FISMA & ISMS ALIGNMENT

A WHITE PAPER PREPARED BY

ADDRESSING OPPORTUNITIES AVAILABLE TO
NIST'S FISMA IMPLEMENTATION PROJECT TEAM
AS THEY MOVE TOWARDS PHASE II IMPLEMENTATION
FINAL V1.0.0TER 2006-12-21

Zygma is grateful to atsec information security corporation, whose Certification Manager, Mrs. Fiona Pattinson, kindly peer-reviewed this paper prior to its publication and offered valuable comments which have enhanced the arguments presented and contributed to the paper's overall input on the FISMA / ISMS alignment issue.

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)).

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: 2006.12.21 21:37:51 Z

CONTENTS

1. Executive Summary

This paper explores the rationale for aligning the (US) Federal Information Security Management Act (FISMA) framework and the international information security management system (ISMS) standards, establishes the key drivers for that alignment and proposes some steps towards the achievement of a practical solution. This is done in the context of NISTS's FISMA Implementation Project. It is the author's contention that the alignment of these two systems is not fundamentally difficult in concept but requires substantial detailed work to develop an effective solution, i.e. the mapping of the processes within each of the two systems such that the rigour and scope is adequately maintained in the resulting integrated system.

2. Scope

This paper explores the rationale for identifying the basis for aligning the FISMA framework and the ISMS standards, establishes the key drivers for that alignment and proposes some steps towards realizing a solution.

3. Introduction

Organizations today need information security. Effective information security requires coordination of a range of activities, hence organizations require information security management. The larger the organization, the greater the need for the management element– small or simple organizations may be able to manage their information security with minimal procedures but for most organizations, even small businesses, effective management and controlled diffusion of policies. is a must. The type of activity in which the organization partakes, and the more critical the activities of the organisation are to the overall good, possibly even to the national infrastructure, the greater the need for effective information security management.[1]

None of the foregoing is news. Recognition of this was the basis for the development of ISO/IEC 17799[2], the international information security management system (ISMS) code of practice, and subsequently ISO/IEC 27001, the international ISMS requirements. Such recognition was also the basis for the passing of the Federal Information Security Management Act (FISMA), in 2002. These two standards are hereafter referred to as simply 27002 (see footnote 2) and 27001 respectively.

Organizations which choose to conform to 27001 may also opt to have their ISMS certified as being conformant with the standard, preferably through a process which enables their certification to be widely recognized, usually internationally.

Federal departments and agencies are required to comply with the FISMA and have their information systems put through a formal certification and accreditation (C&A) process.

Each of these processes puts great emphasis on the information security management, the 'ism' in their titles – they are simply different ways to approach the same issue, the difference being that the US Federal government requires compliance of its executive departments and agencies by regulation, whereas conformity with the international standard is something which any organization can (very generally speaking) take or leave, at its own discretion.

---

[1] As examples of where the need for information security is of great relevance to critical national infrastructures, see material such as:
HSPD-7 (http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html);
The House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations hearing on "Protecting America's Critical Infrastructures: How Secure Are Government Systems?" (http://energycommerce.house.gov/107/action/107-13.pdf);
The Joint Economic Committee of the US Congress report on "SECURITY IN THE INFORMATION AGE" (http://www.fas.org/irp/congress/2002_rpt/jec-sec.pdf) also recognises the value of the 17799 (2000 version) standard (under the heading 'VALIDATING COMPLIANCE - THE FUTURE OF INFORMATION PROTECTION');

[2] This standard is expected to be re-issued in April 2007 as ISO/IEC 27002:2007, and hence any reference to the '27xxx family of standards' includes also this standard in its present published form.

Although ISMS and the FISMA are *different*, they are not necessarily *mutually exclusive* ways of achieving the management of information security. That there are basic similarities in these approaches should be of no surprise, since the principles of information security are well established. What differs is the degree of prescriptivity and the focal point. The ISMS requirements standard is generalized and although it cites 133 specific controls these are not sector- or application-specific; 27001[3] also recognizes that an organization may need additional controls to adequately address its information security. The FISMA is far more prescriptive, not so much in its own wording *per se* but in the framework of additional supporting standards which are published by NIST and which give both explicit requirements and general guidance to Federal entities.

