Proceedings of the 11th Colloquium for Information Systems Security Education
Boston University
Boston, MA June 4-7, 2007

Alignment of Information Security Assessment Best Practices

Richard G. Wilsher, *the Zygma partnership LLC*, and Matt King, *Enspier Technologies, Inc.*

Abstract

The Federal Information Security Management Act places obligations upon Federal agencies and their contractors, effected through National Institute of Standards and Technology standards and guidelines. FISMA compliance has, however, limited recognition beyond the Federal domain, whereas there is an increasing move in the private sector towards the international standard ISO/IEC 27001 ("Information security management systems – Requirements"), formally-certified conformity to which has widespread acknowledgement and international mutual recognition.

This paper compares these two approaches to assuring an organisation's information security management practices and proposes steps to align the two models, yielding economies for those entities which stand to benefit from the fulfilling both sets of criteria.

I. Introduction

Providing assurances as to the security and reliability of information systems has become, and will increasingly be, a major concern for government and industry alike. Governments naturally have a primary focus within their own territories although industry often has to cope with these issues globally.

The assessment processes used to provide these assurances often have, at a simplistic level, similar external appearances and objectives but can vary significantly in their internal composition and functioning.

Many organizations are subject to demands for assurances (often put in terms of having to demonstrate 'compliance') which require them to have in place multiple assessment processes, leading to redundancy, increased costs and limitation to the value derived from any particular assessment.

This paper describes work in hand, deriving from both private research & development undertaken by Zygma in relation to the international Information Security Management Standard (ISMS), ISO/IEC 27001:2005 (27001) [1] and from work sponsored by the Federal PKI Policy Authority concerning the Federal Information Security Management Act (FISMA) [2] and related standards and publications. This work has the ultimate goal of aligning some of the key assessment methods at large today in the United States. In addition, this work has an international perspective and offers a basis for improved return on investment, relieving organizations of some of the load of undergoing multiple assessments whilst giving them greater value from their efforts, because of their ability to provide assurance to a wider range of stake-holders.

II. Principal information security management frameworks

A. The US Federal information security framework

At the national level in the U.S.A., the Federal government has established a plethora of regulation, standards and other publications addressing the security of information systems. Of particular importance is the FISMA, passed into law in 2002.

In response to its responsibility under the FISMA, the National Institute of Standards and Technology (NIST) produced Federal Information Processing Standard (FIPS) 200, "*Minimum Security Requirements for Federal Information and Information Systems*" [3], with which Federal agencies have a mandatory, non-waiverable, obligation to comply. To do so, agencies must first determine the security category of their information system in accordance with the provisions of FIPS 199, "*Standards for Security Categorization of Federal Information and Information Systems*" [4], and then apply the appropriate set of minimum (baseline) security controls in NIST Special Publication (SP) 800-53, "*Recommended Security Controls for Federal Information Systems*" [5], which itself references other required NIST Special Publications.

One can readily see that compliance with FISMA requires agencies to take into account and comply with many other NIST standards and guidelines. How they show their compliance is a process defined by NIST SP 800-37, "*Guide for the Security Certification and Accreditation*[1]

[1] 'Certification and Accreditation' is generally abbreviated to 'C&A': however, the word 'accreditation' gives rise to some confusion when discussing the subjects of this paper with

ISBN 1-933510-96-7/$15.00

of Federal Information Systems" [6] which NIST also produced as a responsibility under the FISMA. NIST subsequently produced further, specific, guidance related to assessing the controls in NIST SP 800-53, which is given in NIST SP 800-53A, "*Guide for Assessing the Security Controls in Federal Information Systems*" [7].

If this is not enough, there are other requirements upon Federal agencies arising from Homeland Security Presidential Directives, Office of Management and Budget memoranda, departmental and agency policies, and a plethora of further NIST standards and publications, all too numerous to mention in this paper, but still demanding, at some level, agencies' attention, if not their compliance.

To bring this to a very high level of abstraction, through FISMA we have a set of criteria (from multiple sources) with which mandatory compliance is required, guidance as to how to comply with those criteria, and a defined process for the assessment of compliance.

