Making Sure of Security: Contrasting FISMA and ISO/IEC 27001

Fiona Pattinson

March 2010

Version 2.0

Background

Information security assurance is a topic that has developed significantly over the past few years.

Drivers for Information security assurance include: the rapid development and adoption of computers and related technology as evidenced by Moore's law during the information revolution of the last century, the connectivity and Internet revolution, the emphasis on critical infrastructure that continues to be emphasized as part of Homeland security, the increased emphasis on corporate governance, and the increasing awareness of security and privacy matters as society realizes the dangers presented by its Information Technology (IT) advances, as well as increasing legislation and regulation mandating it's consideration.

Several security standards have been developed in the last decade to address the management of these technologies, and the needs surrounding them. Not surprisingly, given the rapid development of the technologies that they seek to govern and the slowness of standards development, they were positioned in a somewhat eclectic way.

More recently, standards bodies have been making efforts to rationalize and update the the maturing security standards suites..

In this updated paper we present a discussion that should clarify the key factors, and the different areas of strengths of the two frameworks that have emerged as the most relevant to the U.S. i.e.:

- the standards often used by Federal agencies to meet the FISMA requirements that have been developed by NIST and

- the standards developed internationally that are published by ISO/IEC and adopted by many commercial organizations In the ISO/IEC 27000 series.

Both of these standards provide a general framework for managing IT security.

We note that other standards such as the Payment Card Industry Data Security Standard (PCI DSS) are also now widely used in the U.S. but these restrict their focus to particular information assets and so in practice must be integrated with another more general framework in order to meet the real-world requirements of an organization needing to protect all of their assets.

A quick review of the much used and often misused term "security assurance" reminds us that security assurance is just that. An assurance, or a level of confidence that things are as we said they should be. There are no absolutes. There is no such thing as perfect security. All we can offer is the ability to make an assessment of how likely it is that things will go wrong, and spend varying, yet hopefully appropriate, amounts of money trying to make sure that things do not go wrong.

An Information Security Management System (ISMS) is concerned with a holistic view of information security. Every product, such as a cryptographic module, a firewall, or a database application, makes fundamental assumptions about the environment in which the product is developed and operated, or in which a system is integrated, configured, and operated. It aims to identify the vulnerabilities and threats potentially affecting the assets within the scope, and to identify the controls which are the safeguards that will reduce the risks to the organization's mission. If the environment on which an assurance is made is lacking, then so you lose assurance that you have gained from using a certified or accredited product or system.

The ISMS described by NIST was developed in response to the Federal Information Security Act of 2002 (FISMA). FISMA grew from the need for US government agencies to meet the requirements of US legislation. Applicable to all Federal information systems other than those systems designated as national security systems, as defined in 44 U.S.C., Section 3542. The

standards suite and framework were developed by NIST as other standards were not available at the time that adequately met the needs of the legislation. The system is focused on ensuring that the information systems used in government agencies are secured properly and that, where appropriate, the IT systems are accredited (authorized) by people in authority within the agency where they are operated.

The other ISMS discussed is the international standard ISO/IEC 27001 that emerged from the BS 7799-2 standards. Internationally, the commercial-world uses ISO/IEC 27001 as the framework of choice for independently assessing and communicating assurance of an organization's Information Security Management System (ISMS). Currently nearly 5000 organizations have certified their ISMS and their systems within the defined scope.

These two different frameworks enjoy different focus and emphasis and an understanding of this is important in understanding the relationships between the two frameworks.

Focus

Here we compare how the two differ in some fundamental aspects.

The scheme developed by NIST is used by Federal Agencies, their contractors and those involved as part of the critical infrastructure including utilities (electrical, nuclear, gas and oil, dams), transportation (air, road, rail, port, waterways), Public Health Systems/Emergency Services, Information and Telecommunications, National Defense, Banking and Finance, Postal and Shipping, Agriculture/Food/Water, and the Chemical industry in order to meet their mandatory requirements under the act. To date a great many systems have been certified and accredited under the scheme.

The suite of FISMA standards is close to completion and includes a risk assessment methodology (SP 199) and a detailed controls list (SP 800-53A) with objective assessment criteria (SP 800-53a). Originally it was characterized as adopting somewhat of a "bottom up" approach as the technical focus is firmly on the operational and technical aspects of the IT system. The focus of the framework is on the IT systems, and on their certification and accreditation to operate.

- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information System

- FIPS Publication 200, Minimum Security Requirements for Federal Information and Federal Information Systems

- NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*

- NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems

- NIST Special Publication 800-30, Risk Management

- NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems

- NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems

- NIST Special Publication 800-59, Guide for Identifying an Information System as a National Security System

- NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories

As the FISMA related standards and guidelines have matured they have emphasized the importance of a risk management framework that can be used to augment the baseline control set approach.

