Making compliance simple - not

Reading my email, I sometimes get a laugh just because of the juxtaposition of two subject headings. I just say these two next to each other:

Making Compliance Simple
[ISO 27001] Regarding Asset Classification

The “Making Compliance Simple” advertisement was for a free 1-hour Web-based seminar covering “7 elements of a compliance plan, auditing and monitoring, policies and procedures, education and training, and corrective actions”. That's an average of about 1 minute per element of the compliance plan, 5 minutes to cover auditing, 5 minutes for policies, ... you get the idea. About enough time to explain what a procedure is. Nothing like enough time to even state the requirements of one set of standards with regard to any of these topics.

The “Regarding Asset Classification” discussion was part of a discussion thread associated with ISO 27001 (Information Security Management System) certification in which they were discussing how an oscilloscope used to test out parts of operational information processing systems should be classified as an asset in terms of its potential implications for integrity and availability. This may seem like a trivial detail, but I think it is more meaningful in terms of understanding the nature of compliance than the 1-hour Web-based seminar.

Why did I laugh at this juxtaposition? Because the Web-based seminar seemed to me to be ridiculous and the asset classification discussion seemed to me to be the proof of its foolishness. At the same time, the discussion of the classification of an oscilloscope seemed funny to me because of the trivial nature of the discussion and the difficulty people were having with it compared to the magnitude of a real compliance effort for a major enterprise. If people spend that much time on an oscilloscope, the multi-billion dollar enterprises with tens of thousands employees that I deal with will end up spending millions of hours each year in nearly meaningless trivia in order to meet perceived compliance needs. But if people think that they can simplify their compliance efforts by listening to a 1-hour Web-based seminar, they almost certainly know so little about compliance that it will be a very long time before they are able to comply with any meaningful standard.

Anyone who has ever tried to implement compliance with any real standard knows that it is not simple, and yet it cannot, for any substantial organization, involve details at the level of substantial discussions on how to classify each piece of hardware or each file in each system. Compliance with most standards requires a team effort that reaches from the highest levels of organization involved (usually the CEO or Board) to the lowest level workers who are using the end results of the compliant components. But the effort has to be reasonably constrained so that compliance doesn't defeat its business purpose.

There are two different types of compliance requirements; mandatory and optional. If the law mandates compliance with some standard, you have the choice of breaking the law or meeting the minimum requirements of that standard necessary to pass the minimum audit you can get away with. Optional standards have to have business justification beyond the legally mandated duty to protect, and this justification sets the level of resources and thus the level of detail applied. Compliance for the sake of compliance is a fools errand.

In making the business decision to comply with an optional standard such as ISO 27001, many companies evaluate many different factors. Figure 1 is the evaluation done by one company in making an initial decision to move toward ISO 27001 compliance. In these diagrams, favorability is toward the right and importance is toward the top. The numbers show the "weight" of the combined importance and favorability while the shading indicates traffic light colors for each of the factors in the decision.