B. The international information security framework

Meanwhile, at the international standardization level, in the year 2000 the International Organization for Standardization (ISO) published, in cooperation with the International Electrotechnical Committee (IEC), an information security management code of practice, ISO/IEC 17799:2000, now published as ISO/IEC 27002:2007 [8]. As a code of practice this standard[2] is only informative guidance, but was seen from the time of its publication as a significant and authoritative source of guidance for those developing information security management systems.

In 2005 ISO published ISO/IEC 27001, "*Information Security Management Systems - Requirements*", which put the normative requirements into the international arena and hence available to all ISO members as a national standard.[3] Whereas 27002 provides guidance on the implementation of 133 security controls, 27001 requires conformity to not just those controls (which it defines normatively) but with specific processes to provide for establishing the management system, operating, improving and auditing the system, and expresses requirements for management responsibility.

ISO has also published ISO/IEC 27006, "*Requirements for bodies providing audit and certification of information security management systems*" [9] and is in the process of developing other publications in the 27000 family which will include a freely-available overview (27000), plus guidance on implementing an ISMS (27003), measuring performance of an ISMS (27004), risk management (27005) and guidance for the performance of assessments (27006).

Thus, the ISO ISMS family of standards has a set of criteria (in this case as a single source, 27001) with which conformity is voluntary, guidance as to how to conform to those criteria, and a defined process for the assessment of that conformity.

The FISMA and ISMS models sound similar, and in many ways are, yet they have some significant differences (Figure 1).

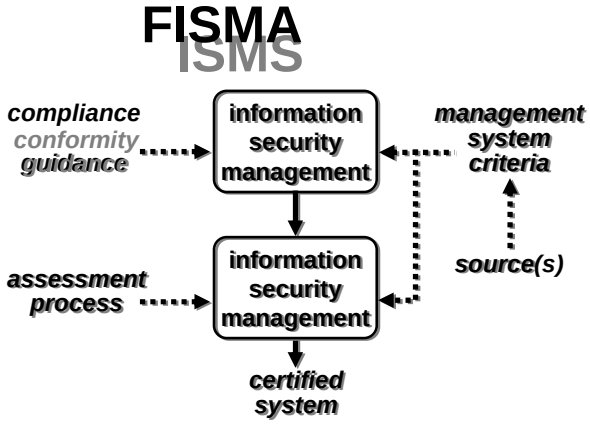

Figure 1 – comparative process models

C. ISMS take-up in the U.S.A.

In May 2002 the Joint Economic Committee of the US Congress reported on "SECURITY IN THE INFORMATION AGE" [10]. This report states "*The defining standard for developing an information*

different groups. In the international assessment arena it is a term used to define the process of determining that a given entity is capable of performing tests or assessments upon other organizations with the purpose of determining their compliance or conformity to a specified standard or process. In this paper '*accreditation*' is used exclusively in that context. Footnote 6 of NIST SP 800-37 [6] states "Security *accreditation* is synonymous with security *authorization*; the terms are used interchangeably in this special publication." This paper will use the word '*authorization*' as a synonym for 'accreditation' when referring to the C&A process, and also when referring to any management authority for a process to operate, e.g. for a system to be put into use. The ISMS usage of '*accreditation*' is generally synonymous with the FISMA term '*credentialing*'.

[2] Whereas NIST publishes standards which are normative (i.e. must be followed) and special publications as informative guidelines (i.e. not mandatory, although you might need to have a good case for ignoring them), ISO standards may be either normative or informative.

[3] BS 7799-2 and its clones were phased out as certifications against those standards required renewal.

protection program around [sic] *is ISO 17799, formerly British Standard 7799* [Part 1]". At that time there was no international equivalent to BS 7799-2, the management system requirements, and one might suspect that it was considered impolitic for a Committee of Congress to recommend a foreign standard as the basis on which to secure the nation's information infrastructure.

