"Securing your business' information"

www.Zygma.biz

White Paper
A new approach to the purposes and application of ISO/IEC 27001 Annex A

2011-02-07

Eur.Ing. Richard G. Wilsher, BSc(Hons), FBCS, CITP, CGEIT

Abstract: This two-part paper sets forth a view as to how the identification and application of security controls and the relevance of Annex A of ISO/IEC 27001:2005 (IS27001) should be treated in the current revision of that standard. This new paradigm for Annex A draws on Zygma's own applied research over the past decade, discussions with peers in the field, debate during recent ISO JTC1 SC27 WG1 Editing Sessions, as a result of which this paper is complementary to ideas discussed with and now published in the Brewer-Nash paper "Insights into the ISO/IEC 27001 Annex A" [Brewer-Nash 2010].

Part I follows arguments put forth at ISO JTC 1 SC 27 #41 (Berlin – DE, 2010-10-04/08) and develops from the general consensus position reached, after debate and informal straw-man voting taken during WG1's editing meetings.

The paradigm set forth may not, it is understood, be satisfactory to all readers: it reflects the opinion and vision of its author and no other persons, organizations or bodies. It is intended to be a contribution to IS27001 in its present revision.

Background: Annex A of ISO/IEC 27001:2005 (IS27001) provides 133 controls, divided into groups of controls and control objective classifications. It is clearly stated[1] that Annex A's controls are neither an exhaustive list, nor the only source of controls. Implementers are therefore encouraged to provide controls from other sources, third-party or of their own invention, to supplement Annex A's, as they see necessary. However, despite the original intention that alternative sources may be utilised, this liberty seems not to be widely understood by ISMS practitioners, and is far less implemented, in practice.

One of the changes currently in contention for the revision of IS27001 is clarification of the application of Annex A and to make clearer the applicability of sources of controls alternative to ISO/IEC 27002.

Part I - Clarifying the application of Annex A

As required by IS27001, following a risk assessment, controls should be selected in order to mitigate the determined risks. These controls should be selected according to various criteria which the user will specify in their risk assessment method. We choose, however, to use the term "Control identification" in preference to "control selection", intending to suggest that the need for controls be determined from the assessment of risks or from some analysis of events and impacts [Brewer-Nash 2010], rather than applied simply because the controls are to be found on a list[2].

Following the control *identification,* the implementer should establish a documented record of: the applied controls; the risks which they are intended to mitigate and; the source(s) from which controls have been identified (which may include 'at the water cooler / bar', i.e. the organization identified the control itself without reference to any external source). To date, this documentary need has been largely fulfilled by the 'Statement of Applicability'. We now suggest that the required documented record be more accurately titled the 'Record of Implemented Controls' (RIC), since the actual application is a more correct statement, rather than whether the control is strictly applicable (but may still not be applied). As

[1] IS27001 §4.2.1 g), "The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected."

[2] Whilst one may question why IS27001 requires the organization to have a risk assessment methodology which suits the organization, but then proceeds to impose a specific order of process itself is not addressed directly by this paper, but we assume that implementers are able to undertake their control identification by a process of their own choosing in a manner which fits into the paradigm being here described.

indicated above, the RIC also includes a reference to the source of the control, i.e. it can no longer be argued that Annex A is the primary or even sole source.

After its initial creation, and at any review point, the RIC should be cross-checked against the Controls in Annex A and be updated with a record as to which applied controls match those in Annex A and which of the Annex A controls are considered to be not applicable. This serves two purposes. In one instance, it serves to determine if any controls have been overlooked, i.e. as a completeness[3] check. The other purpose is to provide an anchor-point against which two ISMS may be compared when based upon differing control sources, which itself guards against the use of inadequate control sources (again, be they originated by the implementer or based upon published sources).

It should go without saying that, although this risk assessment / control identification is a necessary step in the planning and initial implementation of an ISMS, it should also be periodically re-visited in order to ensure that controls remain effective and appropriate to the operating circumstances, and the RIC should be updated accordingly. Note also that the RIC need not be a separate document: it would be sufficient for the required records to be associated with the record of the risk assessment or event-impact analysis outcomes.

