Measuring the Effectiveness of Security using ISO 27001

Steve Wright, Senior Consultant

Whilst the intentions and objectives behind ISO 27001 aren't dramatically different to those in BS 7799:2002, one of the changes with the biggest potential impact to organisations 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 not only demands that businesses specify how these measurements are to be used to assess 'control' effectiveness (there are now 133 Controls in the new *Standard*), but also how these measurements are comparable and reproducible, e.g. 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 (e.g. SLA's, KPI's, ITIL) framework since the mid-1990's 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 organisation or your current service provider.

The whole area of how, and what is good and effective security is often misconstrued, mis-communicated and worse – mismanaged. That said, there are often pockets of good practice within most businesses. This doesn't diminish, however, the fact that we need to think hard about what to measure, how to measure, and when to measure, i.e. it is another process.

As mentioned above, there's often evidence of good security controls already in place in organisations (especially those who have already implemented CoBit, ITIL or BS 7799). Examples include good anti-virus procedures or good physical security. 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.

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 organisations took this to mean 'security awareness training, etc'.

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

Version 1.8
Contact: Steve.wright@iso27002.info

But herein lies the problem, as some companies that have chosen to implement, say, an expensive Intrusion Detection System, but 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 measuring the IDS effectiveness may not have even been considered.

Worse still, very few appear to have done any work on understanding the value or Return on Investment (ROI). In fact, if more organisations weren't 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 costed evidence and we wouldn't be having this discussion. Each control selected would have to define how it was going to be effective and the measurements required would, of course, be documented.

So, how can we select which controls should be measured and, equally importantly, how can these be used to provide 'assurance' to stakeholders and shareholders that 'security controls' are operating effectively?

It's an area of security that's either ignored (for some of the reasons stated above) or is being done – but is not being reported on.

As you may have concluded by now, this isn't a topic that's as straightforward as you might believe. Hopefully, though, what I have achieved by compiling this White Paper is to 'get the ball rolling' on a topic that is difficult and which needs to be fully understood in order to prevent it stifling the anticipated growth in security.

Another reason why this is a particularly 'hot' topic is because industry and leading standards bodies, such as the ISO and BSI, have also struggled to get a grip on it. These organisations are all striving to achieve synergies between ISO 20000, ITIL, ISO 9001 and could really do with finding a set of measurements that can easily be linked in with existing or new Management Systems (e.g. Quality and Service Delivery).

This, coupled with an age of increasing identity fraud, escalating IT costs and frequent corporate scandals, is where regulatory bodies are starting to ask awkward questions about how the CIO, CEO and Senior Management are managing risk and, therefore, the effectiveness of parts of their risk mitigation strategy, including **Security**!

So where to start?

It would be easy to tell you to implement the set of controls contained within ISO 27001 – based on your risks – and to ensure these controls are used to help mitigate, transfer or simply remove identified risks.

That said, please don't make the mistake of ignoring Clauses 4 - 8 (of the *Standard*) as you'll also end up missing out on the fundamentals that make up the ISMS (see Annex A: *Expected ISMS Documentation Set*), which has now become a 'Mandatory' section of the new *Standard*.

In fact, it's often these missing foundation stones that make the task of monitoring effectiveness that much harder to implement. The ISMS is like the house built on solid foundations – when the rain fell, it stood firm.

An ISMS should be implemented by experts – people who understand risk as well as the importance of using the right materials (controls) that will support it as the rain becomes heavier.
An example of a good ISMS might include well defined roles and responsibilities captured within the ISMS Operational Policy This document should also dictate how and where relationships interact i.e. relationships and a communication plan.
An effective ISMS should have clear and unambiguous Management support as well as clear and demonstrable Risk Management – with the ability to link identified risks to Risk Treatment Plans including recorded preventative and corrective actions.

The solid foundations of a well-built ISMS should also have fully documented, tried and tested incident management procedures, full auditing and logging procedures and, above all, a clear strategy of what measurements should be used to measure the effectiveness of security.

So what are the objectives of measuring security?

- To show ongoing improvement;
- To show compliance (with Standards, contracts, SLAs, OLAs, etc);
- To justify any future expenditure (new security software, training, people, etc);
- ISO 27001 requires it. Other Management Systems also require it – ISO 9001, ISO 20000;
- To identify where implemented controls are not effective in meeting their objectives;
- To provide confidence to senior management and stakeholders that implemented controls are effective.

