Achieving policy, regulatory and standards conformity
through implementing an
ISO/IEC 27001
Information Security Management System
(white paper)

v4.0.0 2006-09-14

DISCLAIMER

the Zygma partnership LLC has applied its best endeavours in the preparation of this paper which it freely distributes for public edification but accepts no liability arising from its use or application by any other parties, howsoever arising. The analysis, whilst undertaken diligently and in good faith, may contain oversights or omissions, and in any event is subjective and performed in a general context, without regard to the needs of any specific entity or party. Those who choose to act upon any statements or claims presented in this paper do so as a result of their own freely-exercised choice and judgement and entirely at their own risk.

Zygma regrets that it has to state a disclaimer but, sadly, it's a pretty litigious society these days, so one does the risk analysis and works out one's risk treatment plans (ISO/IEC 27001:2005 §4.2.1 d), e), f), g)).

CONTENTS

1. Introduction

This paper is a revision to an earlier version of the paper published under the same name. This version has been extended to include a generic process model for the mapping between the ISO/IEC 27001 requirements and controls and another reference source, be it some regulation, a contractual requirement, an externally-imposed policy, another standard or any other applicable reference.[1]

By extending the scope of the paper we hope to better assist those organizations choosing to implement an ISMS which may find themselves asking the question "*How can I implement the ISMS standard if I also have to conform to 'xxx'?*", i.e. to some additional reference. This paper provides an approach which allows resolution of that question using the ISMS as the controlling management system for that additional conformity.

Both ISO/IEC 27001and ISO/IEC 27002 recognise the potential need to add additional controls, and encourage implementers to do so when the situation so requires.

This paper describes a rigorous Conformity-mapping model which takes into account the specific legal, regulatory and policy requirements and other chosen standards[2] against which an organisation may have to, or may wish to, show their compliance / conformity.

After an initial view at a high level of abstraction the paper then describes a detail mapping process for performing a mapping exercise between a selected source and the reference set of controls provided in ISO/IEC 27001 Annex A. This offers some options when implementing the process. The mapping process is exemplified by using representative clauses from a generalised regulatory reference source.

The process considers, a four-layer model which maps, or channels, the organization's goal conformity-requirements into the overall ISMS model. In doing so the owner organization could build into their ISMS the specific controls and review processes necessary to achieve and to be able to demonstrate their required observance. The final specific controls would be expressed in the organisation's Statement of Applicability (SoA) which would refer to the controls set out in Annex A of ISO/IEC 27001 and include such additional controls as necessary to provide a wholistic ISMS.

2. Definitions

The concepts put forth in this paper require the use of a few special terms not, at the time of publication, found within the ISO/IEC ISMS standards. The following definitions describe those terms also extend one term from the standards. The definitions are given in dependency order, i.e. a term is defined prior to its use in another definition, rather than being presented in alphabetic order – this style allows the definitions to be read in a 'tutorial' manner.

Reference Controls List (RCL): The control objectives and controls set out in ISO/IEC 27001 Annex A.

Extended Controls Set (ECS): A set of information security controls which are complementary to those in the RCL.

Such controls are derived in response to the requirements of a specified reference source after analysis against the controls and associated implementation guidance of ISO/IEC 17799 has indicated that the RCL

[1] It is usual, in standardization circles, to refer to 'compliance' when the subject entity has no choice in their need to observe a particular set of requirements, e.g. applicable legislation with which compliance is mandatory, and 'conformity' when the observance is self-determined, e.g. in choosing to conform to a technical standard. In this document we use 'conformity' to cover both compliance and conformity.

[2] Such 'standards and specific legislation and regulation' are hereafter referred-to collectively as 'references', a term intended also to cover any other specified requirements which a business aims to include within the scope of its ISMS as a definition of how some process is performed, defined, etc.

controls are insufficient to fulfil the requirements of the cited reference source (we make the distinction here between 27001 and 17799(27002) because the controls in 27001 Annex A are a requirement, whereas 17799 provides guidance intheir selection and application).

An ECS should define only additional controls not contained in the RCL – there should be no redundancy, although reference may be usefully made to any RCL controls which are being explicitly extended.