NIST SP 800-53 "Recommended Security Controls for Federal Information Systems"[4] includes, in its Annex G, a mapping between FISMA and, *inter alia*, §4 - §15 inclusive of ISO/IEC 17799.

In terms of focus we note that 27001 centres its attention on building an organizational management system that will include the systems within it, whereas the FISMA framework focuses primarily on the information systems, and includes the organization around them.

Worthy of note is that within the FISMA framework specific requirements for a C&A process (for information systems) are in-built, whereas the ISMS framework (taking the ISO/IEC 27xxx family of standards as a whole) does not have a similar process defined as a mandatory component. Indeed, to date the process of (ISMS) organizational certification has rested on regional and national practices rather than on a single, common, international standard. However, that is expected to change by the end of 2006, with the recent publication of ISO/IEC 17021 (*Conformity assessment — Requirements for bodies providing audit and certification of management systems*) and its near-term supplementation by ISO/IEC 27006:2007[5] "*Information security management systems - Requirements for the accreditation of bodies providing certification of information security management systems*", and that title alone is enough to lead us into the next section, ……

4. Terminology

It is not the intention of this paper to either define new terms or to recite terms already defined elsewhere, except that in dealing with FISMA and ISMS we find certain key terms used with different meanings and inherently different sequencing in the great scheme of things. They are summarized in the following table.

Where we use these terms in this paper we will, where necessary, qualify them as to on which interpretation we are basing our usage. By this convention we hope to be explicit as to our meaning and despite the wide-spread genetically-imprinted conditioning among most 'Federalists' to use 'accreditation' in the FISMA sense we would urge an evolutionary step towards its replacement by 'authorization'. …… It's a strange feeling, being possessed of this 'voice in the wilderness' syndrome!

5. Basic tenets

The following points are not intended to be a mantra, but are simply stated as underlying tenets which justify the goal of FISMA & ISMS alignment:

- A single process fulfilling both certification needs is a worthwhile efficiency goal;

[3] It is legitimate to focus on ISO/IEC 27001 since it provides the normative requirements for an ISMS and, with the exception of 27006, which when published will be a complementary normative standard, all other currently-planned standards in the 27xxx family are or will be informative guidance based around 27001.

[4] Published as Revision 1, 2006-12-21 - see http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf.

[5] Expected to be published 2007-01 or -02. Note that ISO/IEC 27006 is heavily dependent on ISO/IEC 17021, for which it provides ISMS-specific requirements and hence cannot be used without the latter standard also being applied and conformed-to.

- The 'management' of information security in the context of risk is paramount;
- Assigned management responsibility requires well-communicated policies and comprehensive risk assessments which lead to selection of suitable controls based upon acceptable residual risk, which justifies their acceptance of the management system;
- FISMA alignment to an international standard provides access to benefits of mutual recognition;
- Both systems recognize that management of information security does not stop at the boundaries of the organization itself but extend into third-party relationships.

6. Mapping 27001 to the FISMA Implementation Project's Vision

The FISMA Implementation Project's (FIP) vision is published at http://csrc.nist.gov/sec-cert/. How do its elements compare to the principles and practices embodied in 27001?

The principle vision statement of the FIP's vision is:

> **(to) Promote the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act.**

It then states five goals which are included in the vision. We repeat them here and then comment on how 27001 relates to each of them (clause references relate to 27001).

Term Usage/source	Accreditation	Certification	Authorization	Credential(ling)
FISMA (from SP 800-37)	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	See Accreditation (Note – footnote 6 of SP 800-37 states: "Security *accreditation* is synonymous with security *authorization*; the terms are used interchangeably in this special publication.")	No definition in SP 800-37 or '-53 – generally taken to be the same function as the ISMS term 'Accreditation', i.e. Recognition of the ability of an organization to provide security assessment services for Federal agencies' information systems, so as to support the [FISMA] C&A process.
ISMS (author's own definitions, since none of the related EA and ISO/IEC (17021, 27001, 27006) documents provide one - yes, strange, isn't it?)	The formal recognition by an authoritative body that an organization is competent to perform assessments against ISO/IEC 27001 and grant certificates of conformity against that standard.	The assessment or audit of an information security management system performed by an Accredited Certification Body and the subsequent issuance of a certificate as to the conformity of the ISMS as defined by its Scope, against the requirements of ISO/IEC 27001.	A management assertion that the ISMS may be implemented and operated, implicitly that management also approves "the proposed residual risks" [ISO/IEC 27001 wording].	No such term, for any purposes.