On the other hand, the ISO/IEC 27001 standard is aligned with ISO/IEC 9001 (the Quality Management System) and draws from the lessons learned in the career of that standard, meeting needs in the non-Government arena for scalability and needs to ensure that an organizations management system meets a basic best-practices management system. Its paradigm is, that by ensuring that the organization has an appropriately defined risk management process and assessment methodology, then the treatment of identified risks will mean that appropriate controls can be applied and hence assurance can be gained that the organization's systems are also properly secured. This standard focuses on making sure that the organization has a management system that is capable of managing information security, a necessary approach for the non-government arena where a very wide variety of organizations need to be serviced. Hence, it adopts more of a "top down" approach.

The standards included in the ISO/IEC 27000 family include:

- ISO/IEC 27000 Fundamentals and principles
- ISO/IEC 27001 ISMS requirements
- ISO/IEC 27002 Security controls (Code of Practice for Information Security Management)
- ISO/IEC 27003 ISMS implementation guidance
- ISO/IEC 27004 Information security management metrics and measurements
- ISO/IEC 27005 ISMS risk

Applicability

The FISMA and the standards supporting it are mandatory to US government agencies, and are also referenced for agency contractors in the Federal Acquisition Regulations. It is not formally recognized outside the U.S. National security systems and the CIA are not mandated to use the FISMA related standards produced by NIST.

ISO/IEC's 27000 framework is voluntary and applicable to large and small organizations. It is an international standard approved by over 60 different nations. A mutual agreement is in place between several accreditation agencies with the goal of ensuring conformity in assessment around the world.
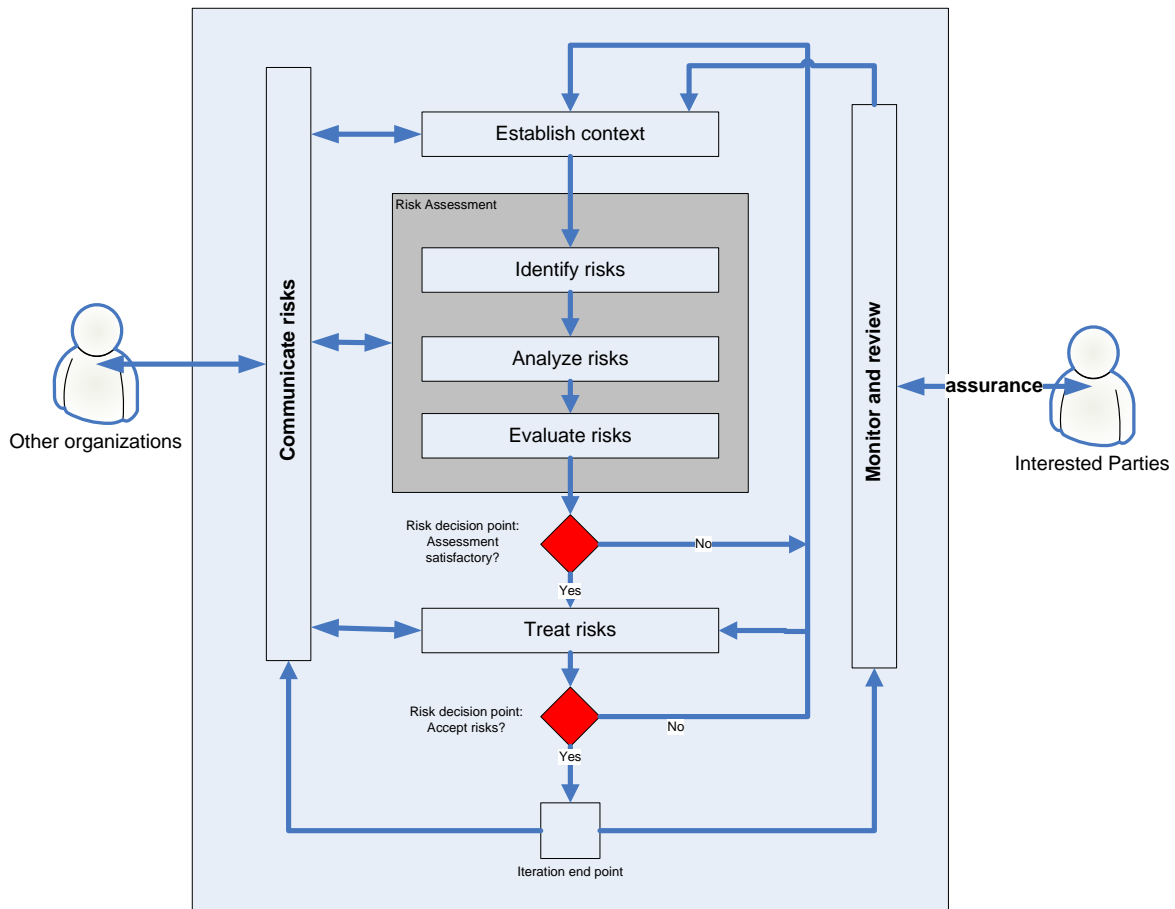
Boundaries