Extended Controls List (ECL): A set of control objectives and controls based upon the **RCL** and extended by the inclusion of further controls from specific reference sources.

These sources would be those which an organisation is required or chooses to observe, stemming from legal, regulatory, or business requirements.

The additional controls would be derived either by explicit extraction from the sources or through inclusion of a previously established **ECS**.

Those controls within an **ECL** which are not within the **RCL** can be considered an **ECS** for the specific set of specific reference sources.

Statement of Applicability (SoA)[3]: *documented statement describing the control objectives and controls that are relevant And applicable to an organization's ISMS* [27001], derived from an **ECL** as a result of a risk analysis.

3. Background to ISO information security management system series

At the time of this paper's publication there are two published standards in this family: ISO/IEC 27001:2005 "Technology – Security techniques –Information security management requirements", and ISO/IEC 17799:2005 "Information Technology – Security techniques – Code of practice for information security management". Other standards are being drafted and will support the ISMS model as defined by ISO/IEC 27001.

In the USA, the ANSI-ASQ National Accreditation Board[4] (ANAB) has established an ISMS accreditation scheme which will grant accreditation to those US bodies recognized as being competent to perform the requisite formal ISMS audits.

The full texts of these ISO standards are available from standards bodies – suggested sources in the U.S. are the American National Standards Institute[5], the International Standards Organization (ISO)[6] or BSI Americas[7], in the UK the British Standards Institute[8].

4. Conformity-mapping process

4.1. The four-layer viewpoint

The principle behind this model considers four layers, defined thus:

Layer 1: ISO/IEC 27001, normative ISMS requirements (ISMS-L1):

Formal requirements for the implementation, operation and management of the ISMS, including the risk management process and the provision of a **Statement of Applicability** which relates to the **Reference Controls List (RCL)** in Annex A of 27001.

Layer 2: ISO/IEC 27002, informative ISMS code of practice (ISMS-L2):

[3] non-italicised text added to the 27001 definition for the purposes of putting into a context appropriate for this paper.

[4] see http://www.anab.org/

[5] see http://webstore.ansi.org/ansidocstore

[6] See http://www.iso.org/iso/en/prods-services/ISOstore/store.html

[7] see http://www.bsitraining.com/infosecurity_standards.asp

[8] see http://www.bsonline.bsi-global.com/

Generic controls with implementation guidance, having a one-one relationship with the **RCL** in ISO/IEC 27001 Annex A.

Layer 3: Reference documents to which conformity is required (ISMS-L3):

Existing policies, legislation, regulation, contracts, international agreements, standards, &c. to which compliance/conformity is required, either by direct imposition (e.g. as laws, corporate policies) or through agreement (e.g. contract, choice of standards).

Layer 4: baseline operational security controls (ISMS-L4):

Controls which are either implemented in order to conform to a standard requiring them or are determined to be required through the organization's own risk analysis or requirements. Baseline controls may also be those directly required by a specific standard.

The focus of this process is therefore on the relationship between the implied controls determined by the conformity requirements of the references which populate the ISMS-L3 and the specific controls implemented in ISMS-L4 and their relationship to the **RCL** of ISMS-L1 (i.e. to the required ISO/IEC 27001 **SoA**).

4.1.1. Analytic approach

Based upon ISO/IEC 27001, an organization implementing an ISMS must prepare a **Statement of Applicability** (**SoA** – ref. ISO/IEC 27001 §4.2.1.j), §4.3.1.i)). The **SoA** must, as a minimum, show how all of the controls listed in the **RCL** have either been implemented or justifiably excluded from implementation, based upon the scoping of the ISMS and the outcome of the risk analysis performed in conformity to ISO/IEC 27001.

It is therefore appropriate that the controls identified in and/or required by other policies, legislation, regulation and other standards etc. should be identified for completeness and sufficiency (where the implementer has any discretion in their application) before the risk analysis draws from them to establish the required **SoA**. This process involves collating controls from all applicable sources into an interim list which we will call the **Extended Control List (ECL)**. This serves two purposes: firstly, to provide the basis of a conformity mapping which can be used to demonstrate conformity against these other references and secondly, to provide a check that the ISMS controls identified through following ISO/IEC 27001 and defined in ISO/IEC 27002 (the latter providing interpretive guidance on their intended scope) are indeed sufficient in their defined scope or whether additional controls need to be stated and/or if additional implementation guidance need be given.

