



by Edward Humphreys

The burning questions that management ask about the information security management systems (ISMS) implemented within their organizations are the following:

- What am I getting for the investment I am making in information security?
- How effective is my ISMS?

Investment in achieving effective information security involves time, money and human resources. It involves not only designing and implementing an ISMS, but also regularly monitoring and reviewing how well the ISMS is performing to counter the risks the organization faces.

If the performance is not good enough, then improvements need to be made. Information security is an on-going commitment if it is to be effective.

Metrics and performance

So how do we check the performance of our information security? We first define a set of information security metrics and performance criteria. We then take measurements using these metrics and assess them against the criteria.

This is where ISO/IEC 27004:2009, *Information technology – Security techniques – Information security management – Measurement*, is proving useful to organizations as it provides guidance on the “why, when and how” of metrics and measurements for information security. ISO/IEC 27004:2009 is part of the ISO/IEC

27000 family of standards that supports the implementation of the ISMS requirements standard, ISO/IEC 27001.

Whereas ISO/IEC 27001 provides the specification of an ISMS which companies use to establish, implement, monitor and review, and continually improve an ISMS, ISO/IEC 27004 provides guidance on measurements to meet the requirements of ISO/IEC 27001 in the same way that ISO/IEC 27005 provides guidance on meeting the risk management requirements of ISO/IEC 27001.

So what help does ISO/IEC 27004 provide? This standard provides information and advice on:

- Principles of measuring information security
- Measurement model, methods, criteria, and indicators
- Developing a measurement programme and system
- Operational aspects of measurements
- Reviewing and improving the measurement process
- Measurement templates
- Examples of some typical measurement examples.

Having a measurement system for information security in place helps organizations to answer questions such as the following:

- Is my information security fit for purpose?
- Is my access control system effective enough to stop unauthorized attempts

- Are my procedures and policies effective enough?
- Is my staff training and awareness programme effective enough for staff to carry out their duties in a way that adequately protects the information they are handling?

Is my incident handling process effective enough to identify, assess and resolve information security incidents in a timely way, whilst minimizing the risks to the organization during the time when the incident is happening?

Help and advice

For those organizations that go through an accredited certification audit in compliance with the requirements of ISO/IEC 27001, one of the things that the organization needs to demonstrate is that they are regularly taking performance measurements.

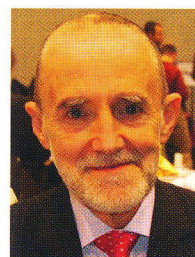
This is where ISO/IEC 27004 is a must since it provides organizations with help and advice to meet these requirements.

Information security is an on-going commitment.

For those organizations not going through an accredited certification audit, but still using ISO/IEC 27001, the questions at the beginning of this article are still valid and are being asked by management on a more frequent basis to justify their spending on information security investments.

So can your organization answer the question, “Is my information security effective and fit-for-purpose?” ■

About the author



Professor Edward Humphreys (FH University of Applied Science, Hagenberg, Upper Austria), is Convenor of ISO/IEC JTC 1, *Information technology*, sub-

committee SC 27, *IT security techniques*, working group WG 1, *Information secu-*