Nevertheless, that didn't stop US organizations (ranging from Federal banks through pharmaceutical and technical businesses to academic institutions) from adopting the ISMS model and getting certified by bodies outside the U.S.A., themselves accredited outside the U.S.A. Today there are US-established certification bodies yet, in the absence of an accepted US accreditation scheme, these are still accredited by foreign schemes (mostly European).

None of this stops the uptake of the ISO ISMS model, and those of us in the business see a bourgeoning interest.

D. Other security control requirements, methods and assessment means

The FISMA and the international ISMS standards are not the only games in town. Within the U.S.A. alone there are many Federal and State acts which require compliance with specific criteria relating to information security. As a brief selection we have, *inter alia*, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley (SOX) Act, California's SB 1386 & AB 1950 (concerning the release of personal identifiable information). Financial institutions have many regulations which relate to them and come with defined audit processes (e.g. the Federal Financial Institutions Examination Council's Information Security Booklet – a 'booklet' of some 130 pages!).

ISO publishes many other standards which are information security related, some in specific technologies and is even proposing new 27000 guidance standards which focus on particular domains. The payment card industry (PCI) has its Data Security Standard. We also find various assessment methods are around – accountancy institutes have schemes set up, such as the Statement on Auditing Standards (SAS) 70, and other schemes, e.g. '*WebTrust Program for Certification Authorities*'[SM/TM].

With such a choice do we need any more standards? The authors believe the answer is no; but moreover that we need to consolidate. Many of the sources referenced above have a closed scope and do not address a comprehensive management approach or lack consistent controls and criteria. This may be good for the value they place in a specific area, but businesses and government agencies need to take a holistic view of their information security.

III. The case for aligning FISMA and ISMS

A. Where FISMA and ISMS interact

The FISMA applies not only to Federal information systems, but to those of organizations in the business-sector who contract with Federal bodies. Thus FISMA's reach is greater than it may at first appear. Whilst FISMA compliance may serve the organization in terms of winning business with the Federal government the qualification has no significant recognition elsewhere, in particular in the international arena.

Other organizations unfamiliar with FISMA may be reluctant to accept a FISMA 'certification' and many are in fact already asking for certification against ISO/IEC 27001. This is becoming increasingly common in the supply chain and the aerospace industry is one such sector where domain-specific 27001 implementation guidance is being developed. For those organizations which want to have the benefit of an internationally-recognized information security certification and yet also satisfy their government clients, a single assessment framework which could address both FISMA and ISMS needs would have significant appeal.

There is, therefore, a strong business case for aligning FISMA and ISMS.

B. The game's afoot!

When we compare FISMA and ISMS, with a view to pursuing their alignment, we notice some strong similarities and some differences which, whilst not catastrophic, require due consideration in aligning them to create a single assessment model.

We also find that in the ISMS requirements there is provision for additional controls as required by the ISMS owner, and in NIST SP 800-53A it states:

> *"The reuse of applicable security assessment results from previously accepted/approved assessments of the information system can also be considered in developing the necessary evidence for determining overall security control effectiveness. Applying previous assessment results to a current assessment requires a thorough analysis of the security controls and state of the information system to determine if any changes have occurred since the previous assessment and if the previous assessment results are applicable to the current assessment."*

Thus, each model is positive towards including additional controls and making efficient use of other assessment outcomes, where they are applicable.

C. Common goals and features

The fundamental similarity between FISMA and ISMS is that they are both driven by a risk assessment and management process. They both embody the principles of:

- Defining the scope and purpose of the information system, the assets it includes and from that, determining the level of criticality/sensitivity of the system;
- Establishing a risk assessment process, identifying and evaluating risks, deciding how to treat the risks, selecting controls which mitigate the risks;
- Gaining approval (authorization) to operate the system;
- Documenting the security management system in place;
- Reviewing and assessing the risks and controls, incidents, and reacting to them to improve the overall system.

If we consider the achievements of the FISMA Implementation Project (FIP) in supporting FISMA compliance we can relate these to the requirements of the ISMS model.