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 be too onerous a task and would cause an already overworked IT Department to crumble under the weight of bureaucracy.

Before we attempt to answer this question, then, we should always understand the requirement for such clarity. Why are you being asked to provide such information? What is the driver? Where does the requirement come from?

Other drivers may exist, too. It could be that the company has just realised that you can get more from ISO 27001, or perhaps it's operational risk management such as BASEL II, SOX, Turnbull (UK Corporate Governance) or simply Regulatory requirements and Legislation that's driving your business.

Either way, you're not alone. Many organisations (but not all) misunderstand the fundamental concepts behind BS 7799 and ISO 27001 and have treated it as a marketing exercise, as opposed to trying to achieve real business benefit and ROI.

Contact: Steve.wright@iso27002.info

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

So what are the benefits of measuring security?

- Actually eases process of monitoring the effectiveness of the ISMS (e.g. less labour 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. Corporate Information Assurance (Corporate Governance), and 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 organisations will soon be able to demand Operational Level Agreements and Service Level Agreements 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).

So what should be measured?

For ease of explanation, the measurements have been broken down into the following categories:

1. **Management Controls:**
   - Security Policy, IT Policies, Security Procedures, Business Continuity Plans, Security Improvement Plans, Business Objectives, Management Reviews
2. **Business Processes:**
   - Risk Assessment & Risk Treatment Management Process, Human Resource Process, SOA selection process, Media Handling Process
3. **Operational Controls:**
   - Operational Procedures, Change Control, Problem Management, Capacity Management, Release

Management, Back up, Secure Disposal, Equipment off site

4. **Technical Controls:**

    - Patch Management, Anti-Virus Controls, IDS, Firewall, Content Filtering

What needs to be measured?

Well, again arguably the whole ISMS (Clauses 4 – 8) section, or group of controls as suggested earlier. Ultimately the risk assessment will confirm the relevance of the most applicable controls that should be measured.

Therefore measurement can be achieved against:

- A particular security control or objective;
- A group of controls;
- Against main controls within a Standard;
- Or the examples given below.

These have been mapped to their nearest ISO 27001 control reference or group of controls (but bear in mind that not all of the controls map easily).

So what is the process for deciding which of these controls (or groups of controls) should be used.

First, you need to:

- Confirm relevance of controls through risk assessment;
- Define objectives, ensuring they map back to the business;
- Use existing Indicators wherever possible, e.g. in ITIL terms, KPIs:
    - A KPI helps a business define and measure progress towards a particular goal;
    - KPIs are quantifiable measurements of the improvement in performing the activity that is critical to the success of the business.
- Within the ISMS audit framework, identify controls which can be continuously monitored, using chosen technique;
- Before using any tools, agree the objectives with senior managers as well as staff. Agree this contractually where external third parties are concerned, or through SLAs/OLAs where internal third parties are concerned e.g. ISO15000 (ITIL);
- Establish a baseline, against which all future measurements can be contrasted/compared;

- Provide periodic reports to appropriate management forum/ISMS owners (show graphs, pictures paint a thousand words);
- Identify Review Input – agreed recommendations, corrective actions, etc;
- Implement improvements within your Integrated Management Systems (IMS) e.g. merged ISO's 9001, 14000, 27001, 20000;
- Establish/agree new baseline, review the output, apply the PDCA approach (Plan – Do – Check – Act).

Measuring the effectiveness of Security - challenges?

Measurement for the operation must:

- Reflect your business goals;
- Be critical to the success of the operation;
- Be measurable, reproducible and contrastable;
- Facilitate corrective action;
- Each measurement requires definition and therefore should ensure the following list is used for each definition:
  - Title;
  - Scope of the metric;
  - Purpose and objectives;
  - Measurement method;
  - Measurement frequency;
  - Data source and data collection procedures;
  - Chosen Indicators;
  - Date of measurement and person responsible;
  - Level of effectiveness achieved (or level of maturity, in case of a maturity metric for controls);
  - Causes for non-achievement.

