



computer

FRAUD & SECURITY

ISSN 1361-3723 February 2011

www.computerfraudandsecurity.com

Featured this month...

A risky business: ISO 31000 and 27005 unwrapped

Although risk management should be a core element of any information security strategy, it is neither a well-understood nor widely employed discipline today. But what might help is the arrival of two complementary ISO standards – ISO 31000 for generic corporate risk management and ISO 27005 for information security risk management.

Cath Everett explores how organisations can benefit from these standards, by looking at what the core principles of both standards are, how they are likely to prove useful and what organisations need to think about if going down this route. And she concludes that the first thing you need to do is take risk seriously.

Full story on page 5...

A new focus for IT security?

When Web 2.0 technology was introduced, few could have predicted the full extent of its role in changing the way we work and the resulting impact – not only on the security of employee and employer data, but in influencing IT policy.

Richard Turner explains why the growing pace of change in Web 2.0 technology and its integration into existing IT infrastructures make the requirement for a clear, effective and workable IT security policy more important than ever before.

Full story on page 7...

The risk of uncertainty

In the dim and distant past, when the office had, at most, a single computer, the wrath of the manager was visited upon staff for taking home pens and notebooks. In the modern world, business staff can remove a great deal more.

The availability of high-capacity storage media and email makes it relatively easy to take sensitive business informa-

tion away from the office for good operational reasons. However, when there is a threat that staff members might be losing their jobs in the near future, the temptation to get access to information that might help them find a job with a rival, or even set up business for themselves is heightened, as Wendy Goucher discovers.

Full story on page 11...

The cost of compliance

Being compliant costs the average multinational company more than £2.2m – but failing to meet regulatory compliance obligations, such as PCI, Sarbanes-Oxley and HIPAA, can cost such firms as much as £5.9m.

Those are the findings of research carried out by the Ponemon Institute on behalf of compliance specialist Tripwire. Based on discussions with 160 business leaders in 46 multinational firms, the

Continued on page 3...

Contents

NEWS

The cost of compliance	1
Cybercrime diversifies	3
Targets of fraud need to share data	20
Cyber-criminals switch to mobile platforms	20

FEATURES

A risky business: ISO 3100 and 27005 unwrapped 5

Although risk management should be a core element of any information security strategy, it is neither a well-understood nor widely employed discipline today. Cath Everett looks at two complementary ISO standards that are less well known than they should be and asks how they might be used to advantage by risk managers. The first step, she concludes, is to really take risk seriously.

A new focus for IT security? 7

Richard Turner of Clearswift explains why the growing pace of change in Web 2.0 technology and its integration into existing IT infrastructures makes the requirement for a clear, effective and workable IT security policy more important than ever.

The risk of uncertainty 11

Since the advent of email and high-capacity storage media, disgruntled staff members can take away more information from a company than just pens and paper from the office stationery cupboard. And the uncertain economic outlook, where many people fear for their jobs, only adds to the problem, says Wendy Goucher of Idrach.

REGULARS

Editorial	2
News in brief	4
Calendar	20

Photocopying

A risky business: ISO 31000 and 27005 unwrapped

Cath Everett, freelance journalist

While risk management should be a core element of any information security strategy – and, indeed, awareness of its importance is starting to mount – it remains neither a well-understood nor widely employed discipline today.

Highly regulated industries – such as financial services, utilities and telcos, as well as process-driven sectors such as manufacturing – have taken the issue seriously for years. Elsewhere, however, it has traditionally been viewed as a tiresome burden or overhead. Attitudes are now beginning to change – but slowly.

This is not least because of a growing realisation among senior managers of the need for effective business continuity provision, which is itself underpinned by an understanding of organisational risk – a situation that is reflected in the growing numbers of business continuity managers now being drawn from the business rather than the IT department, as was formerly the case.

But for all that, risk management per se is still not being embraced at board level. Other than some UK central government bodies, very few organisations of any size or stripe have senior managers who are either trained in or have been made accountable for risk management.

“Although risk managers play a crucial role in helping organisations understand both their own risk tolerance and risk appetite, well-trained and experienced personnel are in short supply”

These, however, have appointed senior risk owners, who are equivalent in status to Permanent Secretaries – the most

senior civil servant in a government ministry who is in charge of running it on a day-to-day basis – in acknowledging the fact that ownership of risk cannot be devolved down to the IT department as has traditionally been the case.

Even at the lower echelons, the current situation is far from ideal. Although risk managers play a crucial role in helping organisations understand both their own risk tolerance and risk appetite – a necessary precursor before any other work in this area can begin – well-trained and experienced personnel are in short supply.

Growing awareness

Nonetheless, Mike Gillespie, director of information security consultancy Advent-IM, is optimistic that things will start to change in the medium term. “I’m seeing a growing awareness and, over the next three years, I expect to see risk management becoming more of a



Mike Gillespie, Advent-IM.

corporate agenda issue, although it’ll be more like three to five years before it’s understood in the small-to-medium business market,” he says.