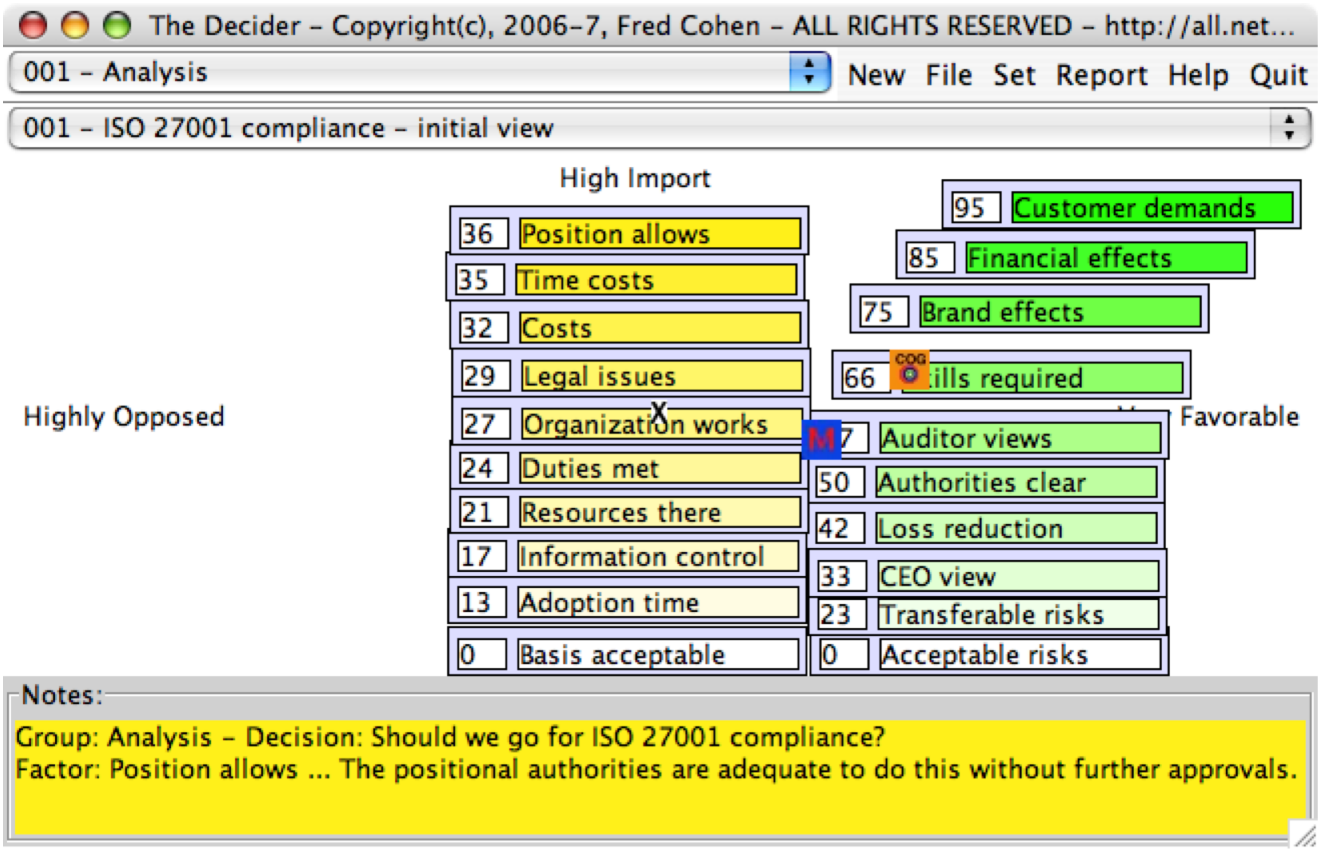

Figure 1: An initial review of a decision to support ISO 27001 compliance

In the beginning most projects are viewed in a positive light and presented in a positive way, or they don't ever get off the ground. But over time, things become far more clear. And with issues of compliance to optional standards, these changes are often substantial.

But the complexities of compliance are often far greater than initially contemplated by those with the vision to try to get them implemented. While many mature companies have little real difficulty with meeting standards such as ISO 27001, this is most often the result of many years of effort to meet other standards such as ISO 9000 and engineering practices associated with regulatory mandates such as building codes. Less mature companies often mistakenly think that they can do anything a mature company can do just because they have grown to the same financial sales levels. But higher sales do not translate into mature security organizations. Almost all companies that experience rapid growth in sales do not simultaneously develop the internal stability and engineering approaches that are required to meet quality standards. And effective information protection is largely about taking a quality engineering approach to implementing and operating information technology. As the reality of

what it takes to meet such standards starts to hit home and executive management finds out what's involved, things often change.