Table 1 – Differential term usage

Goal 1: Standards for categorizing information and information systems by mission impact;
27001 requires that assets be identified and responsibility for them and their usage assigned (A.7.1) and that a classification system be established (A.7.2). The 'mission impact' element would be addressed in a number of ways, e.g. scope and the processes of selecting and applying a risk assessment approach (§4.2.1 (c) to (f) inc.) and selecting controls accordingly (§4.2.1(g));

Goal 2: Standards for minimum security requirements for information and information systems;
27001 states a number of processes (§4 to §8 inc.) and cites 133 reference controls (Annex A) for each of which the ISMS owner must justify the use or omission. NIST requirements are more comprehensive;

Goal 3: Guidance for selecting appropriate security controls for information systems;
17799 gives implementation guidance for the reference controls in 27001 (Annex A) and in addition 27001 recognizes the potential need for organizations to add their own controls (Annex A, first paragraph). Controls cited in NIST's FISMA-supporting standards and publications are more extensive but can in most cases be mapped into the 27001 reference controls, or otherwise added as specific additional needs.

Goal 4: Guidance for assessing security controls in information systems and determining security control effectiveness;
27001 requires that the ISMS be monitored and reviewed (§4.2.3) and maintained and improved (§4.2.4), with (§4.2.3 (b) and (c)) referring specifically to the effectiveness of controls. A further standard[6] presently in early draft form, and at a very immature level of content, is intended to provide implementation guidance, which would address the putting into effect these requirements.

Goal 5: Guidance for certifying and [authorizing] information systems.
27006 will provide requirements and guidance in the area of certification of ISMSs. 27001 also requires that there be a positive management decision to authorize use of an ISMS (§4.2.1(i)). By placing a requirement that an ISMS be in place for each management system then these requirements could arguably be met, but one has to be cautious of some subtle differences. A conformant ISMS requires that this authorization be granted. However, a decision to have the ISMS certified is separate and would follow – indeed, the certification assessment would check and require that such authorization had actually been granted. Thus in the ISMS context the activities are reversed and therefore carry subtly different meanings.

If awarding marks out of ten for the ability of 27001 to satisfy these goals the rating might be (from a maximum of two points per goal statement): 2 - 1 - 1.75 - 1 - 1. This yields a 67.5% alignment rating.

This is a crude assessment but to the author suggests that the potential is there. By creating some specific mappings between the NIST standards and the ISMS processes and controls, and narrowing the freedoms of the ISMS implementers (justifiable where they goal is to jointly fulfill FISMA requirements), a much greater level of alignment can be achieved. In the context of 'manipulating' the ISMS aspects, given the stated intent that the ISMS is a flexible concept in terms of the details of how it is operated (the focus being on the application of the requirements in a manner suitable for the scope of the ISMS), the greatest challenge presented in the above is probably in the last goal.

[6] Presently 1st Working Draft of the intended ISO/IEC 27003, as at the date of this paper's publication.

The FIP's vision continues, stating that the achievement of the above goals will have certain consequences. Again, we comment on how 27001 relates to or complements, each of them.

Consequence 1: The implementation of cost-effective, risk-based information security programs;

Shared by ISMS – it requires that planning and regular review of risks achieve effective controls at a cost which is commensurate with the value of the assets being protected.

Consequence 2: The establishment of a level of security due diligence for federal agencies and contractors supporting the federal government;

Implicit in ISMS, in that management should be demonstrably involved in setting policy, exercising control over the risk management and the selection of controls and exercising control over its third-party relationships. This works both for Federal agencies and contractors supplying the Federal government.

Consequence 3: More consistent and cost-effective application of security controls across the federal information technology infrastructure;

A harmonized relationship between FISMA and ISMS would give greater cost effectiveness than two separate assessment frameworks where the acceptability of their certifications was not harmonized. Fulfillment of Phase II of the FIP can deliver this consistency and cost-effectiveness.

