Global Information Assurance Certification Paper

Methodology for security policy audit using the ISO 17799 framework

David T. Rockwell
SANS GSNA 1.0
July 18, 2001

1.0 Overview

The basis of this practical is the assertion that security policy, the written body of guidelines, standards and rules intended to govern security practice, is itself a worthy object of audit activity, since the content of that policy will,and should, impact security practice across the organization. (ref: Michele Crabb-Guel) . A high quality and complete policy may guide the behavior of the organization, management, and users, while a poor or incomplete one may impede good security practice, for example in platform security parameters, or in end user access controls. Additionally, security policy may provide the framework for security communications, enforcement and prosecution.

The security auditing field is often partitioned according to the "object of service" or broad categories of such objects, (ref: SANS Audit Track) for example:

a. "perimeter", to refer to those parts of the network most exposed to the public internet, and thus most exposed to the largest threat set.
b. "platforms" such as Unix, Windows 2000, MVS, OpenVMV etc.
c. "defenses" including routers and firewalls and intrusion detection.
d. "networks" such as intranet, dmz, and similar security related partitions
e. "applications" such as web applications which run on the aggregate of all those objects

We are familiar with specific audit procedures for specific objects, for example to check an access control feature in Windows 200 server. We can perform a procedure to ensure compliance that a given access control feature is operating. The aggregate of all such procedures for a given platform, are the "audit" process for that object of service.

But what will ensure that the organization will even specify that such feature is required, present and enabled? This is the role of security policy. The evolution of best practices in security gets passed on in many forms, RFCs (e.g. ref: Site Security Handbook, Security Glossary) , "Best-Practice" documents, How-To documents, many different types of forums (e.g. BugCheck) and vehicles (e.g. Incidents.org) Each organization or company has to interpret that body of knowledge in the context of its operations, business needs and relationships. And this must be done in the context of today's computing infrastructure: a rapidly changing, complex and multi-layered environment, presenting a daunting array of implementation choices. Wide inconsistency in security policy from one organization to another, should be not be a surprise, given this situation. Yet we know that complexity and weak links are the friends of the attacker, or put

another way, the security of each depends on the security of all. *"Security is a chain; it's only as secure as the weakest link."* (ref: Secrets and Lies by Bruce Schneier) Clearly this is a recipe for deterioration, unless it is addressed. One such effort has risen to the level of international standard, namely ISO 17799, which evolved from the British Standard 7799.

ISO17799 provides a structured way, a framework, for approaching information security, beginning with security policy. It can be used to derive checklists for policy, procedure and practice. Audit experience has shown that the content of audit plans are often quite close to the content of assessment checklists (ref: Marchany- SANS Audit Track 7.1) . Therefore, the premise is to develop a methodology and process for a policy audit, using ISO derived checklists as the basis for the audit, to help organizations measure performance.

While not perfect, and consensus is very hard, it is :

1. a structured way to examine the policy and
2. a way to institutionalize (collect and improve upon in a public forum) that common body of knowledge that ought to be internalized into policy, and
3. a way to assess a policy and find the gaps (if methods can be found)

This paper will propose a method to perform a policy audit using the ISO framework, and then examine a policy using a selected method. I'll choose one of the 10 ISO domains for an in depth examination of objective scoring techniques which might be applied, for gap detection and policy adjustment.

1.1 Terms

- object - usually something in the physical world, a system, a control, a document, known by its interface. In this paper, a written policy is also an object, and it should function similar to a parent object in the programming world, by providing attributes that are common across child objects
- element - I'll use element to refer to actionable parts of the ISO specification. For example, section 9.2.1 User Access is an element under the grouping "UserAccess" in the domain "Access Control". A grouping has a formal objective while an element contains a set of related controls, that can be implemented to achieve the goal.

2.0 Research

2.1 Current State of the practice

- **Site Security Handbook (RFC 2196)** - this is a guide for developing site procedures and computer security policies. It replaces and builds on an earlier work of the same name, (sponsored by the ITEF, RFC 1244) . Its definition of the purpose of security policy is still an excellent one:

> *"The main purpose of a security policy is to inform users, staff and managers of their obligatory requirements for protecting technology and information assets. The policy should specify the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. Therefore an attempt to use a set of security tools in the absence of at least an implied security policy is*

meaningless."

