

# Measuring Security Effectiveness with ISO 27001

By Steve Wright

**What makes for good and effective security, and how to perform that security, are topics often misconstrued and miscommunicated – and worse, mismanaged.**

What makes for good and effective security, and how to perform that security, are topics often misconstrued and miscommunicated – and worse, mismanaged. That said, there are often pockets of good practice within most businesses. This does not diminish, however, the fact that we need to think hard about what to measure, how to measure, and when to measure. That is to say, it is a process of its own.

## What's different about ISO 27001?

ISO 27001 deepens the impact of measured security controls. While the intentions and objectives behind ISO 27001 are not dramatically different from those in BS 7799:2002, one of the changes with the biggest potential impact to organizations is the requirement to measure the effectiveness of selected controls – or groups of controls – within the new *Standard* (for more details see ISO/IEC 27001:2005 4.2.2 d).

This new requirement demands that businesses specify not only how these measurements are to be used to assess “control” effectiveness (there are now 133 Controls in the new *Standard*), but also how the measurements are comparable and reproducible – that is, so they can be used time and time again.

You could be forgiven for thinking this ought to be a reasonably straightforward task. After all, most IT departments throughout the world have been working within a measurement (SLAs, KPIs, ITIL) framework since the mid-1990s and should, therefore, have been considering how to measure IT effectiveness, as well as providing value for money for their stakeholders and shareholders.

But I'm afraid it's not that simple when it comes to security. As many a consultant would tell you, it's rather a specialist area and, of course, you need an expert to help you. Well, you *do* need an expert to help you, but that doesn't mean you can't find an expert internally, within your organization or your current service provider.

As mentioned above, there's often evidence of good security controls already in place in organizations (especially those who have already implemented ISO 20000, COBIT, ITIL or BS 7799). Examples might include good anti-virus procedures or good physical security procedures. But when you start to dig deeper into what, how, and

why these controls were selected and are now being measured, you start to come unstuck.

The biggest gaps are usually found around the documentation that should state the relationships between the identified risks and what countermeasures were implemented – and why. This gap often originates from a misunderstanding of what the true “essence” of the original BS 7799:1999 *Standard* was all about – Risk Management.

---

**You could be forgiven for thinking this ought to be a reasonably straightforward task.**

---

In fact, this *new* control isn't even new; it's been in existence for years. It's just that previous wording talked about “methods to monitor and maintain the effectiveness of the information security policy.” So naturally, most organizations took this to mean “security awareness training” and so forth.

## The Information Security Management System (ISMS)

In practice what has often happened is that businesses have focused on ensuring that the control objectives (formerly 127 controls) were implemented (and documented in the SOA), and have forgotten to appreciate, or map, the relationship between their organizational risks and the Information Security Management System (ISMS). The ISMS is the framework in which the management of security should be defined, documented and understood by all employees.

But herein lies the problem. Some companies that have chosen to implement, say, an expensive intrusion detection system (IDS), don't always know why or how they came to choose its implementation in the first place. More significantly, the special relationship between risk and cost won't necessarily have been fully thought through, and therefore, a company may not have even considered measuring an IDS's effectiveness.

Worse still, very few appear to have done any work on understanding the value or return on investment (ROI). In fact, if many organizations were not being scare-mongered (by the media) into buying security solutions, and concentrated instead on what is fundamentally a risk issue, security-related decisions would only be based on budgeted evidence, and we wouldn't be having this discussion. Each control selected would have to have a definition of how it would be effective, and the measurements required would, of course, be documented.

---

**In fact, if many organizations were not being scare-mongered (by the media) into buying security solutions... security-related decisions would only be based on budgeted evidence.**

---

So how can we select which controls should be measured? Equally importantly, how can these be used to provide "assurance" to stakeholders and shareholders that "security controls" are operating effectively? This is an area of security that gets ignored (for some of the reasons stated above), or if it is undertaken, is not actually reported on.