- The FISMA has standards for categorizing information and information systems by mission impact; the ISMS model requires that assets be identified and responsibility for them and their usage assigned and that a classification system be established. The 'mission impact' element would be addressed in a number of ways, e.g. by the ISMS scoping and the processes of selecting and applying a risk assessment approach and selecting controls accordingly.

- The FISMA has standards for minimum security requirements for information and information systems; The ISMS model states a number of required processes and cites 133 reference controls, for each of which the ISMS owner must justify the use or omission. Controls cited in NIST's FISMA-supporting standards and publications are more comprehensive and extend to a lower level of granularity but can be mapped readily into the ISMS reference controls.

- The FISMA has published guidance for selecting appropriate security controls for information systems; The ISMS model gives implementation guidance for its reference controls and also recognizes the potential need for organizations to add their own controls. Where NIST's requirements have no obvious match within the ISMS requirements additional controls can be added as needed.

- The FISMA also provides guidance for assessing security controls in information systems and determining security control effectiveness; the ISMS model requires that the ISMS be monitored and reviewed, and maintained and improved, with specific attention given to the effectiveness of controls. Guidance on implementing an ISMS is being prepared, which will address the regular review and checking that controls remain effective.

- The FISMA has further guidance addressing the certification and [authorization] of information systems;
  The ISMS model also provides both requirements and guidance in the area of certification of ISMS.

- Finally, the FISMA also calls for a 'Continuous Monitoring Phase'; which has the same basic goals and elements as would the surveillance and re-certification stages of formal ISMS certification, and hence this principle is shared.

Thus, the goals set by the FIP are largely satisfied by the general principles of the ISMS model, which gives rise to optimism with regard to their alignment.

D. The differentiators

One area of differentiation between FISMA and ISMS is the actual grouping and specification of security controls in the respective standards. The NIST SP 800-53 (December 2006) provides a partial mapping of its controls into those in the ISMS model (addressed further later in this paper.)

The more significant area of difference, and the more demanding to address, is the respective processes. 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 to the organization's missions and business functions**.** That assessment determines the effectiveness of the security controls employed within the organization's information system. Positive outcome of the certification assessment supports an agency management decision to

allow the system to be authorized and thereby to be issued an Authorization To Operate (ATO).

To summarize the ISMS process: Any decision to acquire formal certification is elective. Internal management decisions to accept residual risks, 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. When a formal certification is sought, the ISMS should have been operated through at least one revolution of the basic 'PDCA' cycle[4], i.e. there has to be evidence that the ISMS is in place and is being managed appropriately. Positive outcome of a certification audit leads to the ISMS being formally certified.

It will be apparent that there is some disjunction between these two approaches, principally being the requirement in the case of FISMA to have a certification assessment *prior* to receiving ATO, whilst the ISMS model requires that an internal decision to approve the management system is a pre-requisite to certification, and that a certification assessment can only take place once the system has been operated through at least one management review cycle (Figure 1), although internal review should take place as part of the pre-authorisation process.

Furthermore, whereas FISMA is more system-centric and takes into account the management environment, the ISMS model is more focused on the management system and the systems within it.

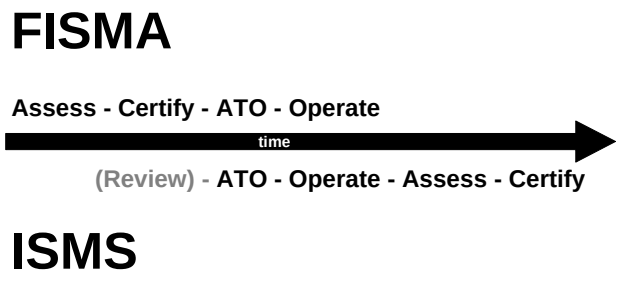

Figure 2 – comparative phasing of assessment stages

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 accreditation process determines that those accredited have the necessary additional competences to satisfy the 'national' need (i.e. the FISMA need), whilst also satisfying the obligations towards international mutual recognition of ISMS certifications.