As each business will probably have its own measurements already in place (e.g. KPI's), the challenge is to set a 'measurement', which is measurable and contrastable for all respondents.

Summary

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 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, e.g. incident management, 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.

You can see from some of the examples below, that measuring the effectiveness of an ISMS is a complex task. It requires time, honesty and a realistic approach to agreeing which measurements can be effective in the business and, significantly, how you intend to measure that effectiveness to ensure results are comparable and reproducible year-on-year.

It's important to ensure all measurements are recorded into tables (i.e. spreadsheets) so that the controls to be measured are captured and comparable. This will also make sure that results from these measurements can be added into the table at different dates and with various results. This will help to assure the integrity of data (as it is captured in one table) and can help when statistical analyses are being prepared (for Senior Management presentations/reports and for calculating expected loss, ROI, etc).

Conclusion

Any organisation that already holds Certification to BS 7799 or ISO 27001 should start to work towards establishing a set of clearly defined measurements. Begin with agreement or commitment from the sponsor (e.g. the business / operations) on defining 'what and how' security should be measured.

In addition, some of the measurements can be used as potential KPI's 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 on what benefits can be demonstrated (or not) by providing such transparency.

That said, by creating such transparency in security, you'll only be judged on your performance. This will help avoid future misunderstandings about what security is and how important it is to the organisation. It could also, of course, serve as your 'Achilles heel' should things not go to plan.

Above all though, it should start to dispel rumours that security is a black art and that it is un-measurable. In fact, we should start to see tangible benefits from measuring and improving the ISMS.

Hopefully, this white paper represents an opportunity for anyone actively involved with ISO 27001 (BS 7799) to start looking at how security can be 'effective' and 'open' to scrutiny, whilst at the same time still achieving your organisation's security objectives.

One final note: Don't forget that all existing BS 7799 and ISO 17799 documentation must have been transferred to the new numbering convention of ISO 27001 (including ISO17799) by 15 April 2007 and that, in addition to legal and regulatory requirements, the updated standard now places extra emphasis on contractual obligations at all stages of the ISMS, including risk assessment, risk treatment, selection of controls, control of records, resources, monitoring and reviewing of the ISMS and in the documentation requirements.

Good luck

Steve Wright

Steve Wright is a Senior Consultant, ISO 27001 Lead Auditor and Heads up the Security Management (ISO 27001 / BS 7799) Team at Insight Consulting, part of Siemens Communications.

Groups of Controls:

1. **Management Controls:**
    - Security Policy, IT Policies, Security Procedures, Business Continuity Plans, Security Improvement Plans, Business Objectives, Management Reviews
2. **Business Processes:**
    - Risk Assessment & Risk Treatment Management Process, Human Resource Process, SOA selection process, Media Handling Process
3. **Operational Controls:**
    - Operational Procedures, Change Control, Problem Management, Capacity Management, Release Management, Back up, Secure Disposal, Equipment of site
4. **Technical Controls:**
    - Patch Management, Anti-Virus Controls, IDS, Firewall, Content Filtering

Management Controls - Examples

Group of Controls Reference	ISO 27001 Reference	Title	Explanation and objective of measurement	Target / objective of measurement, mechanisms	How these measurements are to be used to assess control effectiveness to produce comparable and reproducible results
Clause 4	4.2.1	Effective Information Security Policy	Communicating to the organisation the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement.	Measured through success of achieving initial sign off from CEO/CIO, then periodic reviews performed twice a year.	Measured by how available and widely the InfoSec Policy is known and understood. Interview random employees to quiz on the level of awareness / understanding.
Clause 7	7.2, 7.3 & A.6.1.1	Management Input & Output Review	The management must annually review the ISMS and all supporting documentation. In addition, the Management must review the measurements chosen to ensure improvements are made appropriately and are working effectively.	The input to a management review shall include results from effectiveness measurements. The output from the management review shall include any decisions and actions related to Improvements to how the effectiveness of controls is being measured.	Each year the review should include a review of the previous year's results to ensure similar findings are not being repeated, or remain unresolved. This should provide demonstrable evidence and comparable results.
	4.2.1	ISMS Documentation Set (See supplied example at end of this paper)	Take status snapshot (record as %) of completed Policies and Procedures that support the ISMS	Measure completed documentation by end of Yr 1 – target 90%, and then 95% in Yr 2, Yr 3 should be 100% complete.	Every year review all ISMS documents to ensure still meet objectives and provide comparison to previous years' results.
A.15	A.15.1.2	Effective Technical and Policy Security Measurements	% of IT systems conforming to Security Policies and standards, less than 50% in first year, 75% in year two and 95% in year three.	Measured through a % of security IT spot checks and series of internal IT audits performed in a year.	# of spot checks should start stabilise after 2nd Year. % of opportunities for improvement discovered should decrease over three year period. By end of Yr 1 = <90%, Yr 2 = <80%, Yr 3 = <70% of discoveries.
	A.5.1.2	Effective Security Policy	Additional eLearning and frequent questionnaires on employees' understanding of top ten security issues facing organisation.	% of employees received eLearning training <50% in Yr 1, <80% in Yr2, <99% in Yr 3.	% of respondents to questionnaire increasing year on year. % of respondents tested improving results year on year.
A.7 Information Classification	A.7.2.1	Data Classifications	Number of systems with appropriate data classifications.	Target 90% in first year rising to 100% by year three.	Spot check of systems to ensure appropriate classification.