The analytic approach to generating the **ECL** performs an analysis through a number of stages.

The first step in this process is to identify those references which will form the basis for the **ECL**. These references will be those against which the organization wishes to be able to show conformity through their ISMS. However, it may be that in practice certain references are simply taken at face-value and associated controls are identified as appropriate for inclusion within the ISMS, such as may be the case with adherence to an overall corporate policy or to a standard which mandates certain controls.

The control objectives and controls derived from those references should be used to extend the **RCL**, thus creating the initial **ECL**. This should include all controls, including those which are required by the references which are to be taken at face value (Figure 1).

In order to eliminate unwarranted duplication it is then necessary to assess each of the requirements, for each identified reference, against each of the ISMS controls defined in ISMS-1.

In preparing such a mapping, the analysis should give consideration to the extent to which a particular control from the **RCL** satisfies the requirements of the referenced source. In doing this, interpretive guidance from ISMS-L2

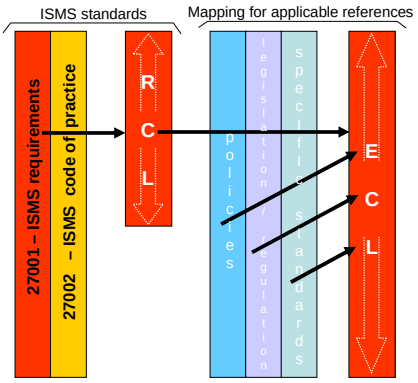

Figure Fig 1. creating the initial Extended Control List

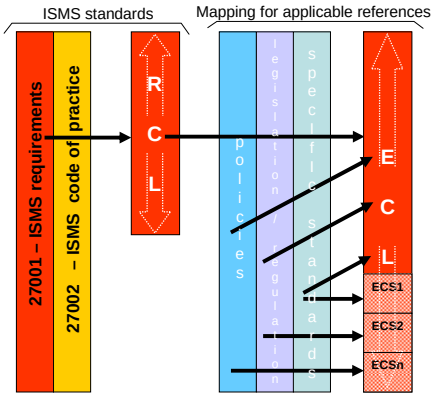

Figure 2. completing the Extended Control List

should be taken into account, as should be any guidance provided in the reference source.

If in the conduct of the analysis there are instances where the defined ISO/IEC 27002 implementation guidance does not adequately provide for the specific requirements of the referenced documents it is necessary to define a specific control for the express purposes of being able to show clearly conformity to the requirements of that referenced source.

At the end of this process the **ECL** will contain a full set of optimized controls which, according to their origins and how the contents have been collated, could possess varying degrees of duplicated control objectives and controls (Figure 2).

Note that it is not the intention to propose that a formalized process be necessarily undertaken in each case; rather that, where an organization wishes to be able to explicitly demonstrate its conformity to any specific reference, that there is a suitable analysis undertaken to identify the applicable controls and thus provide the needed traceability.

It is extremely unlikely that the analysis of each reference source will reveal a neat one-one mapping, for a variety of reasons. The preparation of this analysis requires thought and consideration. For example, we may find that we are comparing a piece of legislation and its associated regulations with a standard: the analysis must recognise that the documents are written for different purposes and from different viewpoints. It is also quite likely that an ISMS control may be an effective measure for more than one requirement within a reference source and, conversely, that a reference requirement may find more than one ISMS control which can fulfil it. In practice a single implemented instance of a control may satisfy more than one need for both the reference and the ISMS standards. Practitioners should not, therefore, be disappointed to find that a simple one-to-one mapping cannot be achieved.

As a consequence of this implementers may develop an **Extended Control Set (ECS)** which relates explicitly to a specific reference source and has the potential for re-use, or may use an **ECS** from other sources. Each **ECS** should be used to supplement their **ECL**. In practice, the requirements of the implementing organization may also require extended controls to be defined.

As a final step in this analytic process, the specific controls implemented by the ISMS-owning organization require selection according to a risk analysis which takes into account the needs of the referenced sources and of course of the organization within the scope). These controls can then be mapped to the referenced sources and the final **SoA** identified (now considered also to include the **ECS**).

