

Information Technology Standards and Practices for Local Governments

September 2007

Introduction

Historically, organizations sometimes struggled to bring their information technology goals into alignment with their business goals. This alignment would allow the organization to promote their IT function from the status of a utility to that of being a strategic partner in the attainment of the organization's Strategic/Business Plans. More recently, state and federal legislation has forced organizations to address this very issue, albeit, indirectly. These regulations focus primarily on managing risk, but include guidelines that ultimately lead to good IT goal alignment and operations. This paper will review a number of these guidelines, including those most appropriate for local governments, and show how they can strengthen the IT function.

Organizations of all types, including municipalities and special districts, are finding value in the use of an information technology guideline or framework to standardize and focus operations. Federal government agencies are now required to be in compliance with the Federal Information Security Management Act (FISMA). The main FISMA guideline, the National Institute of Standards and Technology (NIST) Special Publication 800-30, Risk Management Guide for Information Technology Systems, provides a foundation for the development of an effective risk management program. The ultimate goal is to help organizations to better manage IT-related mission risks.

The reason this works so well is because the selected controls must extend to electronic financial systems, the human resources, and the information technology infrastructure surrounding that organization's data. The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization. The framework is a great vehicle for keeping the focus of the IT risk management process broad enough to be effective, and assure that good security is good business.

Choosing a Standard

Local governments are left to fend for themselves when trying to determine which IT standards framework to use. This holds true especially for cities, special districts, and college districts which are not subject to a single authoritative body, law or regulation prescribing which IT standard to adopted. The IT standards are inconsistent, the sheer number of different standards available to choose from is confusing, and few are directly associated with the growing list of mandatory regulations that even local governments are required to comply with. Few organizations have sufficient time to evaluate each standard to determine which one would best meets the government's business needs.

This paper reviews the various standards IT organizations have to choose from and how some of those can work together to create a world-class IT function within government of any size.

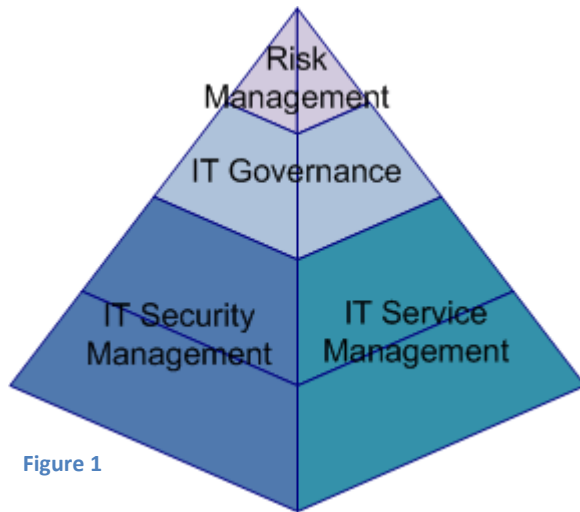


Figure 1

Organizational Framework

At the highest level, an effective framework must focus on risk, be an integral part of the organization's executive strategy, and translate this into manageable terms for day-to-day operations. The relationship of these steps of a top down approach from the more general to the more specific, is illustrated by the pyramid model shown in Figure 1. When selecting any set of IT standards it is important that it be based on business goals, objectives and risks. At the top, risk management helps protect the business and enable the business to achieve its goals. Senior management's risk management activities help set the tone for the entire

organization. Under this concept, management selects which risks they deem acceptable, which risks they deemed unacceptable and identify and implement which mitigation controls will be used to lower unacceptable business risks to an acceptable level. The risk management framework, used by senior management, should span the entire organization and not be specific to only information technology.

Focused on real risks derived from the organizational-wide risk management program, management then uses an IT governance program which specifically handles these risks as they relate to IT. Using the top-down approach to a risk management program, and using a formal IT governance program, assures management is focused on the most significant risks within the IT infrastructure.

The IT governance then feeds into two areas; IT security management and IT service management. The IT service management's portion deals with how services are delivered. The IT security management portion deals with required controls used to maintain the confidentiality, integrity and availability of the information and technology. It is important that the security controls are managed independently from the services. This enables the segregation of duties, itself a fundamental control and a function on which other controls depend.

Committee of Sponsoring Organizations of the Treadway Commission (COSO)
Website: www.COSO.org

Formed in 1985

Objective: to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence.