RFC2196 identified many of the principles, tradeoffs and best practices that became incorporated into the ISO standard. RFC2196 made a distinction between security policy and security plan. Security policy focuses on the networks, the services, and the computing facilities whereas the plan contained the what, who, how details, and specifics on incident handling (ref:RFC2196, section 3.1.1). In the ISO model, this distinction is blurred somewhat, but the basic idea that more detailed, site-specific particulars which might change often, be maintained separate from rules and guiding principles, is a good one, and one which is supported in various parts of ISO 17799.

- **ISO 17799 history** -The ISO Working Group is named the Joint Technical Committee 1 - "Information Technology", Subcommittee 27 - "Security Techniques", Working Group 3 - "Security Criteria" (more simply referred to as JTC1/SC27/WG3 or just WG3 for short). ISO 17799 was prepared from its forerunner BS7799, by the British Standards Institute, then revised and reformatted for international use. BS7799 consists of two parts, a code of practice (-1), and a subset with certification process (-2). Only the code of practice (-1) moved forward to ISO and most of the G7 countries objected. There was considerable debate during its gestation, and several negative committee votes before it was finally adopted. The primary debate is whether such a thing should be a "standard" or rather just offered as a set of guidelines. The controversy centers around "what can be measured objectively", a topic that was also specified as a requirement to consider in the SANS GSNA practical assignment (i.e. this paper), so this appears to be a central difficulty whenever this subject is considered. However now ISO 17799 has passed, and there is considerable demand from customers who want to know where they stand with respect to its recommendations. ISO17799-1 was renamed to 17799:2000. Any certifications regimes related to it will most likely spring from country specific standards, as ISO has indicated that it will not certify. There is a revision to ISO17799 in the works, to be taken up at the ISO working group meeting in Seoul in October 2001. There is some reason to believe that requirements that are part of ISO 17799 might find their way into the Common Criteria (see future directions, below)

- The **Center for Internet Security (CIS)** (ref) has introduced the concept of benchmarking systems with a security benchmark. This would measure the implementation of security controls for systems. This is similar in concept to measuring policy against InfoSec practices embodied in ISO 17799, if a way can be found to express those policy elements in measurable units.

- **Risk Associates -** (ref:) I was able to locate one firm that had developed the idea of scoring a set of ISO derived questions, although the method was not described. A proprietary tool download (Cobra) was available to try on a trial basis. This is a standalone application which poses a series of questions, gathers answers to a database file and provides a report generator. The questions seem to be categorized into optional and required buckets (This is a UK firm and this may be from the UK national standard which does have a certification scheme, however I was unable to obtain it). The resulting report is presented as a Non-Compliance scoring, for example my "Business Continuity Management" was reported as 97.92% non-compliant based on 9 required and 3 optional questions. I was not able to

deduce the method. The "Improvements Needed" section for that domain provided one recommendation, that I should have a managed process for Business Continuity Management. Even so, I felt somewhat validated in a quest for a open method that might be used. I was somewhat confused by the formulation of some of the questions and gaps in the questions relative to the ISO text. At times questions that seemed to relate more to implied implementation details rather than the policy root. What I learned from this is that there is a fair amount of subjectivity and national or regional "color" in the formulation of the questions, even though the claim to "standards" derivation may be valid. I suspect this is unavoidable and in fact a good thing, perhaps it is at the root of ISO's position not to provide a certification regime. Furthermore, the refinement of these derived interview sets and the methods for their scoring may in fact be the differentiator for companies providing services in this area. We are indebted then, to the UK for the BS7799 heritage and to Risk Associates for leading the way with a tool to support it.

2.1.2 Reasons to Change

Improve defenses, remove threats

The ability to effectively prevent and/or prosecute misuse often comes back to the policies which are in place. If individuals have not been informed of surveillance and counterintelligence activities, or have not been exposed to security awareness training, the prospects of civil and criminal remedies may be severely limited. In fact, the organization may expose itself to liability issues when it undertakes certain privacy limiting activities without a supporting policy foundation. (ref: Understanding Cyber Attacks).