At this stage justification needs to be made if controls from the **ECL** are to be included within the ISMS or not, or if only one control is selected from a set of similar controls.

It should be kept in mind that this process is focusing on how to use an ISMS to support an organization in fulfilling its required conformity goals. It does not try to resolve how the organization performs its risk assessment and develops risk treatment plans which implement specific measures to fulfill the needs of ISO/IEC 27001 Annex A. Nevertheless, the final ISMS will need to relate, through its **SoA**, how the organization's specific measures do indeed fulfil the requirements of both ISO/IEC 27001 and other target references (Figure 3).

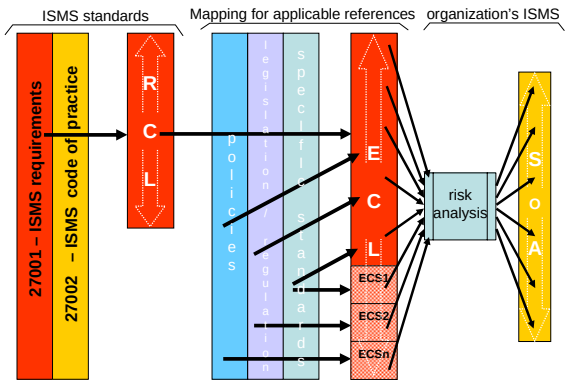

Figure 3. deriving the organization's SoA

This analytic method explains the approach from a somewhat idealist perspective. Reality may dictate otherwise, and another viewpoint should be considered.

4.2. Mapping process

The mapping process is described as number of discrete steps. Implementers should adopt them to their own circumstances in terms of the level of rigour and complexity demanded by their situation. In part, there is a risk judgement to be applied – greater detail will naturally take more time but will reveal greater understanding, which could be crucial to managing the risks. If the ISMS is being used to show conformity with a number of other reference sources then there may be controls already applied for some of them which might suit others, even if the RCL does not readily accommodate them.

4.2.1. Mapping goals

The goals of the mapping are three-fold:

i) to establish the relationship between the two documents;

ii) to determine the extent to which the ISMS controls are able to satisfy the requirements of the referenced source, and;

iii) to determine where additional controls are required to compensate for a lack of a suitable ISMS control or to strengthen existing ISMS controls.

The process to achieve fulfillment of these goals is now described.

4.2.2. Types of documents

In performing a comparative mapping between a specific reference source and the ISMS controls it is important to recognize that the mapping may not be between two documents of a common type, i.e. between documents having the same scope and intent in their usage. For example, the selected reference may be a national regulatory statement as to what organizations in a specific market sector must do in order to remain compliant with those sector-specific regulations; ISO/IEC 27001 is an international standard with required management processes supported by a code of practice (ISO/IEC 27002), related to a set of controls which have generic application, that application depending upon the scoping and requirements of an over-riding policy and business goals.

Thus, at a simplistic level, the comparison would be between a specific and a generic document; between a regulation (compliance with which is probably a legal obligation if operating in the sector which the legislation covers) and a standard (compliance with which is the exercise of choice). An inspection of the legislative impositions and the RCL will show that the former has a set of clauses which state how that document is to be interpreted, which entities are subject to it and what the subject entities are required to do.

Sometimes required actions for the demonstration of compliance may be given. Frequently they are not –legislation often sets the rules and those subject to it have to work out what they must do to achieve compliance, and possibly to justify at a later date. Other standards may be more like the ISMS standards, having normative and informative parts and using similar language, yet may still not have a defined process for demonstrating conformity.

Thus, the implementer needs to be aware of the possible different purposes and structures of the documents being mapped and to keep that in mind when interpreting the respective documents during the mapping.

A consequence of this is that the mapping may need to be done between the reference source and both or either of 27001 and 27002, depending on the nature of its requirements and the extent to which they may focus on process (27001) and/or specific controls (27001 Annex A).