Consequence 4: More consistent, comparable, and repeatable security control assessments;

This is equally true of any well-crafted information security model – the potential to achieve this by aligning FISMA and ISMS is greater by the addition of more international harmonization and recognition which would arise from alignment (see 'Consequence 3').

Consequence 5: A better understanding of enterprise-wide mission risks resulting from the operation of information systems;

The enterprise-wide aspect is better-supported by accomplishing an alignment between FISMA and ISMS, giving greater utility to the resultant certification which will serve wider enterprise goals.

Consequence 6: More complete, reliable, and trustworthy information for authorizing officials--facilitating more informed security accreditation decisions;

Whether FISMA represents 'best practice' as a generally-recognized reference for such is yet to be proven, without suggesting that FISMA represents undesirable or in any way inferior practice. However an alignment between FISMA and ISMS would strengthen the core processes, giving the potential for greater confidence in the fundamental framework.

Consequence 7: More secure information systems within the federal government including the critical infrastructure of the United States.

Aligning FISMA and ISMS may not necessarily make these systems more secure, unless further comparison between the two approaches, including their supporting structures, reveals enhance-ments for the FISMA-perspective which might otherwise not have been there. One could at least expect a solid reinforcement of the FISMA model arising from alignment.

In each of the perceived (and inherently positive, constructive) consequences set out for the FIP, the alignment with ISMS brings is supportive.

7. Aligning the processes

We have considered then how the ISMS processes are supportive of the FISMA goals and anticipated consequences (which might also be regarded as the benefits of achieving those goals). Alignment should be considered as a second layer of framework around the ISMS processes: a means of applying the ISMS processes in the context of a more tightly-defined, closer-scoped framework whilst retaining the ISMS approach overall so as to enjoy the broader benefits of that model. Such an approach has already been applied and proven in the UK, as the *tScheme*[7] project. Alignment between FISMA and ISMS is more complex, because they are two pre-existing, independently-developed frameworks, as opposed to the evolution of *tScheme*, always with the ISMS accreditation and certification concepts in mind.

The FISMA Implementation Project's (FIP) description of its Phase II (at http://csrc.nist.gov/sec-cert/ca-proj-phases.html) states:

> **Phase II: Organizational Credentialing Program (2006-2008)**
>
> The second phase of the FISMA Implementation Project will focus on the development of a program for ***credentialing*** public and private sector organizations to provide security assessment services for federal agencies. The security services involve the comprehensive assessment of the management, operational, and technical security controls in federal information systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
>
> Organizations that participate in the credentialing program can demonstrate competence in the application of the NIST security standards and guidelines. Developing a network of credentialed organizations with demonstrated competence in the provision of security assessment services will give federal agencies greater confidence in the acquisition and use of such services.

If alignment with ISMS is a serious contender for supporting FIP Phase II (which the author firmly believes it is) there are three principal areas to consider:

1. The mapping between the FISMA and ISMS controls;
2. The information security management processes involved;
3. The 'approval framework elements;

Dealing with each of these in turn:

7.1. Mapping controls

NIST SP 800-53 Revision 1 provides (Annex G) a mapping of its controls against a number of other references. One of these references is the ISMS Code of practice, i.e. 17799[8]. The mapping is (unsurprisingly) '800-37 –centric': it lists all of its own controls and identifies those ISMS controls which can be mapped against them[9]. There are 21 of its own controls against which there is no stated ISMS control mapping.

[7] See www.tScheme.org; the author of this paper took a leading role in defining how *tScheme* was developed within the context of BS 7799-2 (at the time the *de facto* world ISMS standard, now superseded by 27001), using dedicated criteria and an extended form of accreditation for '*tScheme*-recognised' Certification Bodies.

[8] Reference to 17799 is perhaps an historic hang-over from when there was no internationally-published set of ISMS requirements. With the existence of a published international standard for ISMS Requirements (i.e. 27001), reference to that standard would be a preferable cross-reference because of its normative nature. As discussed further, this would also have the potential to address the future comparative mapping of the management processes involved. A change to reference 27001 instead of 17799 would not affect existing mappings, other than those made to §4 of 17799.