There are many aspects of security that must be addressed by parts of the organization beyond the security apparatus, for example, the HR or personnel group, the training group, system administrators, and the users themselves. A unified and comprehensive security policy framework which all parties use, will be the focal point for security policy enhancements. When new technologies or products are being developed, it is more probable that appropriate security controls are included if there is a common security criteria. (in fact this is the logic of related efforts like Common Criteria, and Trusted Computing Platform) . Conversely, when new technical implementations of security controls are developed, its much more likely that the policy underpinnings will be developed if there is a pre-existing framework that everyone uses as its starting point.

And in today's hyperlinked world, it is useful to have related information linked, for example, to have the security objective linked to a related security best practice statement which is then linked to implementation details (on multiple platforms if necessary). Clearly if the framework exists, there is an ability to structure downstream data in a way that relates the two, which can only strengthen legal and practical requirements to do so. There have been numerous attempts to do just this at the system level both in software tools and in technique documents, (ref: Naidu - SANS) . With an ISO framework in place, an opportunity exists to take this technique to a new level for security policy.

Who should perform the audit?

There is a reasonable amount of consensus on the who and how when it comes to auditing security practice. Generally, when talking about security implementation and practice, it is considered good practice to have two different groups involved, one group to define and implement policy and a different group to conduct the audit. The person who implements a set of controls on a web application, will probably have a favorable impression of his efforts (see also ref:RFC2196). So we ask a different person, an outsider perhaps, for an objective

appraisal. But it is less clear, for example, who might detect a security practice omission, due possibly to a policy gap. It would follow that an audit of security policy should be performed by an independent entity, and that the policy itself be an object of audit activity. But the questions remain. How do we make the policy itself an object of service? What are the criteria which should be established for the audit? This is where the ISO 17799 framework can be helpful.

What represents a complete policy?

Perhaps the best reason to perform a policy audit against some sort of best practice framework is to detect omissions and gaps. Any individual policy element can usually be qualitatively compared to best practice examples, but by using an audit checklist of essential elements one should be able to identify elements which are missing. Logically, this would be a valuable tool to have, even if it were not addressed by international or national standards.

The case is often made that standards bodies move too slowly in relation to the operational needs in the real world. However, we need not wait for the standard to begin trial implementations. Emerging requirements are often the subject of discussion and education at conferences and consortia such as SANS, where this year four new elements appeared on the SANS roadmap. At the conferences, emerging requirements can be discussed in the context of new technologies or new threats, or proposed security controls. Consensus then builds (or not) with respect to treatment in the standards arena. Major new security topics may become the subjects of various industry consortia with competing alternatives. This is a good thing if excellence rises to to the top and if the standards bodies remain independent, in the role of "institutionalizing" progress.

For the specific case of auditing security policy, security practitioners always have the option to include additional elements on top of the standards base and to differentiate on the basis of coverage of current security issues, much like security software companies differentiate on the basis of rapid updates. However, to the extent that the ISO standard "institutionalizes" the common, long-agreed baseline, we achieve some consistency across that portion of the population that subscribes to it. When all accept the baseline and contribute to it, there exists a common body of knowledge to mitigate the "weakest-link" effect, (ref: Secrets and Lies) wherein a system with a known vulnerability is used to violate a system that would otherwise be secure.

Complexity complexity complexity...

Security was already a huge topic before the web came along, there are numerous RFC's and papers addressing aspects of system and network security. Then came privacy and data protection laws, new security technologies, and an explosion in interconnectedness, to the point where the corporate boundaries are often now defined as much by a series of software constructs as physical ones. Add to the mix a number of wireless technologies with their own individual security issues, web based applications and instant messaging with abilities to traverse firewalls. Bruce Schneier makes the point that this level of complexity is already untenable for the majority of organizations and it is going to get worse. This is the case for security specialization and for managed security services, however, an organization is *never* absolved of the legal, moral and regulatory responsibility for security policy. (ref: Bruce Schneier). The ISO code of practice framework can be a structured way to execute that responsibility and by the same token, a security audit using that framework can be a structured way to examine it.

2.1.3 What can be measured objectively?

There are 10 domains in the ISO standard, they are:

- Security Policy
- Security Organization
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

We can examine the actual "Information Security Policy" if one exists, or more likely we can examine a body of work that is identified as "Security Policy" by those individuals reported as responsible for aspects of security. The bulk of controls that we typically associate with information technology will usually be the assigned to an MIS or IM department, especially controls enumerated under Communications and operations management (section 8), Access control (section 9), and Systems development and maintenance (section 10).