Historically, for some various reasons, ISO 27002 has been seen as the automatic corollary to IS27001 Annex A. This relationship must now be considered over. Although there will always, or at least for some time, be ties between ISO 27002 and IS27001 Annex A, IS27001 need be no more aligned to 27002 than to any other standard (e.g. CobiT, NIST Risk Management Framework, GMITS, etc.).

Retaining the current paradigm, the contents of Annex A will have to change as a consequence of the parallel revision of ISO 27002: the re-sequencing or removal of existing controls and the addition of new guidance for new controls in the latter document will require revision to the former. However, the retention of the mirroring of control objectives and controls in Annex A with the guidance provided in ISO 27002 will continue to unreasonably tie these two documents together. An alternative is required.

Part II - A "New Annex A Paradigm"

The proposal is to replace Annex A with a set of control selection criteria developed from a different perspective. This set of criteria would be the basis of comparison for control sources described in Part I above, and would be the reference list for the proposed RIC. Since the revised ISO/IEC 27001 should have as little affect as possible upon existing ISMSs and certifications, it would be constructive to provide a mapping of the new Annex A control selection criteria to the ISO/IEC 27002 control guidance, which should be provided through a new Annex B, including both the historical mapping (i.e. to ISO/IEC 27001:2005) and also taking into account revisions arising from the emergence of the revised ISO/IEC 27002. Conveniently, [Brewer-Nash 2010] provides the basis for these new annexes in its Appendices F & G, respectively.

Subject to availability, timing and resources, mappings of other well-recognized sources of controls could be included in the new Annex B. The utility of this must be balanced against the potential burden of

[3] 'completeness' is intended to refer to helping ensure that the risk assessment has been as complete as possible, rather than to suggest that the list of controls is guaranteed complete (rather, it should be regarded as comprehensive but not exhaustive).

inaccurate and/or incomplete mappings, as the referenced documents undergo their own revision on independent cycles.

The Control Selection Criteria concept: Part I of this paper identified the need to establish a Record of Implemented Controls and perform a verification of identified controls against it. In order to perform the verification, the organization could take one or more reference control sources, go through each them and consider whether the control applies or not. If it does not, the organization should record why not, lest circumstances change in the future. If the control does apply, then the control should have already been embraced within the control set identified by the organization's risk assessment. If that is not the case, then the organization may have found an omission in its risk assessment and therefore needs to re-evaluate it.

***Application to ISO/IEC 27001*:** The suggestion is that the revised ISO/IEC 27001 adopts the Control Selection Criteria concept. In summary, the text concerning control identification[4] would require the use of at least one source of controls to verify the comprehensiveness of the risk assessment but would leave the choice of source to the implementing organization. Annex A as it currently stands would be re-cast to state the Control Selection Criteria (drawn from [Brewer-Nash 2010] Appendix F), thereby being elevated above that of the actual controls eventually applied. This new Annex A could be supplemented by a new Annex B, a mapping (based on [Brewer-Nash 2010] Appendix G) between the ISO/IEC 27002 controls and the selection criteria presented in the new Annex A to ISO/IEC 27001.

Implications for Certification: Section 8.2.1 of ISO/IEC 27006:2007 ("*Requirements for bodies providing audit and certification of information security management systems*") states "In addition, the certificate should include a reference to the specific version of the Statement of Applicability". Thus, although this is not normative, it may be appropriate for ISO/IEC 27006 to recognise that:

a) Control sources other than ISO/IEC 27002 ought to be identified;

b) Absence of such reference would imply that ISO/IEC 27002 is the reference controls source;

c) If there is a mix of control sources including ISO/IEC 27002, then ISO/IEC 27002 would need to be explicitly identified as one of the sources.

Additionally, there would need to be the *pro tempore* recognition, (*i.e.* until the next revision of 27006), that the RIC served the same essential purpose as the SoA.

Further work: Appendix I to *this* paper proposes changes to IS27001 section 4.2.1 (original text) mapped-through to section 6.2.1 (present fourth working draft text) to apply the concepts described above. These proposed changes require consideration and debate for them to be adopted as text in the next working draft of the IS27001 revision. Additionally, [Brewer-Nash 2010] is based on ISO/IEC 27001:2005 and therefore its arguments, and more specifically, its Appendices F & G, also need to be re-cast as content suitable for inclusion in the next working draft of the IS27001 revision. This would include resolving the present Appendix F into a more formalized set of criteria suitable for use as a basis for comparison of controls from (potentially) any source, and of course creating a mapping to the final set of controls arising from the revision of ISO/IEC 27002:2005.