4.2.3. Mapping the relationships

It is valuable to arrive at the conclusion of the mapping with a two-way correspondance between the RCL and the reference source, i.e. for each control/requirement in the reference source, list all of the ISMS controls which relate to it and for each ISMS control list each of the reference source controls/requirements to which it contributes. This two-way mapping will be valuable whenever a control or the control requirement changes and the corresponding controls need assessment to ensure that the conformity is maintained. The mapping will support both management review, internal audit and the production of evidence of effective management control when the ISMS is subjected to external assessment.

Which of these two mappings is chosen to be the driver for the mapping process does not really matter, technically. However, since the ISMS controls will be the common element when more than one other reference source is mapped, and furthermore the information security management system will be the basis for embracing the other reference source(s), it is strongly recommended that the ISMS controls are taken as the fixed basis for the mapping, i.e. the reference source is mapped *into* the ISMS.

Tables 1 & 2 (all tables are located at the end of the paper) suggest headings for tables which may be used as the basis for recording the results of the mapping. In those tables «RefSrc» refers to the chosen reference source which is being mapped into the ISMS standard(s). These tables provide the basis of a simple cross-mapping: for the sake of these examples mapping against only 27002 is assumed.

How the mapping process should proceed is now explained by using an example. Each clause or discrete requirement / criterion in «RefSrc» is compared against the ISMS controls. Although, with 133 controls against which to compare, this may sound daunting, knowledge of the ISMS controls will help focus, often to within a single group of controls. Note that it is usual to find a one-to-many mapping, so a number of ISMS controls may be relevant.

As an example, the ISMS control (A)14.1.2 “Business continuity and risk assessment” could relate to, e.g., three separate controls in «RefSrc» which relate to having a data back-up plan, having a disaster recovery plan and performing a criticality analysis of applications and data.

Each time that a control mapping is found the «RefSrc» clause identity should be entered into a table such as that shown in Table 1, against the ISMS control, and similarly in a table resembling Table 2, the ISMS control identity should be recorded against the «RefSrc» clause. Ideally, these should be hyper-linked to make easier the processes of cross-checking, implementation and audit/assessment.

Following from the example above, as the mapping progresses, the «RefSrc» requirement for having a disaster recovery plan may (and in practice, probably will) map into ISMS controls 14.1.1 to 14.1.5 inclusive.

Thus, in use, we may find Table 1 developing content which looks like that shown in Table 3.

In the Table 3 example, the text in the 'commentary/observations' column is exemplar, indicating the kinds of analysis that might be derived.

Table 4 gives examples of entries which complement those in Table 3. Note that against the second «RefSrc» clause there is an ISMS control outside of the §14 group which has been mapped. Implementers should be aware that it might not be uncommon to find that a clause in the reference source has a relationship across a number of ISMS control groups. This generally arises because of the different scope, structure and ordering of requirements between the two documents.

4.2.4. Determining ISMS control adequacy

Table 1 includes a column titled "Comparative coverage: 27002 cf. «RefSrc»". This column should be used to indicate the extent to which the ISMS controls can adequately fulfill the requirements of each discrete reference source clause or criterion. This of requires the implementor to establish that, at least in principle, there is an intention to address the same topic between the two documents. There are a number of ways in which that can be done – two are suggested:

One approach is to take a continuum of values and rate accordingly, e.g. 0 – 4. This could be expressed either numerically or graphically, and might use thresholds such as:

□□□□	the ISMS control has ***significant shortcomings*** in its ability to address the scope of the reference source's requirements;
■□□□	the ISMS control ***does not fully address*** the scope of the reference source's requirements;
■■□□	the ISMS control is ***equivalent*** in scope to the reference source's requirements (note – 'equivalent' does not necessarily mean 'equal to' or 'the same as');
■■■□	the ISMS control provides ***additional guidance*** which would assist demonstrating compliance with the reference source;
■■■■	the ISMS control provides ***substantial additional guidance*** which would significantly assist demonstrating compliance with the reference source.

Whilst this approach may give greater insight into the comparative value of each ISMS control, it doesn't immediately resolve the major questions – does the ISMS control apply at all, will it be sufficient and if not, what has to be done?!

Therefore another approach might be to apply one of the following qualifiers against each mapping:

OK	the ISMS control is **sufficient** to address the reference source requirement;
Partial	the ISMS control is relevant but **does not fully** address the reference source requirement;
No	the ISMS control **does not** address the reference source requirement although headings / titling / etc. used in the respective documents suggest that they are addressing a similar concept.