We can ask questions, that is interview site people identified as experts on information security policy. This serves a dual purpose:

1. Get to the relevant documents faster, especially if the organization of documents is less than obvious.
2. Get at "implied policy", that is unwritten security policy, or other kinds of documentation and guidelines which is simply not labeled as such.

We can examine the ISO 17799 standard. This will be the "Ruler". The examiner will be in the position of comparing the ruler to the actual security policy, that is the investigative results. It should be useful to this purpose to derive a set of interview questions, in policy terms .

From the standpoint of the subjective/objective dynamic and looking forward to the happy day when security policies can be evaluated for quality, we should look for ways to express binary questions,

- yes / no
- present / not present
- assigned / not assigned etc.

In some cases, we may be able to split an ISO statement down further, into bite-size binary statements, or to express subjective input which speaks to quality or to completeness as a percentage or score, in order to achieve this.

In almost all cases, though, this is really "subjective", as we are asking humans for a judgment about the element rather than reading a control, or testing a "bit". Enterprises write "policy" to be long lived, describing high level intent and lacking implementation details, which in any case are often platform dependent. For example, a policy on "Remote Diagnostic Port Protection" might indicate the policy goal, while the specifics of "how" to accomplish the goal are left to a set of platform specific documents. When auditing a specific platform, some business critical server for

example, we can often use some tool or utility to read that control. This is quite objective, and it would be desirable to aggregate a lot of such objective evidence into higher level conclusions about policy compliance, if it were practical and possible. But besides taking forever, the audit would miss the parts of policy that relate to human and organizational dynamics.

A better strategy, would be to obtain the objective data on a sample basis or against specific objects of service, and "objectify" the subjective data, as much as possible, to permit reasonable comparison. In the short term, at least, we must ask humans or a consensus of many humans, to try to quantify these judgments. Maybe at some point in the future with natural language processing and unlimited computes and memory it will be possible to feed all sorts of inputs into an objective policy analyzer, but clearly we are not there yet. Furthermore, if we have learned anything about security in the last decade it is that technology alone cannot address the whole problem. A few quotes from the Bruce Schneier book - "Secrets and Lies" (ref: Secrets and Lies by Bruce Schneier)

> *"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology"*
>
> *"Security is a process, not a product."*

Security practitioners who have been consulting in this area for a long time, still point to social engineering, process and human behavioral elements as being the key weak links. from "Information Security Policies Made Easy" by Charles Cresson Wood (ref:)

> *"Information security is just one of many subspecialties within the information technology field, but its costs are also dominated by labor. The information security field is still in an embryonic state, and many of the essential activities have not yet been automated. This means that all organizations, no matter how sophisticated they happen to be, will be critically dependent on the work of people in order to achieve a truly secure information technology environment."*

It follows that observation of and interaction with the customer's people and facilities, will be valuable input for security policy auditing, even if great instrumentation and logging permits the gathering of objective data. So the answer to the question "What can be measured objectively?" is really, not much. We can look to technology for help at the network, and platform level, and for help in gathering, digitizing and analyzing what is essentially subjective data. We can examine written material that actually exists on the customers site, if it is reasonably organized and aggregated, i.e. if there is sufficient time within the bounds of the audit window.

2.1.4 What must be measured subjectively?

There are several broad classes of subjectivity involved in the policy audit.

1. **What is included as policy?** There has been a lot of discussion in the past, about the distinction between security plan, security standard, security policy, and security practice. For the purposes of the audit we want to determine what is addressed by written material intended to guide behavior and practice, regardless of what it is being called or how it is formatted, or which organization is managing. For example, the security policy documents may not be addressing some of the ISO requirements in the personnel domain, whereas the HR website is doing a credible job. For the purposes of the audit, we can evaluate those documents, interviews, and survey responses, even though there may be some work to do in

order to pull that content into a cohesive security framework.

2. **What is included in the audit?** As noted previously, there may be opportunities to quantify some of this input. In other cases, the evaluator may decide to entirely dismiss a category as ambiguous or not applicable to this client for some reason. For example, if the security policy of the site is to disallow all remote access, mobile computing and teleworking, then qualitative information about those is of little value.
3. **What is the quality of the policy with respect to a class of controls?** Estimates of quality and completeness usually require human subjective judgment, that is qualitative information which speaks to the nature of the control or policy element being evaluated. The ISO standard will typically indicate that such and such a control should have attribute A,B and C. Depending on the wording of the interview question, a respondent may want to indicate partial compliance.