Established a common definition of internal controls, standards, and criteria
Sponsored and funded by the following associations and institutes;

American Institute of Certified Public Accountants (AICPA),
American Accounting Association (AAA),
Financial Executives Institute (FEI),
The Institute of Internal Auditors (IIA)
The Institute of Management Accountants (IMA)

Government Finance Officers

Association (GFOA) recommendation to use COSO:

http://www.gfoa.org/services/rp/documents/rpic_040204.pdf

From the IT security and service management, will come the more specific business procedures and processes guiding the day-to-day operations. Thus the day-to-day operations and procedures support the IT security and service management, which then supports the IT governance that supports the organizations risk management activities, which enables the achievement of overall goals and objectives of the local government. This top down approach ensures that IT operations are properly aligned with business goals and objectives.

Now let's see how the respective standards compare to this general process.

Standards On The Pyramid

Using the pyramid model and overlaying the various standards that are followed in the IT industry today, it becomes clearer how they work together and relate to each other. Figure 2 is an illustration of the placement for each of the standards based on their key focus.

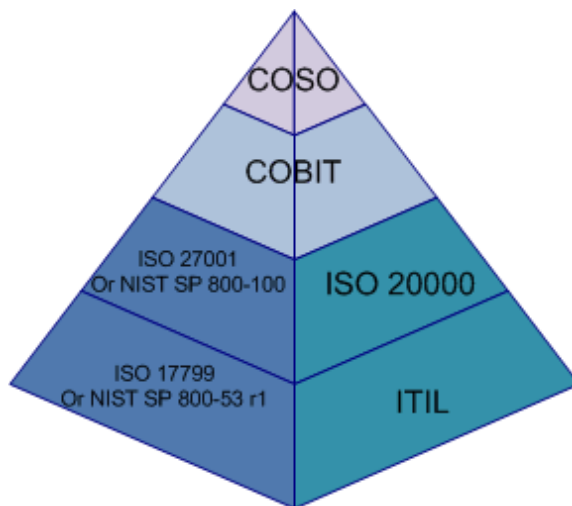


Figure 2

Risk Management

The framework most focused on Risk Management is known as COSO, named after the creators, the Committee of Sponsoring Organizations of the Treadway Commission. The framework is made up of five interrelated components: (1) the control environment, (2) risk assessment, (3) control activities, (4) information communication and (5) monitoring. The COSO framework is specifically designed to address the factors that cause fraudulent financial reporting; however, in 1992 it was broadened to include proper

ISACA, ITGI, CobiT & Val IT

The Information Systems Audit and Control Association (ISACA) was founded in 1967 as the global organization for information governance, control, security and audit professionals, with over 65,000 members, in over 140 countries.

Website: www.isaca.org

The IT Governance Institute, founded in 1998 and established by ISACA as a research think tank that exists to be the leading reference on IT-enabled business systems governance for the global business community.

Website: www.itgi.org

CobiT Supports IT governance objectives, helps ensure that IT processes are defined and assigned, helps to ensure that there is focus on control objectives and leads to more cost-effective IT services.

Val IT seeks to insure business gets a value from IT investments.

Four main questions ask by Val IT:

1. Are we doing the right things?
2. Are we doing them the right way?
3. Are we getting them done well?
4. Are we getting the benefits?

Information on CobiT and Val IT can be found on the IT Governance Institute website www.itgi.org.

ISO

International Standards Organization (ISO) is a non-governmental global organization established in 1947 that works to develop standards across goods and services by providing a means of verifying that a proposed standard has met certain requirements for due process, consensus, and other criteria by those developing a standard.

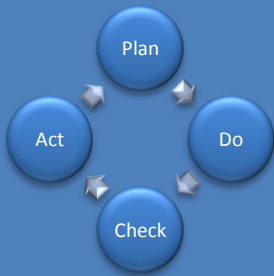
Website: www.iso.org

IT Infrastructure Library (ITIL)

Website: www.itil.co.uk

PDCA

ISO 20000, ISO 27001 and ITIL use the familiar plan-do-check-act (PDCA) approach so, there is greater integration between the standards. Each standard places processes under one of the four phases of the PDCA model. In this way you can apply multiple standards easily.



The IT Governance Institute in the UK Office of Government Commerce have future plans to align CobiT & ITIL with common terms for greater integration. There are a multitude of whitepapers on guidance and mapping for integration of CobiT and ITIL such as "Guidance on Aligning CobiT, ITIL and ISO 17799" in The Information Systems Control Journal (Vol1, 2006).

governance of assets and internal controls related to any aspect of the financial system, which includes the IT infrastructure.