E. A practical, driving, need

The Chairman of the Federal Public Key Infrastructure (FPKI) Policy Authority (PA) has tasked both Zygma and Enspier with activities which lead towards alignment of FISMA and ISMS in a way which will facilitate their use within the FPKI to demonstrate compliance with the many required Federal standards and other requirements. The FPKI PA will be coordinating its alignment work with NIST, to which it will offer its final product. This will allow NIST to consider the work for publication after ensuring that appropriate public review and vetting processes are conducted.

Because of its prominence as the international point of liaison for establishing cross-recognition on behalf of the United States with PKIs in other nations, and its internal role as the 'bridge' between PKIs within other governmental agencies, industry and academia, notwithstanding its sensitivity as a critical part of the nation's infrastructure, the FPKI stands to gain from having an ISMS certification. This certification would provide international recognition, industry recognition and compliance with the FISMA. The FPKI is today the leading organization within government pursuing this objective and driving the work required to achieve it, acting as the pilot for the realization of these goals.

IV. DEVELOPMENTS IN-HAND

A. ISMS research and development

Zygma's private research and development in the ISMS field has developed two models which are key to the ability to use an ISMS as the basis for demonstrating an organization's compliance with other reference sources. By reference sources we mean regulations (e.g., GLBA, SOX, FISMA), NIST or other international standards, etc. Zygma has developed a comprehensive two-way mapping of the HIPAA Security Standards against the ISMS requirements (published 2005). In the process of this mapping it became clear that certain HIPAA requirements simply were not met by the ISMS reference controls (i.e. the controls in Annex A of 27001).

[4] 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 usually getting the credit for its origination, it being known as the 'Deming Cycle').

A new concept, an additional set of controls referred-to as an Extended Control Set, was created to resolve this problem. A paper by Zygma in mid 2006 described this concept, providing a step-by step model which showed organizations how the idea could be adopted. More recently, a further paper has addressed how guidance for domain-specific implementations of an ISMS could follow common guidelines and a *pro forma* document provided, also embodying the Extended Control Set paradigm (2007). [5]

As a voting member of the US national body which reviews and contributes to (*inter alia*) the ISO/IEC 27000 family, Zygma is at the forefront of ISMS development in the US today. Much of Zygma's research and development has been accepted as US input material to the new guidance standards currently being drafted, and has subsequently been adopted by ISO as content for those documents.

This R&D effort has therefore built a basis which will serve a wide audience, not least those wishing to use an ISMS to fulfil their compliance obligations with respect to Federal regulations.

B. Mapping between FISMA and ISMS

This paper has already addressed the differences in the actual controls defined in each model. NIST SP 800-53 provides a table matching its security controls to those of various other standards, one of which is the ISMS model. The shortcoming of this comparison is that by performing it against the informative guidelines standard, it omits any cross-reference with the process and procedure requirements in 27001 (§4 to §8 inclusive) and fails thereby to address the full set of normative requirements for a complete ISMS.

Zygma has recently reviewed Appendix G of SP 800-53 under a Federal contract and created an entirely new proposed appendix, which not only maps the SP 800-53 controls against all of the normative requirements of 27001 but also provides a set of additional '27001-like' controls to address the fact that certain SP 800-53 controls simply have no direct equivalent in 27001. The appendix also provides a reverse mapping from the ISMS requirements back into the SP 800-53 controls.

The need for these additional controls is explained by the desire to use an implemented ISMS to show compliance with SP 800-53. Without the realization of these controls as an Extended Control Set (as previously described), full compliance with SP 800-53 could not be easily demonstrated.

Fortunately, the ISMS requirements positively encourage the implementing organization to create such additional controls as they may require, and this practice is entirely acceptable for the purposes of ISMS implementation and assessment for conformity.

C. Mapping between FBCA compliance and ISMS

One of the benefits from alignment of assessment processes is the opportunity to use a single assessment process to confirm adherence to multiple references (regulations, standards, etc.)