As you may have concluded by now, the topic at hand is not as straightforward as you might have believed. Hopefully, though, what I have achieved by compiling this article can get the ball rolling on a difficult topic that needs to be fully understood in order to prevent its stifling the anticipated growth in security.

Further, this is a hot topic because industry and leading standards bodies, such as the ISO and BSI, have also struggled to get a grip on it. These organizations are all striving to achieve synergies between ISO 20000, ITIL and ISO 9001, and could really do with finding a set of measurements that can easily be linked in with existing or new Management Systems – for example, Quality and ITIL - Service Delivery.

So this coupled with an age of increasing identity fraud, escalating IT costs and frequent corporate scandals, makes little wonder why regulatory bodies are starting to ask awkward questions to CIOs, CEOs and Senior Management as to how they are currently managing their risks. In other words, how can they demonstrate the effectiveness of their management of risk strategy, including security risk management?

## Why measure security?

Well, it would be easy to say we're secure, but how can you demonstrate this? And therefore, how can you:

- Show ongoing improvement
- Show compliance with standards, contractual requirements (measured within KPIs, SLAs, OLAs) and of course legal and regulatory requirements
- Justify any future expenditure on new security software, training, solutions, etc.
- Demonstrate that you are ISO 27001-compliant (other Management Systems also require it – ISO 9001, ISO 20000)

- Easily identify where implemented controls are not effective in meeting their objectives
- Provide confidence to senior management and stakeholders that risk-justified implemented controls are working effectively.

So, which of the 133 potentially applicable controls (within ISO 27001) can be used to measure security?

Well, arguably, all of them. In practice, though, this would invariably pose too onerous a task and would cause an already overworked IT and Information Security Department to crumble under the weight of bureaucracy.

Before we attempt to answer this question, then, we should always satisfy ourselves with the reasons behind the requirement for ISO 27001. Why are you being asked to provide such information? What is the driver? Where does the requirement come from?

## What's driving the move to ISO 27001?

Other drivers may exist than the one you are motivated by. It could be the company has just realized you can get more from ISO 27001. Or perhaps the driver is operational risk management and Corporate Governance requirements such as FSA, BASEL II, SOX or Turnbull. Or, quite simply, Legal and Regulatory requirements are forcing your organization down the ISO 27001 compliance route.

Whatever the drivers are, you're not alone. Many organizations (but not all) misunderstand the fundamental concepts behind BS 7799 and ISO 27001, and unfortunately have only viewed compliance to ISO 27001 as a marketing exercise, as opposed to trying to achieve real business benefit and manage their risks.

ISO 27001 provides much more clarity and goes further into what should be measured for effectiveness. As such, the much-anticipated ISO 27004 (guidelines on how to measure effectiveness) in 2007 should finally put an end to this gray area. Hopefully it will shed needed light on the types of controls to be measured and what results, such as Industry Baseline, we should expect.

## What are the benefits of measuring security effectiveness?

- It actually eases the process of monitoring the effectiveness of the ISMS – less labor-intensive, for example, if using tools; and provides a means of self checking;
- Proactive tools to measure can prevent problems arising at a later date (e.g., network bottlenecks, disk clutter, development of poor human practices);
- Reduction of incidents, etc.;
- Motivates staff when senior management set targets;
- Tangible evidence to auditors, and assurance to senior management that you are in control – i.e., through Corporate Information Assurance (Corporate Governance), and a top-down approach to Information Assurance.

Whatever the driver for implementing ISO 27001, it should no longer be just about identifying the controls to be implemented (based on the risk), but also about how each control will be measured. After all, if you can't measure it, how do you know it's working effectively?

This essentially means that all organizations will soon be able to demand Operational Level Agreements and Service Level Agree-

ments for Security – based on real measurements – and will be able to treat security as a measurable business unit, with targets based on Industry Best Practice or ISO 27004.