Req Pln Do Chk Act Doc	4.3.2d The procedure defines the management actions needed to ensure that relevant versions of applicable documents are available at points of use.	EDMS and Sharepoint (specifically document that this is done in the ISMS docs)
Req Pln Do Chk Act Doc	4.3.2e The procedure defines the management actions needed to ensure that documents remain legible and readily identifiable.	All labeled and all online. No procedure to keep old formats up to date or aasure SW available to read old formats.
Req Pln Do Chk Act Doc	4.3.2f The procedure defines the management actions needed to ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification.	Monthly readiness check, policy on treatment of information in storage and transif based on sensitify (information sensitivity level policy), Expiration dates and review prior to re-availability, record retention and disposal (USP-4) - DON'T KNOW

Figure 2: Some elements of a ISO 27001 compliance review

A good example of the sorts of things that are required for such compliance is given in the above analysis of one part of one business unit within a larger enterprise where they are seeking ISO 27001 certification. ISO 27001 requires a "plan, do, check, act" approach and documentation of everything undertaken. In this case, the requirement level is used to indicate whether the enterprise currently requires this function to be performed. The middle entry is an example where something is required and partially planned, done, checked, acted upon, and documented. But clearly additional changes are required to meet the standard. To become compliant, this and hundreds of other similar things must be done. Is it worth the commitment?

042 - ISMS-A.13 Incident Management	0/0= N/A	0/0= N/A	28/28=100%	28/28=100%
043 - ISMS-A.14 Business Continuity Management	0/0= N/A	3/12=25%	0/0= N/A	3/12=25%
044 - ISMS-A.15 Compliance	0/0= N/A	0/0= N/A	44/44=100%	44/44=100%
045 - ISMS-B (informative) OECD Principles	0/0= N/A	0/0= N/A	44/44=100%	44/44=100%
Overall Total	0/20=0%	95/768=12 %	803/852=94 %	898/1640=54 %

Figure 3: The last part of an ISO 27001 compliance review roll-up

This example is from a mature company that has a lot of regulatory mandates and is already compliant with many other standards in the non-security domain, but is seeking ISO 27001 compliance. They have already adopted ISO 27002 (formerly ISO 17799:2005) and it is largely implemented within this part of this organization. But as the summary makes clear, they still have quite a way to go to get certified for ISO 27001. Will they follow through and accomplish this task for this part of this enterprise? How long will it take?

I cannot answer these questions for them. They will answer them over the next year as they work toward compliance or decide not to do so. The question they have to ask themselves is what the business justification is for meeting this standard. They did so before starting the effort, just as the other company whose initial decision was shown in Figure 1 above did. And they are likely evaluating that decision again as they look at the level of effort required and put it in context of their initial expectations with regard to the business case for gaining certification. At least 4 management levels will be involved in the continuing decision with regard to compliance as they were in the initial decision to work toward compliance almost 6

months ago.

This brings us back to the initial decision made by the company from Figure 1 above. They spent about $125K plus about one person month of internal effort to start down the path of compliance with elements of ISO 27001 and 27002 before getting a clear view on what it would take to continue down this path. Figure 4 shows how the same factors that appeared so favorable in Figure 1 changes with a bit of exploration.