The benefit of this approach is that it is more immediately obvious where additional controls need to be defined.

It should be understood that the mapping has to be conducted with a 'comparative' judgment as to how the implementation of an ISMS based upon the control definitions and implementation guidance in 27002, having regard to the language and description of those controls, would enable the implementor to demonstrate that its conformity against the reference source was being adequately accomplished. That this is to some degree a subjective process is recognized – but then so is information security! This process can be compared to the process of performing a risk assessment (which in kind this mapping is), where an informed

decision is made as to the acceptability or otherwise of residual risk.

The mapping process defined above has so far identified an initial mapping. At the conclusion of this first parse of the reference source there will possibly be some requirements of that document which have not been addressed at all (by an ISMS control).

It would be prudent to cross-check the mapping, and more specifically to verify whether any un-mapped controls (in either document) may in fact be mappable. Using additional resources to do this, which have not been involved in the first parse mapping, will usually be beneficial.

In many cases the lack of a mapping against an ISMS control can be justified on the basis of 'no direct relationship' (to the reference source's requirements) and can be marked as 'not applicable'. This mapping attribute needs to be explicitly stated, so as not to lead to a later uncertainty as to whether the control was checked during the mapping.

'***n/a***' should therefore be added to both the above-defined suggestions for recording the comparative mapping results.

Three important points should now be made. Firstly, it is unlikely that, and it should not be the goal that, each control within the ISMS is mapped to at least one of the reference source's requirements and vice-versa. The broad applicability intended for ISO/IEC 27001 and the more likely narrower focus of the reference source intuitively suggest that a complete mapping is unlikely to exist. Therefore, un-mapped ISMS controls should be anticipated.

Secondly, the fact that there is no mapping to an ISMS control is not a suggestion that that control would have no place in the overall ISMS being implemented – only that it would have an indirect relationship to the specific reference source clauses.

Lastly, the failure to find an ISMS control which satisfies one or more of the reference source's requirements (i.e. where the adequacy mapping is determined to be '***Partial***' or '***No***') should not be seen as a weakness in the ISMS model – it actually points to where an obscurely-stated strength of the ISMS model should now be turned to the advantage of the implementor: define additional controls as required and include them within the overall framework of their ISMS.

4.2.5. Extended Control Sets

ISO/IEC 27001 §4.2.1 (g) states: "*The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected*." Where the reference source's requirements have not been satisfied in whole or part it is now appropriate to define additional objectives and controls, which can be placed into an Extended Control Set (ECS). This ensures that the controls implemented within the final ISMS allow the demonstration of full conformity with the reference source's requirements.

The ECS can be constructed in a number of ways –simply built into the operational procedures and processes, listed in a tabular form to record collectively the additional controls or constructed as a more formalized set of control objectives and controls with implementation guidance in a form which mimics that used in ISO/IEC 27001 Annex A. Table 5 provides an exemplary ECS in this format. Note that in the Table 5 example the individual controls are given discrete clause references so that they may be addressed within the ISMS in the same way that the SoA would address the ISMS RCL.

To complete the mapping, the new controls should be mapped into the table based upon the reference source requirements, which will now record both the matching ISMS controls and the specific ECS controls. Within the context of the ISMS-owner's system, there will be a complete mapping for the reference source.

A potential difficulty which may be encountered during the mapping process could be the introduction of control requirements from sources which may have no accommodation for one another, leading to conflict between their respective requirements. This is essentially a matter which must be resolved during the risk analysis process. Some basic observations can be made. Firstly, if it is possible to accommodate both requirements by partitioning

them through the introduction of additional controls then those controls should, if not already within the scope of the **ECL**, be added, eventually to become a fixture within the **SoA**. Alternatively, one control could be downgraded to limit the degree of conflict, or might be eliminated altogether. In making such a decision any vulnerability created (including a potential non-conformity against the reference source) should be carefully assessed and management must accept and defend the consequences. It also may be practical to obtain a waiver from any contracting party or authority imposing the requirement, following a reasoned argument as to the nature of the conflict and the consequences of reduction or elimination of the control.

