be a major business differentiator, building greater trust with customers and investors.

CONCLUSION

The transition period for ISO/IEC 27001:2022 is set to conclude in October 2025 but Mudd urged organizations to start to the process and conversations now, adding that compliance with the standard is far more than a tick-box exercise.



“It’s a fundamental duty of care to your business, your investors, your shareholders, your owners, and most of all to your customers and clients,” he outlined.

Mudd also emphasized that auditors, such as BSI, are there to support these journeys. “Our role is to understand what you’re going through on that transition and make everything as smooth as possible,” he said.

Hibberd told organizations not to panic and to start by carefully reading the standards before setting out a plan for compliance. This includes analyzing the ISO 27002 document to guide how the information security controls can be implemented.

This was also the message of Williamson, who advised organizations who are certifying to 27001 for the first time to take piecemeal steps. For example, those at the start of their journey should consider starting with smaller standards like the UK government-backed Cyber Essentials scheme before building up to 27001.

This live webinar was broadcast on Infosecurity Magazine’s Webinar Channel on September 14, 2023, and is now available on-demand here.