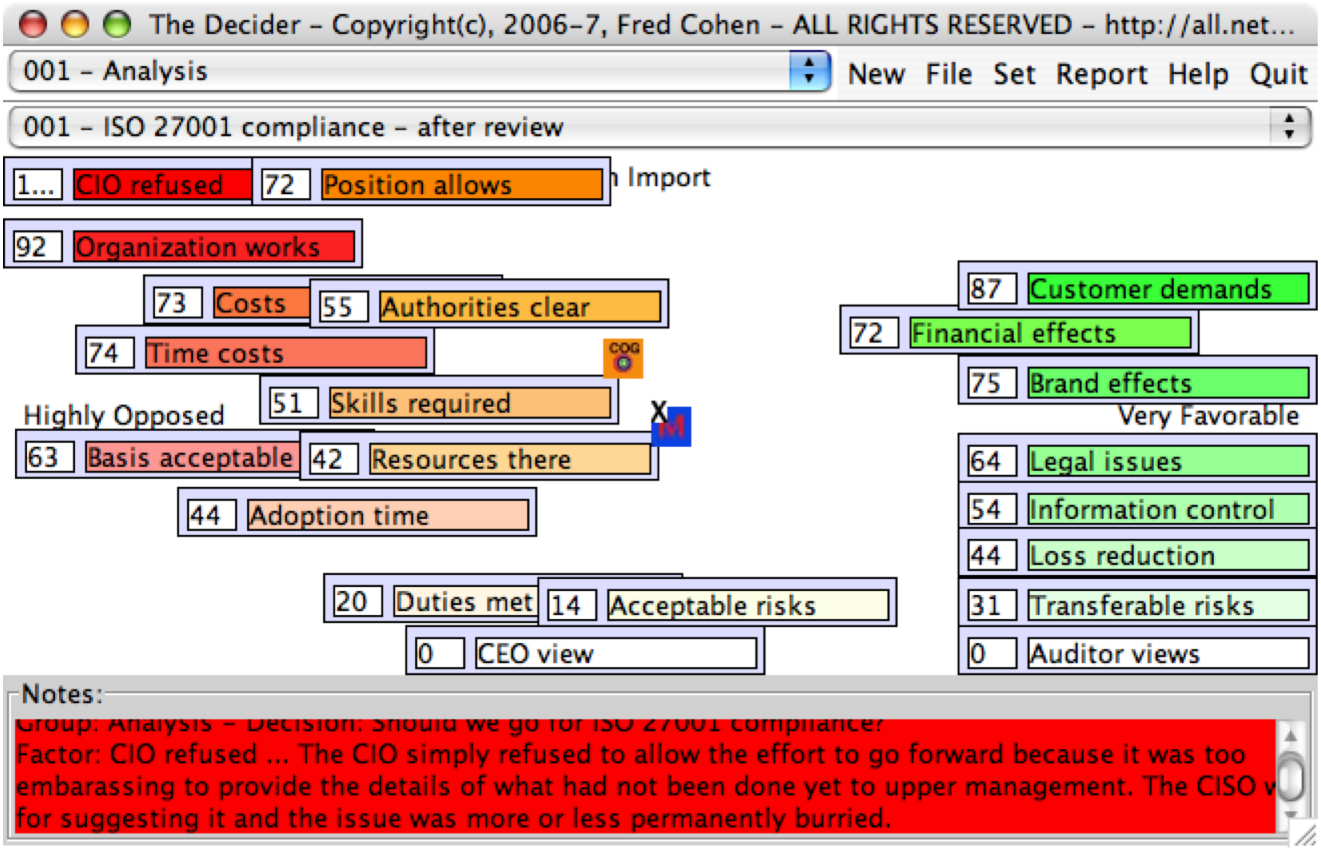

Figure 4: The decision on ISO 27001 compliance after an initial internal review

After the initial review, views of priorities changed substantially. The CIO stepped into the process and made a unilateral decision to stop the process for internal political reasons. The CISO was fired for trying to get this project going, the initial cost and effort estimates made by the directors of different groups were found to be far off base (not the CISO's fault in this case), the business basis for compliance was altered, the effects in business were summarily downgraded, and the project was buried along with the initial reasons for its creation.

At the end of the day, decisions about compliance with non-mandatory standards are not simple, and compliance with almost any meaningful standard is far from simple. At the same time, the minutia of standards definitions and the details of how to do the things involved in the implementation of standards almost never prevent their implementation. These are complex businesses decisions made in the changing context of organizational politics, the business environment, under financial and human constraints, and are subject to all of the human limitations and changes over time of other substantial business decisions. To expect anything different or promote any other expectation is a great mistake.