Business Processes – Examples

Group of Controls Reference	ISO 27001 Reference	Title	Explanation and objective of measurement	Target / objective of measurement, mechanisms	How these measurements are to be used to assess control effectiveness to produce comparable and reproducible results
SOA	4.2.1j	Statement of Applicability	1) the control objectives and controls, selected in 4.2.1g) and the reasons for their selection; 2) the control objectives and controls currently implemented (see 4.2.1e); 3) the exclusion of any control objectives and controls in Annex A and the justification for their exclusion.	Applicability of each control reviewed annually to ensure appropriateness.	% of accuracy to be maintained at >95% year on year and compare accuracy % from previous year.
Risk Assessment & MOR	4.2.1.d,e,f,g	Risk Assessment, Risk Treatment process and Risk Register	Control objectives shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process (including updating of risk register).	All risks should be incorporated within centralised risk register and the # of risks managed should be identified and managed within a specified amount of time e.g. amount of time taken to respond.	Statistical analysis should be used to present graphical representations of MOR and the number of unmanaged risks should remain below an agreed threshold.
Risk Treatment	Clause 8	Risk Treatment Plans	Formulate a risk treatment plan that identifies the appropriate management action, resources, Responsibilities and priorities for managing information security risks.	Risk Treatment is one of the principle objectives of InfoSec and therefore measuring the effectiveness will ensure the results are reviewed and improved.	Number of critical systems with risk analysis conducted equals X, then <X by end of year, /2 by year two.
A.13 Incident Management	A.13.1	Incident management	To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.	Quantity unknown therefore based on less than 90% by end of year three. Or, amount of time to investigate to be reduced by half the response time within a year. Number of days required to help investigators reduced to four days over three years.	Number of security breaches reduced on a year on year basis.

Operational Controls – Examples

Group of Controls Reference	ISO 27001 Reference	Title	Explanation and objective of measurement	Target / objective of measurement, mechanisms	How these measurements are to be used to assess control effectiveness to produce comparable and reproducible results
A.10	A.10.1 Operational procedures and responsibilities	To ensure the correct and secure operation of information processing facilities.	To validate if appropriately procedures are in place to safeguard the organizational assets, the ISMS needs to demonstrate everything has been documented where relevant to the business.	Measurements can be applied by either using the document management system or documents that contain procedures relating to, or potentially affecting the ISMS i.e. Back up Procedures, Off Site removal of assets.	Annual audits and the number of incidents will indicate whether such controls are working and being effectively used. Evidence: ▪ Annual audits of QMS and/or DMS ▪ Number of requests for removal of assets approved by the InfoSec Mgr ▪ Review of Segregation of duties (part of audit process)
A.10.3	A.10.3 System planning and acceptance	To minimize the risk of systems failures.	System planning and acceptance should be controlled under configuration management, change control and capacity planning techniques.	The number of systems / processes that fall within these control mechanisms will determine how much measurement can be applied.	Annual audits and the number of systems that qualify for these controls should be improving. This will indicate whether such controls are working and being effectively used. Evidence: ▪ Audit results confirming change management, configuration management and capacity planning is operational and working. # of Non Compliant findings should decrease year of year.
A.10.5	A.10.5 Back-up	To maintain the integrity and availability of information and information processing facilities.	Whether Back up procedures are being followed according to the policy and procedure, will be used to measure against the Policy.	The objective of this measurement will be to ensure Back-up is done in a coordinated and regular fashion. This measurement will help identify any potential problems with restoring from back-up (a best practice requirement).	Effectiveness will be measured against whether the Back up Policy is being applied across the relevant areas identified as requiring regular back-up. Evidence: ▪ Audit Findings