[9] This observation is not intended as a criticism of the process involved. It would be fair to record at this stage that the introduction to SP 800-53 Annex G states that "the mapping table [provides] a *general* indication of Special Publication (SP) 800-53 security control coverage with respect to [the ISMS] control sets. The security control mappings are not exhaustive and are based on a broad interpretation and general understanding of the control sets being compared."

Further, analysis of the ISMS mappings reveals that of the 133 ISMS reference controls all but 13 of them have been mapped to one or more SP 800-53 controls. A brief review of these un-mapped ISMS reference controls also suggests that, for at least half of them, including them in the mapping would not be difficult and in some cases their inclusion may even be implied.

There may be specific reasons why some controls have not been mapped, but if so, the mappings given do not state any such reasons. It may also be the case that a specific SP 800-53 control indeed has no mapping to an ISMS controlfor the practical reason that there is no suitable ISMS control; in such an instance an extended control or set of controls would be an appropriate way to resolve this[10]. Completion of this mapping and creating the cross-references in both directions between the two sources, plus definition of any required Extended Control Sets, is a necessary step to support alignment.

7.2. Information security management processes

As indicated above, by using 17799, SP 800-53 provides (Annex G) a mapping of its controls against the ISMS reference control set. This annex does also make reference to 17799 §4, which deals with 'Risk assessment and treatment', but this is still only guidance, not explicit normative requirement, which is provided by 27001. Thus, this Annex (or indeed any such mapping against the ISMS model) should address normative sections 5 - 8 inclusive of 27001, as well as the normative controls in Annex A. Sections 5 – 8 of 27001 provide the requirements for the information security management system, addressing management responsibility, internal audits, management review and improvement of the management system. Alignment surely requires that the relationship between this management model and that required by FISMA be understood, and the common and divergent features recognized. Divergent features then need to be understood in order to determine where they can be modified to be common or complementary, or whether they are simply incompatible. In the latter, case the overall impact of that incompatibility needs to be understood in terms of its criticality to alignment, and the extent to which there may be any disruptive effect.

7.3. Approval framework

This area presents the greatest challenge to alignment, not only because of the confusion surrounding the terminology, but also because of specific differences in the two approaches, the points at which authoritative decisions are made and by whom, when assessments take place and when management systems are operated according to their defined processes, procedures and controls.

To summarize the FISMA process: The process is mandatory so far as Federal executive departments and agencies are concerned. It requires that an assessment be performed as a part of the management process to accept risk. That assessment is undertaken by a 'credentialed' assessment organization. A formal 'certification' comes from a successful assessment, and thus this process is generally known as 'certification'. Positive outcome of the certification supports an agency management decision to allow the system to be 'accredited' and thereby to have an authorization to operate (ATO).

To summarize the ISMS process: The process is elective although a decision to acquire formal certification involves a formal process requiring conformity in full. Internal management decisions to accept the risks remaining after selected controls have been implemented and to approve the operation of the ISMS are basic pre-requisites. The ISMS (and therefore the system or systems within its scope) may then be operated without requiring formal certification – indeed, the systems within the scope of the ISMS may even have been running before the ISMS was brought into being. When a formal certification is sought the ISMS should have been

[10] Zygma has published a paper addressing how to develop an ISMS which serves to show compliance with specified legislation, regulation, other standards, &c. – see "Policy, regulatory and standards conformity through an ISMS" at www.Zygma.biz/Pages.cfm.