The boundary described by the FISMA related standards is an IT system or group of systems (and extends to include the organization which controls the systems). For ISO/IEC 27001 the "scope" (or boundary) is typically an organizational unit and includes the systems for which that unit is responsible and has control over. This of course amounts to much the same thing, but belies the history of the standards as the FISMA standards were originally very system focused/oriented often leaving organizational matters outside the boundary.

Risk Management

No matter what the particular needs for information security of an organization are, and whatever the recipe for information security adopted, a risk management process is central to information security assurance.

The FISMA standard suite includes all the elements of the risk management process that must be used. The risk management process is described at http://csrc.nist.gov/sec-cert/risk-framework.html

Establish context

Risk Assessment

Identify risks

Analyze risks

Evaluate risks

Communicate risks

Monitor and review

Other organizations

Interested Parties

assurance

Risk decision point:
Assessment
satisfactory?

No

Yes

Treat risks

Risk decision point:
Accept risks?

No

Yes

Iteration end point

Figure 1 A basic risk management process

Establish Context

Establishing the context for risk management is an important step.

ISO/IEC 27001 achieves this through ensuring that the scope of the management system is well defined, the organization's management are properly involved, and ensuring that the legislative and regulatory framework is considered up-front.

With the FISMA standards the scope is equally important, but for the published standards designed to be applicable to government agencies at least some of the organizational context is pre-defined, (a Federal Agency!) and the focus is very much on meeting the requirement of the Federal Information Security Management Act.

Risk Assessment

Because of the differences in the focus of the frameworks, and the boundaries of the problem there are some differences in the assumptions that are made by each framework about the risk assessment methods adopted.

In fact, when we consider an organization as a whole we generally see several assessment methodologies in use within a single organization. Consider a typical organization that needs to effectively manage:

- Business risk, perhaps managing currency fluctuations, market and industry vulnerabilities
- Project risk, focusing on the efficiency and effectiveness of particular projects
- Information security risk, often called out as a separate entity
- Product/Service development risk, managing the risks inherent in the offering. That perhaps, if realized, may affect the customer of the organization rather than the organization directly.

The way that this is often dealt with is to tailor the risk assessment methodology to meet the needs of the organization.

Often each "C" level organization will affect its own assessment methodology, and we note the concomitant needs for communication of risks between these areas.

There are literally hundreds of defined methodologies and tools, and often an organization develops its own methodology that is tailored to match its emphasis and needs. Whatever the risk, assessment methodology or tools selected, the basic risk management process remains the same.

ISO/IEC 27001, with focus on organizations, defines the attributes of a high level risk management process. It does not provide a specific risk analysis or risk assessment method.

The FISMA ISMS framework can make some assumptions about the organization in which it operates (The U.S. government) and has focus at an IT system level. It can afford to not only prescribe a risk assessment methodology (FIPS PUB 199) but also to prescribe at least some of the risk assessment which is given in FIPS PUB 200.

Risk Treatment

Risk treatment includes all the actions that may be taken to reduce risks. It includes risk transference, avoidance, acceptance, and the application of selected controls (also known as safeguards). There has recently been a lot of excellent work performed on the subject of controls. These standards document a best-practice activity that if correctly chosen and applied can contribute to risk reduction activities. Simple examples are performing backups, carrying out background checks on personnel, or using a virus scanner. Of course the control lists are inevitably long and not comprehensive.

- For the ISO/IEC 27001 framework, the control list is given in ISO/IEC 27002.
- For the FISMA framework, the list is given in NIST's SP 800-53. (currently Revision 3)

Both are the results of hundreds of expert man-years work. Note that NIST's SP 800-53 also provides a mapping to the ISO/IEC 27001 control set.

Communicate Risks

Communicating risks is an important part of the process. Identifying the correct audience is an important part of this. In the FISMA system, this is clearly defined as the accreditor and through the reporting process to the OMG. The risks are reported to the accreditor through the certification report.

The audience is defined similarly by the ISO/IEC 27001 standard. The standard defines the need to communicate (and seek acceptance of) residual risks to the "management". Once this is done permission to implement and operate the ISMS is sought from "management".