Is COSO an appropriate framework for local governments? Good business practice requires selecting an internal control framework and a risk management process. So, yes it is. But isn't COSO too elaborate for local governments? No, the Government Finance Officers Association specifically recommends the use of COSO for local governments. In addition, any organization receiving federal funds is required by OMB A-133 to establish internal controls and it specifically mentions COSO as an appropriate means to establish internal controls. For guidance on implementing COSO in a small organization see The "COSO *Guidance for Smaller Public Companies*", available on the COSO website. Whether a local government or a multi-national corporation, following COSO can enable organizations to demonstrate due diligence and still meet their goals and objectives.

IT Governance

The most common framework or best practice used to implement IT governance for COSO is CobiT (Control Objectives for Information and related Technology). Created in 1992 by the Information System Audit and Control Association (ISACA) and the IT Governance Institute, CobiT (currently in version 4.1) defines 34 IT processes with 214 specific detail control objectives. Each process has indicators, measures, and best practice recommendations for developing appropriate IT governance.

ISACA also produced the Val IT framework, which integrates CobiT with control objectives, to ensure proper IT investment governance (getting value from your information technology). Together, the frameworks ensure information technology has controls and brings value to the organization. COSO, CobiT, and Val IT framework control objectives are very high level and do not have specific procedures written into them. Other frameworks or other standards provide specific IT service management and IT security management implementation procedures at lower levels.

IT Service Management

The IT service management framework defines and enables the desired level of service to assure reliable business critical applications

and IT infrastructure. In the IT service management world there are two complementary standards: first is ISO 20000, developed by the International Standards Organization and IT Infrastructure Library or ITIL, developed by United Kingdom Office of Government Commerce.

ITIL is the most widely accepted approach to IT service management in the world today. ITIL has a comprehensive set of practices that are well-defined, and drawn from public and private sectors from around the world. ITIL is further divided into service delivery and service support. IT services benefit from ITIL by: more customer focused quality, better managed costs, and the development of a clear and efficient IT structure. With ITIL, it is easier to manage IT processes as they become standardized and integrated, creating a demonstrable and auditable process.

ISO 20000 exists at a higher level than ITIL and was developed to give organizations the ability to certify by an external independent party that there is an IT service management framework in place. Basically, the certification demonstrates that an ITIL framework has been implemented. The only need for certification would be if a third-party relied upon the service provided by the organization, and the third-party needed a level of assurance. If there are no third parties asking for certification, there would be no need to implement ISO 20000.

IT Security Management

For IT security management there are two competing sets of standards; ISO standards such as ISO 17799, and special publications by the National Institute of Standards and Technology (NIST).

First published in 2000, ISO 17799 is the oldest and most recognized ISO standard in information technology security. The current version was updated in 2005, and will be updated again and renumbered to ISO 27002. Currently, ISO 17799:2005 is divided into 11 sections with 133 different controls. ISO 17799 is a code of practice, and as such, listed elements are not mandatory but instead are recommendations for possible controls to be implemented based upon identified risks.

ISO 27001 was developed after ISO 17799 and serves the same purpose ISO 20000 does for ITIL it defines an audit process which enables and organization to become ISO 17799 certified.

The other set of competing standards is the National Institute of

NIST

The National Institute of Standards and Technology (NIST) is the standards-defining agency of the US government, formerly the National Bureau of Standards, a non-regulatory agency of the United States Department of Commerce. The NIST mission is to advancing American economic growth through the use of technology. NIST is responsible for developing IT security standards for federal agencies.

Publications:

<http://csrc.nist.gov/publications/nistpubs>

“The FISMA Implementation Project was established in January 2003 to produce several key security standards and guidelines required by Congressional legislation. These publications include FIPS 199, FIPS 200, and NIST Special Publications 800-53, 800-59, and 800-60. Additional security guidance documents are being developed in support of the project while not called out directly in the FISMA legislation. These publications include NIST Special Publications 800-37, 800-53, and 800-53A. It should be noted that the Computer Security Division continues to produce other security standards and guidelines in support of FISMA.”