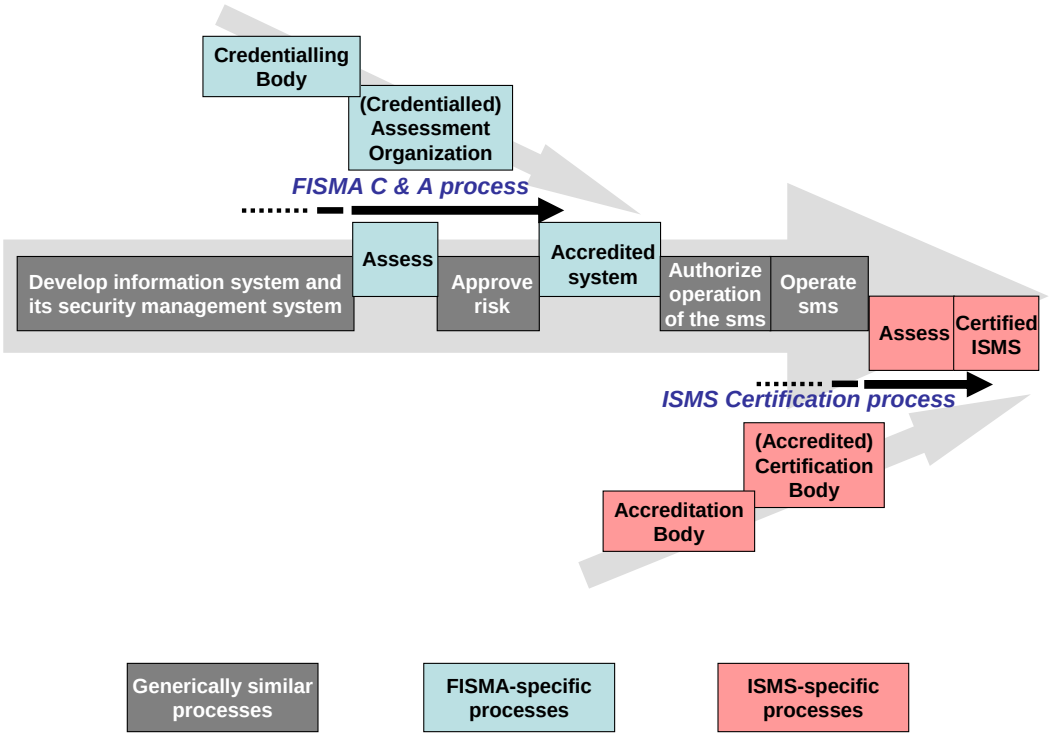

Figure 1 – comparative steps in the FISMA & ISMS frameworks

operated through at least one turn of the basic 'PDCA' cycle[11], i.e. there has to be evidence that the ISMS is being appropriately managed. Positive outcome of the certification audit leads to the ISMS being certified.

It will be apparent that there is some dis-junction between these two approaches, indicated graphically in Figure 1. However, there is good reason to consider that these differences are manageable.

With reference to Figure 1, the term 'security management system', abbreviated to 'sms', is used as a generic reference to the process in either the FISMA or ISMS models.

The element 'Develop information system ..' covers what in FISMA (i.e. SP 800-37) is described as the "Initiation Phase". It involves agency internal roles. The ISMS equivalent would be "Establishing and managing the ISMS" (27001, §4.2), also a process involving the management of the organization owning the ISMS and its subject systems. In each case the principles addressed are policy determination, the identification of assets and other resources, assessment of risk, the selection of controls and the documentation of the management system and the system itself.

The next step in FISMA is the 'Security Certification Phase'. In FISMA a certification assessment is undertaken at an earlier stage than in the ISMS model. In the former the certification, undertaken by an external party (as it should be within an ISMS, whether by an independent external audit or by a formal certification audit), serves as the input to the 'Security Accreditation Phase'. Assuming a

[11] PDCA – Plan, Do, Check, Act, the basic steps in a process improvement framework originated by Walter Shewhart in the 1930s, and later adopted by W. Edwards Deming (the latter in fact usually getting the credit for its origination, it being also known as the 'Deming Cycle'). See the Introduction to ISO/IEC 27001.

successful certification assessment, the results of certification serve as the basis for accepting the residual risks in the system and granting an approval to operate (ATO). As already noted, the ISMS model differs in that the security management system should first be authorized as being fit to operate (a management decision, not an assessor's) and then shown to operate before the independent assessment is undertaken, although there is nothing to stop an earlier assessment being introduced and, subject to observing applicable rules regarding the impartiality of the audit team, this could be performed by the same body as that performing a formal certification.

In an ISMS audit it is normal for documentation to be provided to the assessor(s) who then conduct a 'Stage 1' audit, basically a desk-audit. After resolution of any issues arising from that audit the 'Stage 2' audit is performed at the ISMS-owner's location, actively examining records, sampling evidence, and observing operations including visiting different sites where appropriate. It is not inconceivable that in the ISMS model a 'Stage 1b' audit could be inserted between Stages 1 and 2, and that a combination of 'Stage 1' and 'Stage 1b' could fulfill the FISMA 'Certification Phase' requirements, with the ISMS 'Stage 2' audit leading to the formal third-party Certification once the system, granted its 'ATO', had been put into operation.

