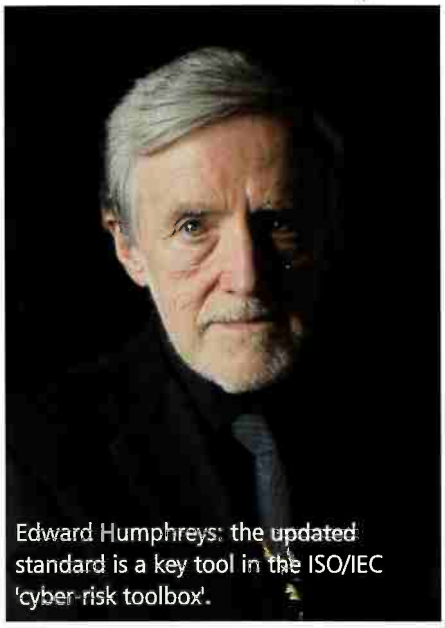
TIME FOR A DEEP HEALTH CHECK

IN OUR HYPER-CONNECTED, TECHNOLOGY-DRIVEN WORLD, DATA BREACHES AND CYBER-ATTACKS REMAIN A SIGNIFICANT THREAT TO ORGANISATIONS AND A LACK OF AWARENESS OF THE RISKS IS OFTEN TO BLAME. A NEWLY REVISED STANDARD MAY HELP



Edward Humphreys: the updated standard is a key tool in the ISO/IEC 'cyber-risk toolbox'.

Protecting the security of a company's information - whether that might be commercially sensitive or the personal details of their clients - has never been more under the spotlight. New legislation such as the European GDPR means organisations are under even greater pressure to ensure their information is secure. But having the most appropriate technologies and processes can be a minefield. The newly revised ISO/IEC 27005:2018, Information technology - Security techniques - Information security risk management, provides guidance for organisations on how to wade through it all by providing a framework for effectively managing the risks involved.

Complementary to ISO/IEC 27001:2013, which provides the requirements for an information security management system (ISMS), ISO/IEC 27005 has recently been updated to reflect the new version of ISO/IEC 27001 and thus ensure it is best equipped to meet the demands of organisations of today.

It provides detailed risk management guidance to help meet related requirements specified in ISO/IEC 27001.

Edward Humphreys, convener of the ISO/IEC working group that developed both ISO/IEC 27001 and ISO/IEC 27005, says the updated standard is a key tool in the ISO/IEC 'cyber-risk toolbox'. "ISO/IEC 27005 provides the 'why, what and how' for organisations to be able to manage their information security risks effectively in compliance with ISO/IEC 27001," he says. "It also helps to demonstrate to an organisation's customers or stakeholders that robust risk processes are in place, giving them confidence that they are good to do business with."

ISO/IEC 27005 is one of more than a dozen standards in the ISO/IEC 27000 series that make up the cyber-risk toolkit, led by the flagship ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements. Others in the series include those for protecting information in the Cloud, information security in the telecoms and utility sectors, cybersecurity, ISMS auditing and more.

ISO/IEC 27005 was developed by working group 1 Information security management systems of technical committee ISO/IEC JTC 1, Information technology, subcommittee SC 27, IT Security techniques, the secretariat of which is held by DIN, ISO's member for Germany.

INFORMATION SECURITY RISK MANAGEMENT - THE BENEFITS

Effective information security risk management should contribute to the following:

- Risks being identified
- Risks being assessed in terms of their consequences to the business and the likelihood of their occurrence
- The likelihood and consequences of these risks being communicated and understood
- Priority order for risk treatment being established
- Priority for actions to reduce risks occurring
- Stakeholders being involved when risk management decisions are made and kept informed of the risk management status
- Effectiveness of risk treatment monitoring
- Risks and the risk management process being monitored and reviewed regularly
- Information being captured to improve the risk management approach
- Managers and staff being educated about the risks and the actions taken to mitigate them.