Source: <<http://csrc.nist.gov/sec-cert/>>

National Technology Transfer and Advancement Act (NTTAA)
<http://ts.nist.gov/Standards/Conformity/nttaa.cfm>

OMB Circular 119-A
<http://www.whitehouse.gov/omb/circulars/a119/a119.html>

Standards and Technologies Special Publications (NIST SPs) in the 800 series. These standards were created by the US government primarily as guides for other federal agencies, but are useful for any organization including corporations, governments and nonprofits. In 1996 the National Technology Transfer and Advancement Act, Public Law 104-113, was passed, which requires NIST to coordinate federal, state and local government technology standards activities, and recommend to them the adoption of NIST standards for federal, state and local governments. OMB circular A-119 gives a number of reasons why voluntary use of these standards is good for governments, including lower cost, wider acceptance, efficiency, and a set of government friendly standards.

In 2002, the Federal Information Security Management Act, also known as FISMA, was passed as part of the E-Government Act of 2002. FISMA is designed to bolster computer network security within federal government agencies and affiliated parties and requires the adoption of NIST standards for federal agencies. Further, the act requires that any third party who transmits, stores, or processes data owned by federal government agencies to adhere to the NIST standards.

The FISMA framework, outlined by NIST, requires a certification and accreditation process before a system can come online. This process is outlined at a high level in the NIST SP 800-100 and NIST SP 800-37. Certification and accreditation is a methodology used to ensure that controls are established for information systems, the controls are functioning as expected, and management has authorized the system to operate. The control catalog in NIST SP 800-53 rev. 1, outlines specific controls to implement, based upon the risk level of the system, in order to preserve the confidentiality, integrity and availability of the agency's data.

Many state agencies and non-government organizations that are processing, storing or accessing data owned by a federal agency are now required to become FISMA compliant. Private companies with federal contracts are now being required to be FISMA compliant. Local government agencies will most likely see FISMA requirements coming soon. If a local government does not have a security framework in place and is looking for one, they may wish to get ahead of the game and implement FISMA and begin realizing the benefits sooner.

Compulsory Standards

There are several other standards which are compulsory in nature. If your organization processes credit card information, the payment card industry requires you to follow their Payment Card Industry (PCI) data security standard. If the organization fails to follow the PCI data security standard, fees for processing credit cards will increase, the organization will be subject to fines, losses of cardholders and banks, and potentially losing the privilege to process credit cards. Some states have made the PCI data security standard law for organizations that process credit cards.

“The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The PCI Security Standards Council’s mission is to enhance payment account data security by fostering broad adoption of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.”

Source: www.pcisecuritystandards.org

There are a number of other laws which require protection of certain classes of information. For example, information about someone's health care is protected under the Health Insurance Portability and Accountability Act (HIPAA). Another example is the California Breach Disclosure Act. This law was enacted to protect consumers and citizens from damages caused by exposure of personal information and organizations suffering a security breach or suspected breach are required to report exposures to all those persons affected. Organizations properly protecting this type personal information with encryption are exempt from this reporting requirement.

Local governments face additional regulations unique to their specific function. For example college districts or school districts are charged with protecting the privacy of students as a result of the Family Educational Rights and Privacy Act (FERPA). Another regulatory example is The Biosecurity Act of 2002, which requires

water districts and water companies to perform a vulnerability assessment and to implement physical security and cyber-security for their SCADA systems. Recent changes to the Federal Rules of Civil Procedures effect how the organization’s IT group can comply to new guidelines to preserve legal status in law suits and defend themselves in a court of law.

For local law enforcement the U.S. Department of Justice in the “*Law Enforcement Tech Guide for Information Technology Security*” published in 2006 recommends the NIST framework for local law enforcement. Although FISMA compliance is not required for access to the Criminal Justice Information System (CJIS) or the FBI National Crime Information Center (NCIC) at this time, however, the NIST standards that make up the FISMA Framework are recommended guidelines.

Compliance with these compulsory standards and laws can be difficult to achieve and confusing. However, with the proper IT governance framework, an organization will ensure it can quickly and efficiently adapt to any new legislation or multiple compulsory standards.

Conclusion

After review of the various standards, regulations, and guidelines, it becomes evident that no single standard will suffice for the needs of local government organizations. Likewise, not all of the available standards are applicable or appropriate. What is required is a judicious combination of standards. The pyramid model shows the relationship of these respective standards.