In the same way that the uptake of quality and information security management standards was driven by large enterprises demanding compliance from smaller suppliers, risk management will likewise be adopted as a result of market forces, he believes.

“Over time, it will be a case of standards by stealth, which means that you get to the point where, if you’re not doing it, you’re the odd one out, while the opposite is true today,” he Gillespie. says.

“Another key benefit of the document is that it defines common methods and terminology to ensure that risk is measured consistently”

Luckily, for those organisations wanting to get a good handle on risk management now, a couple of ISO standards have recently been made available to help them. The first is ISO 31000, a high-level, generic enterprise risk management standard that was released in November 2009 and is industry- and business-neutral. It is intended to provide principles and general guidelines on how to undertake risk management at the corporate level and is considered a good starting point for anyone either coming to the subject for the first time or wishing to know more about it.

Another key benefit of the document is that it defines common methods and terminology to ensure that risk is



Catherine Everett

measured consistently and that everyone both speaks the same language and uses it in the same way.

A common framework

A big problem today is that, all too often, different parts of the business employ their own jargon to describe risk, while at the same time measuring its impact and the probability that it will manifest itself in a subjective fashion.

Simon Oxley, managing director of risk management software supplier Citicus, explains: "If you ask the owner of a business system what impact there would be if it went down for a day, they might be afraid of losing their job and so they'll say 'very serious'. But in the great scheme of things, it may not be the case."

On the probability side of the equation, however, "people often just put their finger in the air and guess, so it's very unreliable and un-reproducible," he adds.

Therefore, as a starting point, Oxley advises information security professionals to encourage business system owners to read ISO 31000, which is written in business language, in order to gain an understanding of key risk management concepts and terminology. Not only will this make their own lives easier, but "by having a common framework for managing different types of risk across the organisation under the umbrella of ISO 31000, everyone can measure risk in the same way, whether they're physical or information security-related, which helps to avoid turf wars," Oxley says.



Simon Oxley, Citicus.