Baseline Approach

The FISMA framework differs significantly from that of of the ISO/IEC ISMS framework in it's specification of baseline control sets. The risk management framework proscribed includes categorizing the systems and the information they contain into low medium or high impact according to FIPS 199. It then provides a minimum set of controls to protect them. These can be augmented or added to as a result of the risk assessment for the systems at hand, but they must implement the minimum set. ISO/IEC 27001 does not use such a concept, and the entire control set applicable to a system is driven by the risk management process.

Certification and Accreditation

This is a subject area that requires careful navigation, as in some cases the same terms are defined differently in each framework.

System: In FISMA the term is used to refer to an IT system. This is the subject and focus of the certification.

"A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

In the ISO/IEC 27000 ISMS framework, the term *system* generally refers to the management system, although it may also be used to refer to an IT system.

Certification: In the FISMA model an IT system is certified by assessors who have audited the IT systems compliance with the standards and the implementation of the appropriate controls. A certificate is issued attesting to the correct implementation of the controls specified to protect the IT system in question.

"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."

In the ISO/IEC 27001 ISMS frameowrk, the term *certification* is used when an independent 3rd party certification body makes the assurance that the entire management system is conformant with the standard. A certificate is issued attesting to the management systems conformance to the standard.

Accreditation: In the FISMA scheme the term *accreditation* is used to indicate that the system has been certified and approved for operation. The IT system is accredited for operation.

"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"

In the ISO/IEC ISMS framework, the term *accreditation* is used to indicate that a certification body has met the standards of an accreditation body such as, in the US, ANAB.

The assurance gained from participating in a scheme that is ensuring conformance to the standards is not drawn solely from the *security* of the system in question but is also related to the trust and reputation of the people and organizations making the assurances. In the FISMA

framework as applied to the U.S. Government, the trust is derived from the U.S. Government. For the ISO/IEC 27001 scheme, the trust is derived from the accreditation agency.

Look for independence in your providers of assurance as well as third-party measures of the organizations competence. If there is a vested interest in the outcome then you should consider if it is appropriate that your confidence should be reduced.

The role of accreditation agencies for the ISO/IEC 27001 standard is to accredit the organizations performing the conformance audits, the "Certifying Bodies" (CBs). The CBs must be able to be trusted by their clients that the claims they make about an organizations management system are objective and trustworthy. A competent operational accreditation agency in the U.S. has been late to emerge and instead U.S. based CBs have turned to established and experienced accreditation agencies in Europe and other areas of the world in order to show their clients that they are trustworthy.

Integrating FISMA and ISO/IEC 27001

This is certainly technically possible. And there are a several methods and associated methodologies that can be used (See Karapetrovic & Jonker). The selection of these methods is dependent on the goals of the integration and of course to the stakeholders involved.

Two basic strategies can be adopted, either one of alignment or one of full integration and each has its advantages and disadvantages. Full integration is harder to achieve but maximises the benefits of reuse of processes such as training, measurement, document and record management etc.

Considering the different strengths of each of the frameworks, a non-government organization that needed assurance for its high or medium impact systems might well benefit from adopting the FISMA standards as the basis of their ISMS, while commercial organizations, perhaps a contractor of a US Government, could equally well find that the ISO/IEC 27000 ISMS framework is the best basis for their organizational solution.

It is imperative that the organizational management system meets the basic standards and it should of course be remembered that the assessors of each framework do need to make their own independent determination of compliance.

Conclusion

Both the FISMA and ISO/IEC 27000 ISMS frameworks have been discussed and the differences and similarities discussed. Both are maturing frameworks and actively maintained by their relevant standards bodies. The FISMA framework is unlikely to be of relevance outside the mandates provided by the US legislation whilst ISO/IEC is an international standard that can be relevant globally, and is often used by organizations with a global or international presence.

It may be appropriate for some organizations to consider conformance to both frameworks and a brief discussion of this topic has been provided.

References

Federal Information Security Management Act of 2002 (Public Law 107-347, Title III), December 2002.

Further Information

The standards that form the FISMA framework are available free of charge from NIST at http://csrc.nist.gov/sec-cert/

Standards in the ISO/IEC 27000 family are available from ISO standards selling organizations including ISO at www.iso.ch and from ANSI at www.ansi.org

The FISMA project web site is at http://csrc.nist.gov/sec-cert/

The International User Group for 27001 is at http://www.xisec.com/

ISO's booklet "The integrated use of management system standards"

ISBN 978-92-67-10473-7: http://www.iso.org/iso/pressrelease.htm?refid=Ref1144

Karapetrovic, S. & Jonker, J. 2003, 'Integration of standardized management systems: searching for a recipe and ingredients', Total Quality Management & Business Excellence, vol. 14, no. 4, pp. 451-460.

Wilsher, R,G, "Federal Information Security Management Act and its harmonization with ISO/IEC 27001' available from http://www.zygma.biz/FISMA.cfm