The Federal Bridge Certification Authority (FBCA) is a major component of the FPKI. As a part of an assignment to assist the FPKI Operational Authority (OA) with the implementation and operation of an ISMS (which is intended to act as the overall framework for the OA's compliance efforts) Zygma has mapped all of the present compliance points (in excess of 1400) to the ISMS requirements. This has provided mappings to at least 36 documents, not including all of those underpinning FISMA. This has proven to be an extensive, at times exhausting, process resulting in some 5,000 mappings in its raw state.

Following the approach devised by Zygma in its paper on Extended Control Sets, once operational, the OA's ISMS will allow the OA to have performed an assessment which will demonstrate its compliance to each of these requirement sources. This process alone will bring significant efficiencies since it has the potential to fulfil the triennial requirements for C&A assessment and for annual requirements from other quarters, including its own policy.

This will be accomplished by undertaking the ISMS assessment and using demonstrated conformity with each requirement to illustrate, by inference, compliance with the corresponding set of Federal requirements.

Building the OA's ISMS continues and is targeted at being operational before the 2008 annual reviews are scheduled, allowing formal certification to be based upon established operational experience. Having in place by June 2008 the mechanisms for enabling the formal ISMS certification to satisfy the FISMA C&A requirements is essential to allow the OA to gain the efficiencies this process will offer and to prove the process such that other organizations, within and without government, can benefit from these measures.

D. A Comparison of FPKI Policy Requirements and NIST SP 800-53 Security Controls

The Federal PKI Audit Working Group (WG) operating under the FPKI PA focuses on issues relating to audit

[5] Refer to Zygma's website for white papers on these subjects.

affecting the FPKI and entity Certification Authorities (CA) who are cross-certified with it. One of the issues currently being addressed by the group is how well Entity CAs implement security controls listed in NIST SP 800-53, as required by the FISMA.

To assist the Entity CAs in showing that they meet these requirements, Enspier Technologies was given an assignment to conduct a mapping between the FBCA Certificate Policy (CP) and SP 800-53. Since cross-certified entities must maintain policies that are compliant with the FBCA CP and must also undergo compliance audits to prove they are following those policies, the results of this mapping will be able to show which security controls listed in SP 800-53 are satisfied by a cross-certified entity which fulfils the compliance audit criteria.

The ability to reuse the FPKI-required compliance audit results to show how a majority of SP 800-53 security controls are met will save agencies and auditors significant time, money, and effort when C&A required by the FISMA is conducted.

Further development of this work under the proposed aligned assessment framework, will provide a thorough-mapping between the ISMS controls and the FBCA and hence provide the basis on which both FPKI and SP 800-53 controls compliance requirements could be satisfied simultaneously.

V. FUTURE WORK PLANNED

These current activities are paving the way towards making the assessment processes more cost-effective and more marketable, but substantial further work is required to formalize the FISMA-ISMS-FPKI CP alignment and to refine the principles espoused in this paper and others, and to prove them in a real-world system. Some specific steps can be identified from the foregoing.

The key issue is the alignment not of the controls but the processes of assessing the system and gaining approval. A prospective solution to this is to take the ISMS framework as the over-arching scheme and within that establish specific rules for ISMS development which accommodates the FISMA requirements.

In an ISMS assessment it is normal for documentation to be provided to the assessor(s) who then conduct a 'Stage 1' audit, basically a desk-audit. This essentially presumes that there has been management approval of the residual risks and consequently that the ISMS has been approved for operation. After resolution of any issues arising from that the Stage 1 assessment the 'Stage 2' assessment is performed at the ISMS-owner's location, actively examining records, sampling evidence, and observing operations including visiting different sites where appropriate.

It is conceivable that in the ISMS model a 'Stage 1α' assessment could be undertaken, effectively the FISMA C&A assessment, at the time at which the management acceptance of risk is given, thus coinciding with that decision, and potentially reinforcing it. That it would be undertaken by an external party rather than management directly would not be a significant issue so long as the outcome could be jointly approved. This would fulfil 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 process for accreditation (credentialing) of the assessors for this process may also need attention. From the theoretical point of view of the respective models, a FISMA-credentialed assessor could perform the Stage 1α assessment whilst the other two were performed by a separate ISMS-accredited assessor. From both commercial and practical standpoints however, this makes little sense, and it is therefore proposed that an 'add-on' to the ISMS accreditation be created, thus offering dual-accreditation.