[4] section 4.2 of the published version of ISO/IEC 27001, section 6.2 of the fourth working draft extant at the time of this paper's publication

Conclusion: The paradigm described in Part I makes no fundamental difference to the actual ability of ISMS to be developed from alternative and multiple sources – this ability has always been there, if not readily or willingly understood. What it does do is develop revisions which make this liberty much clearer and defensible, and to provide a framework within which a consistent set of requirements can be developed to support this approach. The resultant requirements have no retrospective affect upon ISMSs in place, be they certified or not, and the transition from 'SoA' to 'RIC' would involve minimal effort (since a direct mapping to Annex A is most likely to pre-exist). Indeed, the revision of Annex A to reflect revisions in ISO 27002 (being developed in parallel to the revision to IS27001) is likely to have a much greater effect.

Part II takes the argument to the next logical stage in making Annex A a slightly more abstract, but equally-justified, basis for comparing applied controls between ISMS implementations whilst retaining (through the proposed Annex B) a tie to ISO 27002 which should reasonably satisfy any legacy approach.

The benefits of adopting these ideas are:

a. It can resolve the problem with the current dilemma regarding Annex A;

b. It creates a win-win situation for all protagonists, particularly as the control selection criteria do not favour any particular source – all are regarded as equal;

c. It has the potential to increase the market for ISO/IEC 27001, drawing in those organizations and associations who have hitherto demonstrated reservations and have argued in favour of the outright removal of Annex A;

d. It retains the favour of those who argue for the retention of Annex A: the 'safety net' concept of Annex A is retained, whilst ISO/IEC 27002 is retained as a reference source;

e. It retains the favour of those who regard having a comprehensive list of controls in ISO/IEC 27001 to be a benefit to smaller organizations;

f. It establishes an 'anchor point' from which any variation can be determined.

Further changes will be required within the revised ISO/IEC 27001, to bring management review, revision of the risk assessment, etc., into line with the above changes. These are not considered to be important for the sake of making the case for change.

Additionally, these ideas require refinement to align with revisions to ISO/IEC 27002 and to derive content in a form suitable for inclusion in the proposed new ISO/IEC 27001 Annexes A and B.

Appendix I Proposed alternative requirements versus the current fourth working draft ISO/IEC 27001 text

I.1 Comparative text with mark-up

The following table offers alternative text for the principal clauses relating to risk assessment and the identification of controls, to accomplish the principles put forth in this paper.

4WD text	5WD Proposed new text for 27001
6.1.1 Information security risk assessment The organization shall: a) Define the information security risk assessment approach of the organization that aligns with the organization's strategic risk management context in which the establishment and maintenance of the ISMS will take place. … etc. … d) Evaluate the risks. 1) Compare the assessed risks with the risk criteria established in 6.1.1 a) 2) and prioritise risks for possible treatment.	No changes
6.2.1 Information security risk treatment 18 a) Identify suitable risk treatment options, taking account of the established risk criteria 6.2.1 a). Possible options include the following: 1) avoiding the risk; 2) taking or increasing the risk; 3) removing the threats; 4) changing the likelihood; 5) changing the consequences; 6) sharing the risk with another party or parties; 7) retaining the risk by informed decision.	No changes
b) Identify suitable controls for the risk treatment option(s) chosen (see 6.2.1 a)). a) Controls shall be identified and implemented to meet the requirements identified by the information security risk assessment and treatment process. This identification shall take account of the risk criteria established in 6.1.1 a), legal, regulatory and contractual requirements, existing controls and commonly accepted practice. NOTE: Annex A contains a comprehensive list of reference control objectives and controls that have been found to be commonly relevant in	b) Identify suitable controls for the risk treatment option(s) chosen (see 6.2.1 a)). Controls shall be identified and implemented to meet the requirements of the information security risk assessment and treatment process. This control identification shall take account of the risk criteria established in 6.1.1 a), legal, regulatory and contractual requirements, existing controls and commonly accepted practice; c) document, as a Record of Implemented Controls (RIC), the controls identified and implemented, including: 1) the implemented control objectives and controls (see 6.1.1 c) 2)); and