2.2 Proposed Method -

1. **Preparation -** Develop the "*Interview Set*". While this is mostly one-time work, there should be a post-engagement feedback step to look for opportunities to improve the Interview Set.

   Elements from the ISO 17799 standard must be distilled into questions. Questions should generally be of the form:

   "Does the policy address....?".
   "Is there a policy that...?"

   Its OK to have qualifier questions that ask about security practices to ascertain implied policy as long as the main element is addressed.
   There will be both objective and subjective elements mixed together, since this is a grouping according to the ISO framework.

2. **Data Collection -** In this phase are the normal audit activities of inspection, interview, data gathering. This is many-time work, a process that must be repeated for each audit.

   Collect into one place all the written policy elements.
   Determine who are the right interview candidates for a given policy domain (e.g. network administrator to answer network access control set). A preliminary questionnaire sheet sent to a wide distribution may help identify the right participants.
   Conduct the interview(s) with the objective of answering those questions.
   In some cases, it may be desirable to get several knowledgeable people in a room and try to achieve group consensus on the answers to the interview set for a domain. This is particularly true if there is no central repository or central department for security information. In large organizations, it is typical that HR control personnel and security awareness training, that a Security organization deal with "guns and badges", physical security, facilities etc., and an MIS or IT group deal with systems and networks.

3. **Analysis -** In this phase consensus best practice, as represented by the ISO framework is compared to information from the data collection phase, in other words comparing what policy is to what it should be. The main activity with respect to ISO comparison, at least in the early application of this method, is expected to be identifying gaps in coverage. An example of a gap would be no policy at all with respect to error logging or clock synchronization. In some cases, little analysis will be required as the answer will be supplied in total by the data collection step. In other cases, for example the "I don't know" from the interview, the evaluator will have to resort to secondary evidence, additional investigation, collected documents and other on-site data to come up with the answers.

4. **Reporting -** this is just the normal step at the end of any consultative process where the results of the analysis are summarized and documented and presented to the client.

2.3 Scoring the responses

2.3.1 Hierarchy of Interview Questions

After reading the ISO standard, I had the distinct impression that the framers deliberately chose wording and partitioning that would lead one down the path I was headed, that is to partition the information space into smaller manageable parts. The process of deriving interview questions seemed very straightforward. My experience was that I tended at first to formulate questions in terms of practice rather than policy, and some discipline was required to keep at the policy level.

- An element in a given ISO domain is examined.
- Ask whether there is a policy dealing with this topic. I came to think of these as primary questions. A given ISO element might give rise to one or several primary questions.
- Ask more questions dealing with the controls which are suggested. I saw many cases where affirmative answers might lead to related follow up questions to determine additional levels of detail or to get to qualitative information about the topic. These I came to think of as qualifiers or secondary levels.
- I did not notice cases of tertiary levels, but if one is going to partition the interview set in a hierarchical way, it would seem prudent to allow for this in any scoring methods that might be chosen.

There are 10 *domains* in the ISO standard, they were enumerated above. Each domain in the ISO standard has some number of topics, a (sometimes broad) set of related practices, for example in the Physical and environmental security domain there are 3 such groupings

1. Secure areas
2. Equipment Security
3. General Controls

   Each grouping has a business goals objective and a short narrative to describe best practice in a very general way, followed by some number of specific best practice *elements* or *controls*. For example, the "Secure Areas" topic has the elements:

   1. Physical Security Perimeter
   2. Physical Entry Controls
   3. Securing offices, rooms, facilities
   4. Working in secure areas
   5. Isolated delivery and loading areas

Within each element, I would try to derive a set of primary questions, and secondary questions intended to qualify or expand a given primary. I would try to preserve the element heading text and numbering for subsequent cross-reference back to the standard.

2.3.2 Scoring alternatives

I considered two scoring methods.

On the first pass, after deriving perhaps half the interview questions, I felt that I would be able to

frame the primary questions as binary questions, with an affirmative answer being an enabler for a secondary set of questions on that element (if there were any). The secondary set of questions would be weighted take-aways from an affirmative. For example, a primary with 6 secondary qualifiers, and only 4 being addressed by the policy and site standards, would yield a 1*4/6 or 2/3 score (66%) for that element.