Whatever the outcome in such a situation, the risk analysis and the **SoA** must record the decision and its effect upon policy and the implementation of controls.

4.2.6. Managing Extended Controls

How extended controls are managed within the context of a specific ISMS and in a wider context will depend on a number of issues which may include, *inter alia*, the following:

Is this a 'one-off' requirement? If so then recording the ECS locally may be sufficient. If not, what might be the other uses of it? The ECS could be 'packaged' and made available to other parties within the same organization, or within the sector or some other community of interest. There is the potential for, e.g., a library of full 'other reference'-to-ISMS mappings to be established as a kind of library, including the ECS. Issues of commercial confidentiality may come into play, which are not addressed here.

Is the mapping done purely for internal reasons? If so, the ECS could be simply appended to the SoA derived from the RCL, or even integrated within it where the RCL control groups cover the general area of the extended control.

Is there a need to show conformity to an external (or possible a specific internal) party? If so, a separate SoA might be constructed which contains all, and only, the controls required to show that conformity. The complete ISMS may therefore have two (or more if desired) SoAs allowing different specific conformities to be demonstrated. Between multiple SoAs there will most likely be a high degree of commonality: The ISMS must address all controls within its scope; each reference source-specific SoA will have its own (sub-)scope. Although this sounds potentially overwhelming, it is simply a way of extracting a set of controls from those making up the full ISMS implementation. Essentially, this can be accomplished by having a matrix which lists the full set of controls in one axis and the specific reference sources' use of controls in the other (the full ISMS can be excluded from the matrix since it ***is*** the full set).

4.2.7. ISMS scoping and operation

The ISMS certification process is most directly concerned with determining the conformity of the management system to the normative requirements of ISO/IEC 27001. However, where an organization wishes to use its ISMS to additionally indicate its conformity to other key references it would be wise to include such a claim within the scoping of its ISMS, thus requiring that the assessor looks explicitly for the evidence of that conformity within the ISMS.

Within the PDCA framework of the ISMS each of these ECS would be treated uniformly and consistently in terms of management, review, improvement etc. This will provide both informal and formal forms of evidence of best endeavours to attain conformity, a measure which may prove to be a useful defence in the case of any challenges to a claim of conformity.

Inclusion of evidence of conformity in this manner may eliminate the need for a separate conformity assessment, and will in any event

make more efficient the provision of evidence and the ongoing conformity oversight (through inclusion within the broader PDCA processes of the ISMS).

Apart from controls, some frameworks provide certain process requirements. It may be necessary to have an additional document showing how additional management processes or procedures supplement the ISO/IEC 27001 requirements.

5. Acknowledgements

This paper has been substantially enhanced and strengthened through contributions submitted by fellow INCITS CS1[9] members Fiona PATTINSON and Scott E. ERKONEN.

[9] INCITS/CS1 serves as the US National Body (NB)/Technical Advisory Group (TAG) for ISO/IEC JTC 1/SC 27 and all other SC 27 Working Groups. See: http://cs1.incits.org/.

6. Tables

Table 1 - headings for mapping against ISMS controls:

ISO/IEC 27002:2005 control	Matching «RefSrc» clause/section	Comparative coverage: 27002 cf. «RefSrc»	Commentary / Observations

Table 2 - headings for mapping against «RefSrc» controls:

«RefSrc» requirement	Matching ISO/IEC 27002:2005 implementation guidance	Commentary / Observations

Table 3 - content after mapping against ISMS controls:

ISO/IEC 27002:2005 control	Matching «RefSrc» clause/section	Comparative coverage: 27002 cf. «RefSrc»	Commentary / Observations
14 BUSINESS CONTINUITY MANAGEMENT	§ 101(a) *Contingency plan*		27002 devotes a whole section to this subject and provides detailed controls and guidance whereas the «RefSrcs»'s requirements are stated in a series of brief paragraphs. «RefSrcs» also only refers to incidents which 'damage systems', rather than considering the loss of information *per se*.
14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT			See subordinate 27002 clauses.
14.1.1 Including information security in the business continuity management process	§ 101(a)(ii) *Disaster recovery plan*		
	§ 101(a)(iv) *Applications and data criticality analysis*		
14.1.2 Business continuity and risk assessment	§ 101(a)(i) *Data backup plan*		
	§ 101(a)(ii) *Disaster recovery plan*		
	§ 101(a)(iv) *Applications and data criticality analysis*		
etc.			
14.1.5 Testing, maintaining and re-assessing business continuity plans	§ 101(a)(i) *Data backup plan*		
	§ 101(a)(ii) *Disaster recovery plan*		
	§ 101(a)(iii) *Emergency mode operation plan*		27002 has no explicit reference to an 'emergency mode', although it would be included within the general scope of item (c)(iii). Alternative wording for «RefSrc» recommended to be used in the 'SoA': "(iii) fallback procedures which describe the actions to be taken to: move essential business activities or support services**, and required off-site back-ups,** to alternative temporary locations **from where emergency mode operations can be run, and;** bring business processes back into operation within the required timescales." (bold indicates new text beyond that presently in 27002).
	§ 101(a)(iii) *Testing and revision procedures*		
	§ 101(a)(iii) *Contingency operations*		

Table 4 - content after mapping against «RefSrc» controls:

«RefSrc» requirement	Matching ISO/IEC 27002:2005 implementation guidance	Commentary / Observations
§ 101(a) *Contingency Plan*	**14 BUSINESS CONTINUITY MANAGEMENT**	
§ 101(a)(i) *Data backup plan*	*10.5.1 Information Back-up* *14.1.2 Business continuity and risk assessment* *14.1.3 Developing and implementing continuity plans including information security* *14.1.4 Business continuity planning framework* *14.1.5 Testing, maintaining and re-assessing business continuity plans*	
§ 101(a)(iii) *Emergency mode operation plan*	*14.1.3 Developing and implementing continuity plans including information security* *14.1.4 Business continuity planning framework* *14.1.5 Testing, maintaining and re-assessing business continuity plans*	

Table 5 - exemplar Extended Control Set

«RefSrc» clause/ section	Control objective	Control	Implementation guidance	Related «RefSrc»& ISO/IEC 27002:2005 clause(s)
«RefSrc».101 Administrative safeguards				
«RefSrc». 101.1	Emergency mode continuity planning	Within the single framework of business continuity plans there shall be described, with appropriate priority, procedures to ensure protection of electronic personal identifiable information while operating in emergency mode.	Business continuity plans should (ref. 27002 §14) should describe the approach to provide fallback procedures which enable an emergency mode continuity plan to be put into effect, which takes into account the following actions: a) move critical business processes, and required off-site back-ups, to alternative temporary locations from where emergency mode operations can be run, and; b) bring business processes back into operation within the required timescales. Other information These controls should be integrated with the overall access control used by the organization, as covered by 27001 A.14, in particular A.14.1.4.	§ 101(a)(iii) *Emergency mode operation plan* *14.1.4 Business continuity planning framework*
«RefSrc». 101.2	Testing, maintaining and re-assessing emergency mode plans	Business continuity plans for operating the business in emergency mode should be tested and updated regularly to ensure that they are up to date and effective.	Business continuity plan tests should ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security, including transfer to emergency mode, and know their role when a plan is invoked. The test schedule for business continuity plan(s) should indicate how and when each element of the emergency mode plan should be tested. Each element of the plan(s) should be tested frequently. Other information Techniques used in order to provide assurance that the plan(s) for switching to emergency mode will operate in real life should follow, and be integrated with, those described in 27001 A.14.1.5.	§ 101(a)(iii) *Emergency mode operation plan* *14.1.5 business continuity plans*

Table 6 - mapping content (in the form of Table 3) after creating the ECS:

«RefSrc» requirement	Matching ISO/IEC 27002:2005 implementation guidance	Commentary / Observations
§ 101(a)(iii) *Emergency mode operation plan*	*14.1.3 Developing and implementing continuity plans including information security* *14.1.4 Business continuity planning framework* *14.1.5 Testing, maintaining and re-assessing business continuity plans*	«RefSrc».101.1 «RefSrc».101.2

Digitally signed by Richard G. WILSHER
DN: cn=Richard G. WILSHER, c=US,
o=the Zygma partnership LLC, ou=CEO
Reason: Approved for public release
Date: 2006.10.20 02:02:28 Z