It is recommended by Government Finance Officers Association for local governments to implement COSO as an internal risk management framework. Even without their recommendation it is a good business

Microsoft Operations Framework (MOF) was designed to give business a actionable and prescriptive way to implement ITIL in their organizations.
Website: www.microsoft.com/mof

practice and the best place for local governments to start. With a top down approach CobiT is best suited for an internal IT governance framework that suitably supports the adoption of operational standards.

For IT service management ITIL is the clear choice. Industry leaders, such as Microsoft, have adopted ITIL as the preferred service management standard and other industries have started to adopt ITIL as well. There is no need to implement ISO 20000 unless

required to independently prove that IT service management is in place and effective.

For IT security management there are two choices, however there is a growing push for local and state governments to adopt the NIST framework developed for FISMA. If state or local governments are forced to adopt an IT security standard it would most likely be the NIST framework used for FISMA. The NIST framework is already recommended for local police stations by the U.S. Department of Justice. Although OMB Circular 130-A requires security for organizations who receive federal funds, it does not specify the security standard. All federal agencies already require contractors to be FISMA compliant. It is logical that federal funding will likely soon be tied to FISMA compliance.

There is a growing group mandatory compliance requirements, such as PCI, HIPAA, and the California Breach Disclosure Act. Compliance with these and future requirements does not currently depend on or require specific standards, but is easier to achieve if there is a proper IT security framework in place and it is not that hard to implement the standards discussed in this whitepaper.

This white paper has hopefully illuminated some of the differences among the various IT standards and cleared up some of the confusion about which ones apply. Local governments need to adopt a set of standards that help achieve regulatory compliance in an affordable and effective manner and prepares for the likely inevitable requirement to become FISMA compliant as well.

Additional Resources

We have an additional paper available that shows the alignment between the Municipal Information Systems Association of California's (MISAC) Excellence in Information Technology Practices and some of the various standards in use today. In addition the California County Information Services Directors Association developed the *California Counties "Best Practices" Information Security Program* in 2002. The series of documents are great for templates for procedures and policies.

Municipal Information Systems Association of California (MISAC)
Website: www.misac.org

California County Information Services Directors Association (CCISDA)
Website: www.ccisda.org

For additional whitepapers, presentations and resources check out our website at:
<http://www.mazeassociates.com/resources.htm>

About the Authors

Donald E. Hester

Donald's clients include local municipalities, non-profits, corporations and federal government agencies, specializing in a wide array of compliance programs and security assessments such as PCI, FISMA, COBIT and ISO17799. He is a Guest lecturer and speaker on security topics and he has served on various advisory committees and as a Subject Matter Expert in Information Technology and Security. Donald received his bachelors, with honors, in Security Management with a concentration in Information Security from American Military University. He has over 15 years of experience in the security field. His certifications include; CISSP, CISA, CAP, MCT, MCSE Security, MCSA Security, MCDST, Security+ and CTT+. Donald also teaches Microsoft and information security courses at San Diego City College and for the California State Chancellor's office.

William Putman

William Putman has over thirty years of IT experience, starting with punched card tabulating equipment at U.C.L.A.'s Office of Academic Computing. He attained the corporate position of Vice President at Security Pacific Corporation (acquired by Bank of America) and is the former Information Security Officer at Irwin Home Equity Corporation. Ten of those years were devoted to information security related functions at the three organizations. William earned the Certified Information System Security Professional (CISSP) credential and has been consulting since October of 2000. His consulting expertise covers guest lecturer, information security instructor, and subject matter expert in information security management. His major clients have included NASA, Perot Systems, SecureNet Technologies, Irwin Home Equity Corporation, Think Security First/Walnut Creek Chamber of Commerce, and Maze & Associates. William is a Marine Corps veteran and devotes considerable time and effort to community, regional, and national civic/veteran activities.

Philip A. Bandy

Phil Bandy is a security professional with 17 years as both consultant and executive for major corporations, businesses and organizations. His practice specialty is protecting sensitive information and defending companies against cybercrime and disasters. Phil was the guardian for the 2006 election for the California Secretary of State and at Experian he managed security programs that still have an untarnished record of protecting the private consumer records of 280 Million Americans. He also was security officer for the team that built NASA's Mission Control Center. Phil has a background in Information Technology and provided security leadership and advice at Universal Studios, NIKE, Federal Reserve Bank, and Boeing. He holds a number of professional certifications, including the CISSP, CISM, CPP, and the NSA-IAM. He is active in various professional security organizations, author of numerous professional articles and public speaker on security matters.