Then, a refinement was added to allow a primary and any associated secondary questions to be ignored, NA for Not Applicable.

After it became apparent that many elements had standalone primary questions, to which binary answers would or could be misleading, I settled on a simple uniform range scoring for all questions. As long as the range included zero and one, yes or no answers could still enable any qualifier questions. A finer granularity was possible in either case. I decided on six selections for all questions, for example.

Does the policy require that remote users be authenticated? (Q:9.39)

○0 ○.25 ○.50 ○.75 ○1 ◉na

3.0 Application

3.1 The Audit

3.1.1 The One-Time preparation work

The first step is to obtain a copy of the standard from ISO or the US board at ANSI (reference) and derive questions which will be answered by a combination of investigation of written documents, observation and interview. Doing this for the entire standard is beyond the scope of this paper, because it is a very large task, at last count approx 350 interview questions. Instead, I'll show one domain in detail, the last domain "Compliance", ISO 17799 Section 12, for which I developed 30 questions.

I chose an HTML form for the display of the interview questions, because of the powerful linking and wide area data gathering opportunities that become available by using the ubiquitous browser interface. The HTML format is equally adaptable to laptop use during a live interview. Any post processing or data reduction tools could be used as well on the laptop, or served from a standard web server CGI interface.

After trying a few presentation alternatives, I decided to add some cross-reference aids.

1. Question Counter: so that question identifiers on the forms could be exactly matched to results displayed and stored. I decided to maintain a count within each domain and also a running total across all domains.
2. Headings: to match the ISO standard down to two levels. This is used to provide some contextual meaning in synch with the standard, for example, that this small set of questions is about "data protection and privacy" under the broad heading of "Legal Requirements". The level of granularity was somewhat arbitrary but experience with the standard usually led to a smallish number (2-4) of questions and this felt good. Somewhere in my past I learned that humans like things in small doses.

3. Section numbers: to match the ISO standard table of contents. This is provided purely as reference for examiners who might be likely to actually purchase a copy of the standard. For those who might not spend the money, I considered a help facility to provide additional meaning to questions (see future directions)

I also added a text area so that comments/clarifications about a question could easily be related back to the question that prompted them (the name for the text area control uses the same question identifier from the counter.) The result was presentation like this:

Regulation of Cryptographic controls (12.1.6)

- Does the policy address import/export of cryptographic controls? **[Q:12.18]** /18
  ○ 0 ○ .25 ○ .50 ○ .75 ○ 1.0 ○ na

The completed form is attached to this document:
See Attached: Interview Questions ISO17799 Sec 12: Compliance domain

3.1.2 The Data Collection Phase

I took the following steps in the data collection phase.

1. I explained what I was trying to accomplish to the IM security manager of a large Fortune 500 company, who assigned someone to answer the questions.
2. In conversations with my contact,it quickly came out that the company did not have a information security policy per se, rather sets of internal standards, policies, and procedures split between various organizations.
3. I was given access to the intranet at one site and a list of several sites containing company-wide policy info. I located and read as many of the policies as I could, that seemed to fit into my chosen domain, section 12:Compliance
4. There ensued a time consuming iterative process of discovery, which parts of the company controlled which documents (e.g. human relations (HR), Safety, Information Management (IM), and Security) and to identify the right individuals who would be available for interview. My contact was able to supply other contacts, for specific elements. Some were unavailable. All were physically distant.
   Finding#1: This revelation (probably an obvious one for established audit practitioners) led to my first resolution for "future directions", a preliminary questionnaire to assist in this discovery.
5. Therefore, it became necessary to expose the same questions to multiple individuals to obtain a complete picture of policy in this domain. This was done at considerable physical distance so the forms were emailed.
6. I developed a prototype Web CGI application, to display a results page, which then could be emailed back to me. (see attachments)
7. I received some redirection which refined the policy sites to look at and the people to ask. One participant called to explain that Intellectual Property Rights questions would be better handled by another group. One participant provided primarily names in the comments box, who she felt could better answer the questions, which resulted in another round of introductions and sending forms. I received better than 50% completion from three participants.

Finding#2: Another approach, assuming the proper participants had been identified, would have been to use the knowledge of which departments managed which policies to prepare per-department customized interview sets.