The FISMA 'Continuous Monitoring Phase' has the same basic goals and elements as would the monitoring and re-certification stages of formal ISMS certification.

As the above would suggest, it is the author's belief that the differences in these approaches can be overcome by defining a unified methodology which will preserve the specific control and decision points which FISMA requires whilst applying the ISMS certification methodology. The benefits of a single assessment and a wider recognition of the resultant certification are manifest.

Commensurate with the alignment of these methods is the need that the assessing parties are qualified to perform the assessment role in both FISMA and ISMS contexts. The implication is that a single accreditation process (in the ISMS sense) be employed to recognize the competence of bodies to perform assessments within the aligned schema. That schema will have to be a modified ISMS framework, i.e. ISMS for FISMA, which ensures that the final certification fulfills the 'national' need (i.e. the FISMA need), whilst also satisfying the obligations towards international mutual recognition of ISMS certifications.

8. A rare opportunity

Alignment of processes presents NIST with a unique opportunity. Despite the fact that 27001 was published in September of 2005, there has yet to appear any sign of a reliable US-based ISMS accreditation scheme being implemented[12]. NIST appears to be committed to the establishment of a credentialing scheme, in support of FISMA 'C&A' assessments: why shouldn't that process be based upon the ISMS accreditation approach and related standards (see footnote 12) and be the US accreditation body for ISMS, including establishing the proper affiliations to ensure that certificates issued by its accredited[13] assessors have international recognition?

By so doing NIST could most likely provide itself with a 'credentialling' market which was wider than FISMA assessments alone (and if it can establish a means to benefit from it, create for itself a greater revenue stream with which to cover its costs in establishing and operating this framework). Furthermore, since the international standards for application and operation of such a scheme are established, the set-up costs should be reduced by the absence of need to originate much of the required material. The cost required would be to understand

[12] In this context the author would consider 'reliable' to mean having a proven and competently-managed process for the receipt of applications from and the resultant issuance of accreditation to bodies having the skills, resources and impartiality to effectively perform ISMS assessments according to ISO/IEC 17021 and ISO/IEC 27006 (the latter being in its final stages of pre-publication by ISO).

[13] ISMS usage

and align the relationship between FISMA and ISMS and build that additional layer to interface them. The potential size (volume) of this market requires some analysis, a focus beyond the scope of this paper.

9. Recommended steps

Drawing from the above, the steps described below could be adopted by NIST's FIP Management Team to accomplish the FIP Phase II (assuming the objectives set out in this paper):

1) ***Mapping Controls***: Complete the analysis of FISMA controls against the controls of ISO/IEC 27001. Prepare the 'reverse analysis' – i.e. map which ISMS controls relate to which FISMA controls: (an ISMS implementer must still respond to all 27001 controls and will need to show, from their ISMS Statement of Applicability, how the FISMA controls are met;

2) ***Information security management processes***: Map FISMA to the requirements of ISO/IEC 27001 §4 - §8, i.e. to the required processes and procedures, in addition to the reference controls of Annex A (and construct the reverse mapping to complete the process of step 1, above);

3) ***Approval framework*:** Compare the ISMS 'Accreditation - Certification' model and processes of ISO/IEC 27006 to the FISMA 'Certification – [Authorization]' model of SP 800-37, and explore ways in which to leverage the ISMS approach within the specific context, constraints and controls which FISMA overall requires;

4) ***Approval framework*:** Establish an Accreditation Body under the auspices of NIST/NVLAP, with agreements with the appropriate bodies to facilitate international harmonization and mutual recognition agreements, e.g. through the International Accreditation Forum. The goal should be to enable an ISMS performed with the specific goal of FISMA-compliance to be acceptable within the context of FISMA C&A and within the global ISMS community.

In undertaking these steps there may be a need for broader participation at the international level.

10. Why shouldn't alignment be achievable or practical?

In painting such a positive picture of the prospects and feasibility of alignment it would be careless to ignore the likelihood that some counter-arguments will be raised, and quite possibly some serious ones!. Whilst not claiming, or even attempting, to identify all potential counter-issues which may arise, some possible arguments might be pre-empted and addressed.