4WD text	5WD Proposed new text for 27001
organizations; users of this International Standard are directed to Annex A as a starting point for control identification to ensure that no important control options are overlooked; the control objectives and controls in Annex A are not exhaustive and an organization may consider that additional control objectives and controls are necessary c) Compare the controls identified in 6.2.1 b) with those in Annex A and justify inclusions and exclusions. 8 In addition, the following shall be 1) the reasons for their identification: e.g. the risks addressed, or the business requirements, legal, regulatory or contractual requirements; 2) the implemented control objectives and controls (see 6.1.1 c) 2)); and 3) the exclusion of any control objectives and controls in Annex A and the justification for their exclusion. NOTE: This comparison provides a summary of decisions concerning risk treatment. Justifying exclusions provides a cross-check that no controls have been inadvertently omitted	2) the reasons for their identification: e.g. the risks addressed, or the business requirements, legal, regulatory or contractual requirements; 3) a reference to the source from which the control has been identified; 4) a reference to the point within the ISMS at which the control is implemented. NOTE 1: The RIC may be a stand-alone document or a distinct component of another document or documentation set. NOTE 2: Some controls may be identified by the organization itself, rather than from other (external) generally-recognized sources. NOTE 3: The RIC supplants the SoA referred-to in the first edition of this International Standard. ~~NOTE: Annex A contains a comprehensive list of reference control objectives and controls that have been found to be commonly relevant in organizations; users of this International Standard are directed to Annex A as a starting point for control identification to ensure that no important control options are overlooked; the control objectives and controls in Annex A are not exhaustive and an organization may consider that additional control objectives and controls are necessary~~ ~~c~~d) Compare the controls identified and recorded in 6.2.1 b) & c) with th~~os~~e Control Selection Criteria in Annex A in order to: ~~and justify inclusions and exclusions. In addition, the following shall be~~ 1) verify whether any necessary controls have been omitted~~the reasons for their identification: e.g. the risks addressed, or the business requirements, legal, regulatory or contractual requirements;~~ 2) ~~the implemented control objectives and controls (see 6.1.1 c) 2)); and~~ ~~3)~~ justify the exclusion of any ~~control objectives and~~ controls which would fall within the Control Selection Criteria in Annex A ~~and the justification for their exclusion~~. The RIC shall be updated with the results of this comparison. NOTE 4: ~~T~~Documentation of this comparison provides a summary of decisions concerning risk treatment. Cross-checking against the Control Selection Criteria helps ensure~~Justifying exclusions provides a cross-check~~ that no controls have been inadvertently omitted. Justifying exclusions provides a cross-check for completeness and the RIC is proof of having completed the cross-checking.

I.2 Clean text

The following text is the proposed alternative text in a clean, readable form.

6.2.1 Information security risk treatment

a) «*no change proposed for this sub-clause*»

b) Identify suitable controls for the risk treatment option(s) chosen (see 6.2.1 a)). Controls shall be identified and implemented to meet the requirements of the information security risk assessment and treatment process. This control identification shall take account of the risk criteria established in 6.1.1 a), legal, regulatory and contractual requirements, existing controls and commonly accepted practice;

c) document, as a Record of Implemented Controls (RIC), the controls identified and implemented, to include:
   1) the implemented control objectives and controls (see 6.1.1 c) 2)); and
   2) the reasons for their identification: e.g. the risks addressed, or the business requirements, legal, regulatory or contractual requirements;
   3) a reference to the source from which the control has been identified;
   4) a reference to the point within the ISMS at which the control is implemented.

NOTE 1: The RIC may be a stand-alone document or a distinct component of another document or documentation set.

NOTE 2: Some controls may be identified by the organization itself, rather than from some generally-recognized sources.

NOTE 3: The RIC supplants the SoA referred-to in the first edition of this International Standard.

d) Compare the controls identified and recorded in 6.2.1 b) & c) with the Control Selection Criteria in Annex A in order to:
   1) verify whether any necessary controls have been omitted
   2) justify the exclusion of any controls which would fall within the Control Selection Criteria in Annex A.

   The RIC shall be updated with the results of this comparison.

NOTE 4: Documentation of this comparison provides a summary of decisions concerning risk treatment. Cross-checking against the Control Selection Criteria helps ensure that no controls have been inadvertently omitted. Justifying exclusions provides a cross-check for completeness and the RIC is proof of having completed the cross-checking.