3.1.3 The Analysis Phase

The results from IM, Business Practices and Security departments were received. None were complete and there was some overlap This posed some unanticipated scoring problems. I talked to the individuals to clarify which department was responsible. Where there was joint ownership or ambiguity I decided to use the lower score reasoning that this was most conservative risk estimate. Some algorithm to combine scores, or average might also be a reasonable approach.

The combined result page is the 3rd attachment., in the same format as the CGI program returns.

In addition I gathered some general comments from phone interview and email.

- "Some of these questions come close to 'please state the date when you stopped beating your wife' ".
- How are you going to combine responses?"
- first lastname owns that
- "talk to legal"
-

The result page was saved as a flat file and post processed with a simple perl script getscore.pl (see attachments) to do the scoring. The answers are listed by the program, the answers tagged as Not Applicable are removed from the total and the remainder scored, producing as output as follows for this audit:

```
Total Questions Applicable: 26
Domain Score: 0.754807692307692
Domain Risk Factor: 24.5%
```

The comments which returned provided clues as to additional documents and people who should be queried. The analysis of these inputs, along with some explanatory text around the score, provide the narrative of the audit. A full ISO 17799 review is beyond the scope of this paper, however the analysis for Section 12 is included in the audit report attachment.

3.2 Evaluation of the Audit Method

The primary shortcoming of this audit was its dependence on the survey method. The results could have been obtained far more effectively in a face to face workshop of the participants, if circumstances had permitted. And I believe the quality of the output and feedback to the interview question set would have been better.

Clearly, preparation is the most important success factor, followed by easy access to the policy information and the people involved with the policy.

I am not satisfied with the interview question set. I really think its going to take a while to refine this.

A preliminary questionnaire to relevant departments would have identified the participants sooner, also making the process smoother and faster.

These factors translate into improvements for future work, identified in the next section.

3.3 Directions for future work

What can be done to improve the state of the practice?

More modern collection tools and post processing of data would be helpful. The auditing of controls will increasingly be subject to technology solutions to read status of those controls and compare with desired state. But I doubt that the auditing of policy will succumb to such solutions very soon. This is because of attributes like human behavior, emphasis on process, and subjective interpretation of guidelines. Nonetheless, we can certainly improve the tools available to the examiner.

I use the analogy of the lie detector and the FBI examiner. It is generally accepted that the validity of those tests, a type of audit, depend heavily on the skills of the examiner. The methods and machines have gradually improved from the days of analog instruments, to the application of digital techniques and mathematical algorithms which can achieve 97% accuracy, in the hands of a trained examiner. However, achieving that level of accuracy still depends heavily on the understanding by the examiner of the context of the inquiry and the framing of the questions, which requires far more preparation and investigation, than the actual examination (source: recent McNeil/Lehrer interview with FBI examiners).

In a similar vein, we can provide improved tools and processing capabilities to the policy auditor, to augment his expertise.

1. **Preliminary Questionnaire** - A process step of discovery, that yielded a fairly complete list of participants and documents, would have greatly compacted the time involved in the data collection phase. I believe that the survey method, with questions suitably framed, could accomplish this.

2. **Process Improvements** - Use a workshop type face to face meeting of the participants. In addition to meeting the audit goals this would be an opportunity for security education and consensus building for the company, and valuable feedback for improving the interview question set. A survey method only captures what people are willing to write down and misses the synergy of a team working together on a common problem. This idea is reminiscent of the case study in the Time Based Security (TBS) section of the SANS Audit track (ref: Marchany- SANS Audit Track 7.1) . The TBS committee did not go beyond the scope of the IS assets, however a full 17799 review in a real world company, would need to expand this scope to include whatever departments were responsible for the various domains or sub-domains (for example, HR and Legal).

3. **Interview Questions** - Bring experts together to formulate, test, refine and standardize the interview set. Experience should improve the interview set in any case, but a pooling of expertise to refine the set could conceivably get to a better place, faster. At the national level it should be possible to deliver a certification process, as some other countries have done. (e.g. Sweden, UK). Some countries like Japan are taking this a step further and requesting that 17799 type requirements be included in the Common Criteria (ISO 15408 reference) which is a mutual recognition pact between many countries to recognize each others validation bodies for IT security evaluation. So far the Common Criteria has primarily

dealt with product and system level issues. The Common Criteria has spawned industry consortia to produce things like the Security Policy for the Trusted Computing Platform. (reference)

4. **Tools- Web-Based policy audit application - Interview Set**- The Cobra tool (reference) was clearly a step in the right direction. A web based application should be developed and deployed on an intranet. It should have separate text-based components that are easily customized for local language and supersets of ISO and national requirements. I expect to see both Open Source and proprietary implementations that differentiate on quality of ISO interpretation, national extensions and 'leadership" extensions based on proposed or de-jure or emerging policy practices.

