

## CS1/06-0184 the Zygma Partnership Contribution: Proposed US position regarding 2<sup>nd</sup> WD 27003

The US NB believes that the basic document structure is too restrained by its focus on the PDCA perspective; furthermore, operating an ISMS has perspectives which cannot be neatly packaged within the PDCA notion.

Additionally, the content of the document has a number of problems: many sentences whose meaning is very difficult to comprehend (possibly a linguistic problem or one of translation from original text); many sentences whose value is minimal – they state the obvious which any reasonably competent implementer should understand; a general superficiality of the content; unnecessary repetition of material which is already in 27001/02. These issues seriously impede the goal of providing useful guidance to users of the final standard.

The US believes that greater innovation and imagination is required in the preparation of this standard. The (revised) doc should address practical issues which concern ISMS implementers and operators. These may address any or all parts of the PDCA cycle, and issues beyond, but the doc should not adopt a PDCA-focus not structure. Following mandatory (ISO-required) introductory sections, each subsequent section should address a discrete issue. Consideration should be given to providing examples where they add clarity to the principle being discussed. These should be included as annexes, thus creating a division between the descriptive text discussing the issues addressed and the annexes which provide examples (or a single annex which holds all examples).

The issues to be addressed should include, *inter alia*:

- Σ *Building and retaining senior management commitment and participation*
- Σ *Creating an Information Security Forum (ISMS management board / steering cmt)*
- Σ *Scoping*
- Σ *Matching the ISMS to extent/size of scope*
- Σ *Setting policy*
- Σ *Hierarchical policies*
- Σ *Compliance with & conformity to other references*
- Σ *Integration with other management standards*
- Σ *Level of implementation*
- Σ *Cost factors*
- Σ *Ensuring successful audit outcomes*

### Scope

The document should complement, not repeat, the scope and content of other 27xxx documents. It should be guidance for implementers to consider and apply, taking into account their own circumstances and needs.

## **Support for revision of 27003**

The USA commits to providing tangible input towards the development of the revised 27003.

The following text provides brief outline coverage for the issues proposed above

### *Building and retaining senior management commitment and participation*

Address the need to accomplish this within the context of the SCOPE of the ISMS – if the scope is for a small department the management of that department (as a minimum) must be fully supportive of AND OWN the ISMS. Explain what this means in terms of their contribution to the setting of policy and in the ongoing management review of the ISMS. Also make clear the consequences of not having this support, including the difficulties which will be faced in gaining or retaining certification.

### *Creating an Information Security Forum (ISMS management board / steering cmte)*

More about having management commitment and involvement, but identify the required roles and explain what they are (almost in a job description' fashion. Explain that size DOES matter – if there are (say) ten roles, then in a five (or two) person business a single person can (must) have more than one role.

### *Scoping*

Determining the boundaries of the ISMS and the factors which dictate them – managerial, technical, geographic, ...

### *Matching the ISMS to extent/size of scope*

NB – **NOT** the size of the organisation – this is a red herring (maybe not a good term in the context of an international doc).

### *Setting policy*

'Inherited' (God-given) from corporate level or from legislative environment (corporate governance, accounting, environmental, health, privacy, &c). Driven by business needs and legislation. Sets initial direction but is developed and refined as ISMS is developed. Subject to review just like everything else – responsive to business and legislative revision.

### *Hierarchical policies*

How to establish them and differentiate if they are to be separately operated – arfeas of commonality, management control through the hierarchy, ...

### *Compliance with & conformity to other references*

As per paper already submitted and being enhanced by addition of case studies.

### *Integration with other management standards*

Principally 9000, 14000 series, but others (inc. non-ISO) may apply – principles of achieving this.

### *Level of implementation*

Discuss three levels and implications (in terms of benefits, addnl activities and obligations).

Level 1 – entirely internally-driven; internal auditor is only (pseudo-)independent check mechanism outside of the management processes. Limited use – internal comfort but limited external credibility, other than having some process in place.

Level 2 – external auditor – greater objectivity in audit, auditor qualifications of note – formal and extensive experience. External value may be enhanced if the Auditor has a recognised formal qualification or their name (hence credos) are widely recognised. Incurs additional cost (on a like-like basis): auditor fees; addnl internal effort to management and potentially respond to NCRs; potential savings if auditor can find problems which internal audit did not; enhanced external credibility.

Level 3 – gaining and retaining formal certification. Additional costs of certification, surveillance visits, possibly of having to maintain more rigorously-applied auditing standards: benefits from positive external visibility, which could lead to reduced costs re insurance, avoidance of clients wanting to inspect, evidence of ‘due diligence’. This represents the real goal behind publication of 27001 and should be the best practice which ISMS-owners should seek.

### *Cost factors*

Let’s face it – it isn’t free, nor necessarily cheap. Indicative costs might be helpful, if subject to wide variation and possibly setting a benchmark. Plus, who will give honest input, and need it be anonymous? Valuable guidance but very contentious. Could at least identify the Ares in which cost should be expected. Therefore needs a balance with benefits such that a judgement can be made.

Potential cost factors are:

- Learning about ISMS principles;

- Preparing the cost-benefit case;

- Training of staff in ISMS principles, awareness and (for some) audit (or recruiting staff already familiar, but with what cost of integrating them into the business);

- Use of external (**aaaaaaaaaargh, consultant !!**) expertise;

- Staff investment in developing the ISMS - will depend upon balance between direct staff and third-party support;

- Required coverage which the business does not already address;

- Overhead / new costs of applying the ISMS processes and procedures;

- Independent audit

- Certification / surveillance and re-certification (make point that this is an ongoing process, not a one-off). Poss ref to 27006 for description of the accredn/certn processes).

Counter-balanced by the benefits:

- Greater internal confidence that practices applied follow best practice in the industry;

- Enhanced external perception through independent assessment and (preferably) certification;

Enhanced info sec and consequent risk reduction;  
Selling point in proposal submission;  
Potential alternative to client walk-throughs (which potentially introduce their own security vulnerabilities  
Should it be required, evidence of due diligence (esp. of certification is held);  
Possible reduction in insurance premiums of best practices/due diligence can be shown (esp. if supported by formal certification).

*Ensuring successful audit outcomes*

Guidance on how to prepare for and to facilitate a successful outcome from a certification (or surveillance / re-certification) audit. This isn't about cheating, its about proper preparation in order to be responsive to the auditor's attention. Behind it all lies the need to have in place an effective ISMS which is being properly operated and managed. Could also address how to handle Level 1 and 2 audits, but far less of an issue.

**Summary**

The above is a tentative list of issues which implementers should address. All of them have pertinence to at least one of the PDCA stages - many of them have impact upon the operation of an ISMS through the whole process. This orthogonal approach, subject- rather than process- driven, provides the readers with a more coherent approach which the USA commends to SC27 WG1.