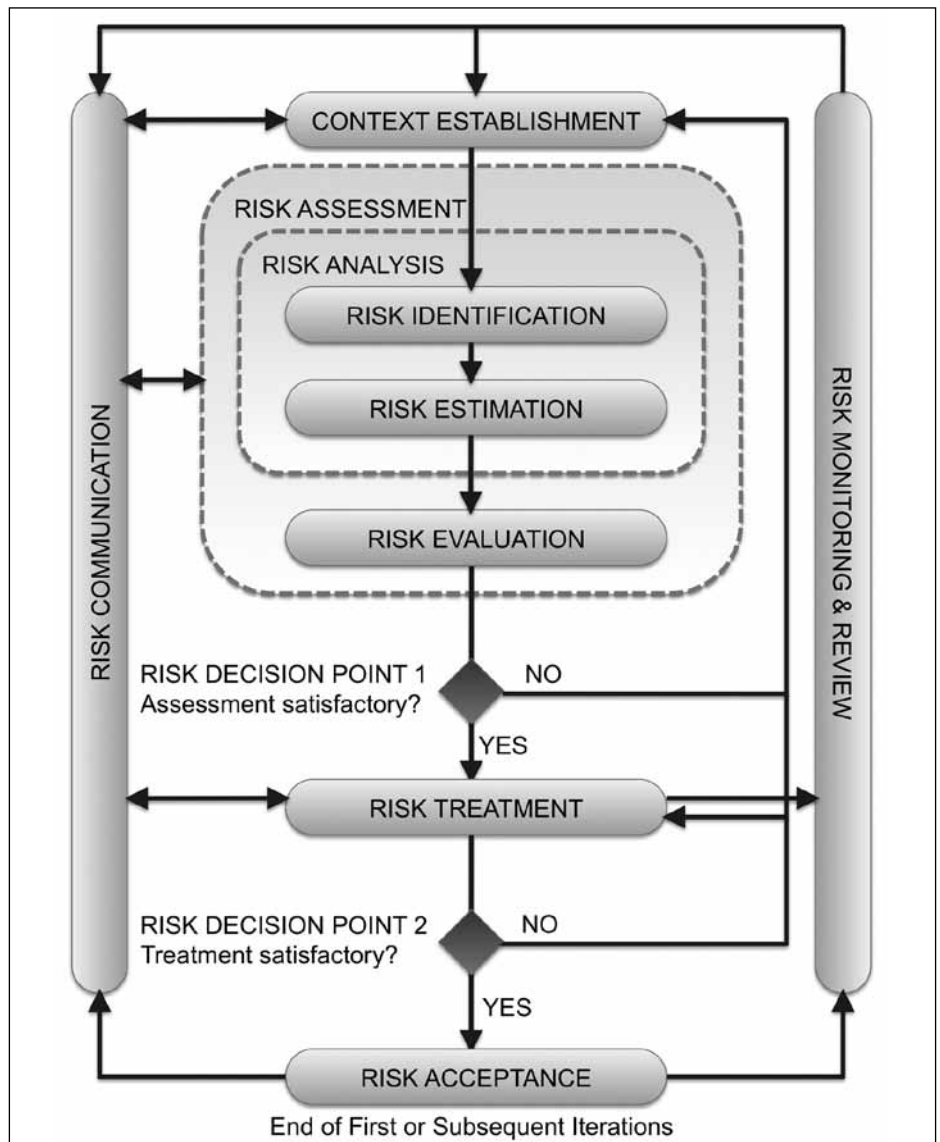


Figure 3: The information security risk process as outlined by ISO 27005.

The standard itself was born out of AS/NZS 4360:2004, which was developed by the joint Standards Australia and Standards New Zealand Technical Committee OB-007. Although it has no accreditation process associated with it, it does come with a complementary code of practice in the shape of ISO 31100, an updated version of which was published at the end of 2010 to provide additional guidance on how to implement a corporate risk management strategy. While widely adopted in Australia, ISO 31000 has, so far, barely been heard of in the UK or US.

ISO 27005

There's also another standard that dovetails nicely into it, and this is ISO

27005. This provides guidelines for information security risk management and was released in June 2008. Much of the language used in the two standards is common and both are based on the same flow diagram showing the key components of the risk management process.

"It's no good knowing that you've got a risk unless you understand what to do about it, even if it means doing nothing"

One of the first elements here is 'context establishment'. This involves defining how to undertake risk management, writing down procedures and aligning them with corporate agendas. The next step is

to undertake a risk assessment in order to identify potential risks and their possible impact, before building a risk-treatment process, which involves working out what to do about them. Finally, a formal, structured way of collecting data, recording it and reporting on the findings to management needs to be established.

But Gillespie warns: "One of the areas where business has gone wrong for a long time is that they'll assess risk, but don't move forward into pragmatic risk management. It's no good knowing that you've got a risk unless you understand what to do about it, even if it means doing nothing."

Business language

One of the key things to bear in mind in this context, however, is that risk registers should not be overly complex, but instead should be written in business language rather than technical jargon. Risks should also be laid out under broad headings along with their potential impact on business operations rather than listed in endless detail.

"You need it to be concise enough so that you can visualise the overall risk profile. If you make it overly complex and list thousands of risks, things can be lost in the detail," says Gillespie.

Such headings can be gleaned from a number of annexes contained in the standard, which include lists of potential threats that can simply be lifted wholesale, although they should also be worked on in tandem with business system owners.

"Information security professionals should have a co-ordinating role so the job of a chief information security officer is to be a driving force – someone who is responsible for implementing the process and making it work," says Oxley. "But that means engaging with business people and ensuring that they know their own risks and take action. And the ISO standards give a good framework for doing that."

Complementary standards

Despite the complementary nature of both ISO 31000 and ISO 27500, however, neither makes explicit reference to the other. And ISO 27005 does not specify, recommend or even name a particular method for risk analysis as it is meant to be just a framework and does not outline normative controls. Therefore, like ISO 31000, it is not subject to an accreditation process.

"The ultimate aim is to have a consistent, metrics-based approach across multiple risk areas, with information security risk integrated with operational risk reporting and a clear view of return on investment"

But despite its relative newness in standards terms, ISO 27005 is starting to become more commonly deployed,

particularly in relation to the more widely adopted ISO 27001. The latter specifies what an information security management system (ISMS) is and how to build one based on a risk approach, but does not lay out how risk management should be undertaken. This means that the two standards are, in fact, complementary and should ideally be used in tandem.

"What ISO 27005 is trying to do is push organisations into the upper levels of a risk-management maturity model," Oxley says. Although most companies today tend to spend their time fire-fighting, use inconsistent language and fail to document anything, the ultimate aim is to have a consistent, metrics-based approach across multiple risk areas, with information security risk integrated with operational risk reporting and a clear view of return on investment.

But as Gillespie concludes: "The first thing you need to do is be prepared to take risk seriously. Risk management has to be seen as an inherent part of good governance, but if all you're doing is paying lip service to it and playing around with it reluctantly because you think you should, you'll be wasting your time and money."

About the author

Cath Everett is a freelance journalist who has been writing about business and technology issues since 1992. Her special areas of focus include information security, HR/management and skills issues, marketing and high-end software.

A new focus for IT security?

Richard Turner, Clearswift

When Web 2.0 technology was introduced, few could have predicted the full extent of its role in changing the way we work and the resulting impact – not only

on the security of employee and employer data, but in influencing IT policy.

Just three years ago, only one in 10 employers allowed staff to engage in

social media activity such as Twitter and Facebook. However, recent Clearswift research on IT policies, showed that attitudes have changed dramatically, to a



Richard Turner