Technical Controls (examples):

Group of Controls Reference	ISO 27001 Reference	Description of KPI	Explanation of measurement:	To measure the effectiveness of the selected controls or group of controls	Specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results
A.12	A.12.6.1	Availability of patch management facilities	To validate if the patch management facilities are in place to safeguard the organizational assets, the ISMS needs to demonstrate everything has been documented where relevant to the business.	The number of systems / processes that fall within these control mechanisms will determine how much measurement can be applied.	% systems under central patch management equals Z, <Z by end of year one and so on.
A.13	A.13.1.1	Time to deploy patches (critical, intermediate, low)	The time taken to deploy measurements should be considered as a key indicator as to how well the patches can be deployed from identification of a vulnerability.	The number of systems / processes that fall within these control mechanisms will determine how much measurement can be applied.	Average implementation time critical patches equals W, then <W by the end of year one and so on until 100%.
A.10	A.10.10.3	Availability of log collection facilities / access to security log information	The availability of log information and the collection process will help to validate if the process is in place and operating effectively.	The number of systems / processes that fall within these control mechanisms will determine how much measurement can be applied.	% systems monitored (IDS and/or log collection), target all critical services by end of year one.
A.8	A.8.3.3	Time to revoke account from notification	The time taken to revoke an account from the systems demonstrates how well an organisation is controlling access in the first place.	The number of systems / processes that fall within these control mechanisms will determine how much measurement can be applied.	Average account revoke time equals W, then <W by the end of year one and so on until 100%.

Annex A:

Expected ISMS Documentation Set:

- Information Security Policy (one page document);
- ISMS Scope;
- ISMS / BS7799 Project Initiation Document (PID - Project Plan);
- ISMS Operational Manual (Org chart and reporting structure / objectives);
- ISMS Roles and Responsibilities (Project sponsor and business owners);
- Information Security Forum (Terms of reference);
- Information Asset Register (All critical business information assets);
- Risk Methodology and Risk Treatment (Policy and Procedure);
- Security Improvement Programme (Incorporating risk assessment results, Pen test results, audit results, etc);
- IT Technical Security Policies (e.g. Change Management Policy, Malicious Code Policy, Software Development Policy);
- Security attributes of IT systems (e.g. ISMS Scope only e.g. Access Policy, RAS Policy, Security Network Topology, BS2000 Mainframe Security Access Control Policy;
- Security Awareness Campaign Programme (PID - project plan, objectives);
- Statement of Applicability;
- Security Audit Policy & Framework;
- Audit procedures and schedule – tied in to QMS?);
- Security incident, investigation & response procedures;
- Monitoring, Logging (IDS and Firewall) policy & procedures;
- Data retention policy & procedures;
- Business Continuity Plans and DR procedures.

Summary:

Steve Wright is a highly qualified, motivated and adaptable Team Leader / Business Development Manager/ Information Security Consultant who is an effective communicator and organiser, accustomed to meeting deadlines and targets. With a wide range of experience and proven track record, possesses positive self-motivation as well as excellent interpersonal and presentation skills.

He is the Senior Consultant providing Professional Services in relation to Information Security/Technology/Management to meet BS7799, ISO27001, ITIL, BS15000, Tickit and ISO13335 compliance. Working with best practices in Risk assessments methodologies, like CRAMM, COBRA, RA etc including, Business continuity management with PASS56.

He is currently project managing many implementations of ISO27001 IMS systems, both virtually and physically, from initiation through to final delivery, to meet certification requirements of BS7799 / ISO27001 and BS15000 in both financial, private and public service sectors, two of which have recently achieved Certification to ISO/IEC27001:2005.