5. **Tools- Web-Based policy audit application - Back-End Processing** - The Cobra tool provided a percentage Non-Compliance scoring in the standalone application. This was provided at the top level domain. Expressed in this way, the larger score can be interpreted as a risk factor in that domain, which is a perfectly reasonable assertion. Back-end processing for a web application could easily provide a similar function. Furthermore, it should be straightforward to provide additional scoring granularity, for example a score for "Compliance with legal requirements" which accounts for 22 of 30 questions in the Compliance domain.

6. **Database aggregates and trend analysis-** various aggregation projects across the internet have shown the value of getting a larger view of the data, for example to have a view of Internet threats which spans multiple companies and countries, or a view by industry type (for example, the Internet Storm Center). If these data could be saved in an anonymous fashion, and with various spanning views in mind, similar utility might accrue to people principally responsible for developing and maintaining policy. For example, having received a score, representing some risk in a given domain, it might be useful to compare score in a given domain for my industry, so that I can appropriately prioritize my investments in this years budget.

7. **Help System** - in addition to the cross-reference to the applicable section in the standard, an indexed help system for clarification as to the meaning of questions and highlighted terms linked to a glossary.

8. **Risk Weighting** - One refinement which might improve utility for internal use in a company, would be to provide an weighting factor, to represent the importance that the company places on the topic. Some of the elements in the standard appear written for mainframe environments (for example a section on terminals), I received some survey feedback along these lines. Other elements may be somewhat esoteric in a smaller company (for example a section on protecting audit tools). A weighting factor would be a way of expressing that this section is to be considered but is low risk in our environment. Of course, this defeats the purpose of having standards in the first place, and such matters can always be taken into consideration when using result data, so the implementation of such a feature would need to be carefully considered.

4.0 References

1. ANSI Webstore - one place to obtain the ISO 17799 Standard
   http://webstore.ansi.org
2. SANS GSNA curriculum
   http://www.sans.org/
3. The Center for Internet Security
   http://www.cisecurity.com
4. RFC2196 - Site Security Handbook
   http://www.ietf.org/rfc/rfc2196.txt
5. RFC2828 - Internet Security Glossary
   http://www.ietf.org/rfc/rfc2828.txt
6. Toward Standardization of Information Security: BS 7799 Timothy Stacey September 22, 2000 http://www.sans.org/infosecFAQ/policy/standardization.htm
7. Model Security Policies, Michele Crabb-Guel
   http://www.sans.org/newlook/resources/policies/policies.htm
8. Security and Complexity - Bruce Schneier presentation
   http://www.counterpane.com/complexity-presentation.pdf
9. Secrets and Lies : Digital Security in a Networked World by Bruce Schneier
   Secrets and Lies @amazon
10. Information Security Policies Made Easy by Charles Cresson Wood
    http://www.pentasafe.com
11. Understanding Cyber Attacks by Kevin Mandia - Foundstone
    (presentation to ISSA-New England)
12. How to Check Compliance with your Security Policy by Krishni Naidu
    http://www.sans.org/infosecFAQ/policy/compliance.htm
13. Risk Associates - COBRA tool
    http://www.securityauditor.net/
14. NIST Common Criteria - evaluation and validation scheme (ISO 15408)
    http://niap.nist.gov/cc-scheme/ also http://www.commoncriteria.org/
15. Trusted Computing Platform Alliance, or TCPA
    http://www.trustedpc.org/home/home.htm

5.0 Attachments

Interview Questions ISO17799 Sec 12: Compliance domain

Developer Note: Change Form Action tag to point to your scripts area where interview.pl is copied

Perl CGI Script - Interview.pl

Developer Note: Copy to your web scripts area

Combined Results Page

Perl Script - getscore.pl

Developer Note: run locally to score results.txt (requires Perl)

ISO 17799:12: Compliance-Audit Report

Revised: July 18, 2001