VI. CONCLUSIONS

With the second phase of the FISMA Implementation Project just getting under way, and intending to address the issues of credentialing and assessment, the time is ripe to explore these opportunities to use an established and globally-accepted information security management and assessment process as the basis for resolving those needs. As the above would suggest, it is the authors' 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.

The ability to operate within a single assessment framework, using a single assessment process allowing agencies and private sector firms to demonstrate that their IT systems comply with multiple sets of criteria will provide significant benefit in terms of the internal effort required to operate the requisite management systems. By giving organizations the opportunity to use their ISMS as the fulcrum of their compliance system they will be able to reduce the costs of audit, both internal and external, save time and enjoy greater value of the resultant certification through its widespread recognition. The model developed by Zygma and now being adopted by ISO as the *pro forma* approach to showing how the ISMS

model can be used to implement its controls in specific domains supports this objective in a structured manner consistent with the application of the existing standards, both by implementers and assessors.

Such a framework will allow a single assessment of a system's information security management, showing a list of requirements with which the system is compliant – even though the list of requirements may be compiled from a variety of sources. For example, a system that is required to undergo a compliance audit by the Federal Public Key Infrastructure (FPKI) Policy Authority could use the results of that audit to show compliance with many of the requirements set forth by NIST SP-800-53 if there was a formalized process to recognize compatibility of requirements. (As previously stated, NIST SP 800-53A explicitly recognizes the efficiencies of re-using assessment results where they can be shown to meet the requirements of another system.)

We see challenges but no barriers – alignment of FISMA and ISMS is technically feasible and requires knowledgeable crafting to dove-tail the systems and produce a description of the processes required to have them work in a mutually-supportive fashion.

The end result will be an assessment framework which will satisfy government and industry, national and international, needs across many sectors. The developing set of domain-specific guidance being developed by ISO and IEC, and the model for describing such criteria developed by Zygma, support the inclusion within an ISMS of additional criteria which address other specific needs, such as the operation of Certification Authorities and SOX, HIPAA compliance etc.

This, being based upon a consistent set of reference controls, will give greater confidence in an organization's information security management system's effectiveness for all its stake-holders.

VII. Acknowledgements

The authors wish to acknowledge the following colleagues for their time and wisdom applied in reviewing this paper prior to its completion, and to their encouragement and support for the work described herein, for which we are grateful. Nonetheless, any opinions expressed are solely those of the authors, who must assume responsibility for any errors or omissions.

Dr. Peter Alterman, Assistant CIO for E-Authentication, NIH; Chairman, Federal PKI Policy Authority;

Dr. Ronald Ross, National Institute of Standards and Technology, Manager of the FISMA Implementation Project.

VIII. References

[1] ISO/IEC 27001:2005, "*Information Security Management Systems - Requirements*", 2005-08.

[2] (US) Federal Information Security Management Act, 2002.

[3] NIST FIPS 200, "*Minimum Security Requirements for Federal Information and Information Systems*".

[4] NIST FIPS 199, "*Standards for Security Categorization of Federal Information and Information Systems*".

[5] NIST SP 800-53, "*Recommended Security Controls for Federal Information Systems*".

[6] NIST SP 800-37, "*Guide for the Security Certification and Accreditation of Federal Information Systems*".

[7] NIST Special Publication 800-53A "*Guide for Assessing the Security Controls in Federal Information Systems*".

[8] ISO/IEC 27002:2007, "*Information Security Management Systems – Code of practice*", 2007-04 (formerly ISO/IEC 17799).

[9] ISO/IEC 27006, "*Requirements for bodies providing audit and certification of information security management systems*".

[10] *Joint Economic Committee of the US Congress report "SECURITY IN THE INFORMATION AGE", May 2002.*