### What should be measured?

For ease of explanation, the measurements have been broken down into the following four categories<sup>1</sup>:

<b>Management Controls:</b>	Security Policy, IT Policies, Security Procedures, Business Continuity Plans, Security Improvement Plans, Business Objectives, Management Reviews
<b>Business Processes:</b>	Risk Assessment & Risk Treatment Management Process, Human Resource Process, SOA Selection Process, Media Handling Process
<b>Operational Controls:</b>	Operational Procedures, Change Control, Problem Management, Capacity Management, Release Management, Backup, Secure Disposal, Equipment Off-site
<b>Technical Controls:</b>	Patch Management, Anti-virus Controls, IDS, Firewall, Content Filtering

So what is the process for deciding which of these 133 controls (or groups of controls) should be used to measure the effectiveness of security within your organization?

#### Well, first you'll need to:

- Confirm relevance of controls through risk assessment;
- Define objectives, ensuring they map back to the business;
- Use existing indicators wherever possible – or for example, in ITIL terms, KPIs:
- A KPI helps a business define and measure progress toward a particular goal;
- KPIs are quantifiable measurements of the improvement in performing the activity that is critical to the success of the business.
- Identify controls within the ISMS audit framework which can be continuously monitored, using chosen techniques;
- Agree upon the objectives with senior managers as well as staff, before using any tools. Agree this contractually where external third parties are concerned, or through SLAs or OLAs where internal third parties are concerned, e.g., ISO 20000 (ITIL);
- Establish a baseline against which all future measurements can be contrasted and compared;

- Provide periodic reports to appropriate management forum or ISMS owners (show graphs – pictures paint a thousand words);
- Identify Review Input: agreed recommendations, corrective actions, etc.;
- Implement improvements in line with your existing Integrated Management Systems (IMs), e.g., merged ISOs 9001, 14000, 27001, 20000;
- Establish and agree upon a new baseline, review the output and apply the PDCA approach (Plan – Do – Check – Act).

Hopefully, each business will have its own measurements already in place (such as KPIs). The challenge is to set a “measurement” which is realistic, measurable and reproducible for future comparisons.

### Conclusions

Any large ISMS needs to supplement formal audits with self-checking mechanisms aligned with the equivalent of a performance indicator. Nevertheless, for any ISO 27001-compliant or certified ISMS, no matter how small, some basic measurement is both expected and required. Otherwise it will be impossible to demonstrate that any improvements have either been made or are required for corrective purposes. Consider using tools (indicators) that will help assess the effectiveness of a particular security control; examples might include capacity management, where often software-based analysis techniques can be used to supplement any human effort.

Senior management and possibly auditors are more likely to want to see the big picture. Therefore, consider monitoring the effectiveness of a group of controls, incident management for example, plus others. Encourage senior managers to set realistic goals, thereby ensuring that there is demonstrable evidence of good Corporate Governance.

In a changing environment, new baselines need to be set each time a major change within the ISMS occurs. So this is just the beginning. In addition, some of the measurements can be used as potential KPIs, and could help form part of an Operational Level Agreement or Service Level Agreement with internal or external third parties. Either way, you need to be clear about what benefits can be demonstrated (or not) by providing such transparency.

That said, just by creating such transparency in security you may be specifically targeted and judged on your information security effectiveness performance. This will help avoid future misunderstandings about what security is, and how important it is to the organization. However, should things not go according to plan, your efforts could serve as your Achilles heel.

But in the end, a program along these lines ought to begin dispelling rumors that security and risk management is a black art and an unmeasurable one. In fact, we should start to see tangible benefits from measuring and improving ISMSs globally.

Good luck!

### About the Author

*Steve Wright is a Senior Consultant and ISO 27001 Lead Auditor, and heads up the Security Management (ISO 27001 / BS 7799) Team at Insight Consulting, part of Siemens Communications. He is the Senior Consultant providing Professional Services in relation to Information Security / Technology / Management to meet BS 7799, ISO 27001, ITIL, ISO 20000, PAS 56 and ISO 13335 compliance.*

<sup>1</sup> Ted Humphries and Angela Plate suggested the four categories of measurement to be used.