One-such issue might be protecting the national interest – the suggestion that adopting an international standard and aligning to international mutual recognition processes might give external parties an undue influence over how national policy is planned, controlled and implemented.

We don't see this as a serious threat: by having a US body fulfilling the Accreditation Body role (NIST is proposed, but even if it were to be another obviously US national body) and by having NIST actively participate because of their FISMA interests, i.e. they manage a FISMA add-on, the USA would retain control on a national basis. Any potential 'loss of control' would only extend to the question of mutual recognition, which at the national level (e.g. protection of the critical national infrastructure) becomes moot.

Further, the 17021/27006-defined process is very unlikely to change, and would not do so without adequate prior notice and opportunity for USA to comment and opt out of if it so chose. Even if an opting-out were to be effected, a de facto mutual recognition situation would likely exist anyway. As a further protection, adoption of the international standard by ANSI effectively says that the accreditation and certification processes would be against national standards.

Related to the national interest perspective is a further issue: the FISMA approach is a prescriptive one which seeks to reduce the risk to the nation by using the blanket effect. It considers 'the organization' as the U.S. Government and seeks to reduce the risk at that level. Even when individual agencies or departments may actually end up with their risk increased, or at least not being optimally efficient. Against this, 27001 focuses on individual small organizations or departments (as per the ISMS scope) and optimises the risk assessment at that level.

Thus, in order for a system at the agency level to contribute to the national good, its risk assessment may be non-optimal within its discrete scope. In that case, assuming that this circumstance is recognised and is not so by inadvertent good-fortune, it should be a case of the ISMS management accepting the residual risk and selected controls justified on the argument of 'being for the greater good'?

This should not present a difficulty if formal certification were to be sought. The need for a level of applied security above that which may be 'locally' optimal can be easily justified as an imposed policy, within which the management system has to function. Remember, it is not the assessor's job to optimise the risk assessment and selection of controls, only to determine that there is a conscious, competent and consistent approach to the management of information security, which clearly there would be.

11. Conclusion

For the adventurous Federal agency or commercial body which can benefit from having an ISMS (optionally a certified ISMS) and which also needs to demonstrate FISMA compliance, a combined solution is viable today. There is a growing body of work already performed to support them (ref. the Federal PKI Operational Authority's ISMS[14]) although there remains work to be done.

Significant economy, and consistency, would be achieved if NIST were to provide, as a part of its PHASE II FISMA Implementation Project, resolution of these issues. Both the Federal government and US industry at large would benefit.

To ensure broader recognition the alignment tasking could benefit from inclusion of those international parties with whom mutual recognition is sought. Noting that there are other nations interested in the FISMA approach, itself a positive sign, we should encourage international collaboration through established standardization fora.

Many of the nations having interest in the FISMA model already have a strong commitment to the ISMS model as well and will want to see that preserved, and strengthened. A FISMA model aligned to ISMS would have significant international impact and appeal and could potentially lead to changes to existing, or the provision of new supporting, international standards (principally in this context through ISO/IEC JTC1 SC27, the body responsible for the ISO/IEC 27xxx family of standards).

The steps outlined above propose a plan to accomplish all this. With the resources which have been applied in the preparation of this paper it would be foolhardy to say that everything is 'done and dusted' and that all potential issues have been addressed and resolved.

Undoubtedly, developing a unified approval framework presents the biggest challenge, but it represents the keystone on which overall alignment must be built, and it is achievable. Our experience has shown that, and Zygma is ready to assist with the realization of that goal. We hope that this paper presents a helpful contribution towards that end.

[14] the Zygma partnership is contracted to assist the Federal PKI Operational Authority in the development of an ISMS covering the OA's systems.

12. Amendment record

Version	Date	Notes
v1.0.0	2006-12-06	Initial release to web site.
v1.0.0bis	2006-12-19	Minor revision to correct date of FISMA release (cited as 2003, but was in fact 2002).
v1.0.0ter	2006-12-21	Minor revision to update with references to formal release of NIST SP 800-53 Revision 1. Just unfortunate timing.