



MARCH 2009

NASCIO Staff Contact:
Charles Robb
NASCIO Issues Coordinator
crobb@AMRms.com

Desperately Seeking Security Frameworks – A Roadmap for State CIOs

Introduction: The Complex IT Security Environment in State Government

The IT security programs in state governments have evolved and are administered within a context of dynamically shifting configurations of hardware, software, and network capacities, which increasingly are interwoven into a fabric that delivers government programs to citizens — what NASCIO has called the digital infrastructure. These programs have in common the goals of maintaining the integrity of the systems and data that deliver state government programs and services, but they vary significantly in their individual capabilities, administrative positions, and the strategies, policies, standards, and physical security those programs bring to bear to accomplish that aim. Additionally, there are significant differences in fiscal and human resources security programs have had available to them.

In the current environment, in which state IT resources are severely constrained due to budgetary shortfalls, state governments are being impacted by the infusion of massive federal stimulus funds from the American Recovery and Reinvestment Act of 2009. Formula and grant funds are flowing into states already, putting significant new pressure on state IT staffs to quickly and transparently deliver on business demands and the requirements of expanded or entirely new programs. The speed of these allocations and the sense of urgency regarding implementation will certainly create security risks as standard controls and compliance rules are under stress.

Against this backdrop, external security standards, regulations, and guidance have been developed or promulgated by a variety of standards-making bodies, organizations, and the Federal government. Some of the regulations, such as those imposed by the Health Insurance

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

Copyright © 2009 NASCIO
All rights reserved

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9153
Fax: (859) 514-9166
Email: NASCIO@AMRms.com

Portability and Accountability Act (HIPAA) or the Family Educational Rights and Privacy Act (FERPA), impact vertical lines of business and have limited relevance outside of that vertical, while being at the same time fundamental to the IT architectures and business practices of the agencies for which they apply. Other sets of standards are more general in nature and have broader application, though they may take significant resources in terms of time, staff effort, and money to implement and administer.

A **technical standard** is an established norm or requirement. It is usually a formal document that establishes uniform engineering or technical criteria, methods, processes and practices. (Wikipedia)

No single set of standards meets every security requirement and obviates the need for security professionals to continue monitoring and cross-walking a wide variety of security policy, standards, implementation guidelines, and controls. These standards themselves do not stand still. Neither does the landscape of threats to state systems and data. This creates a playing field within enterprise IT security in state governments that is uneven, sometimes confusing, and consistently challenging for security leadership.

This brief discusses key standards frameworks available to states, looks at examples of where and how they are employed or are already impacting states, and provides a map of the general regulatory terrain. While there is no “You are here” data point on the map, it is critical that state CIOs have general awareness of the environment’s complexity, the multiplicity of requirements that need to be addressed, and the trade-offs that exist between adherence to one set of standards versus another. Most fundamentally, the CIO has to develop a clear picture of the risks associated with implementing or not implementing a given set of security requirements.

IT SECURITY STANDARDS FRAMEWORKS

ISO 27001

ISO 27001, whose formal title is *ISO/IEC 27001:2005 - Information technology — Security techniques — Information security management systems – Requirements*, is an information security management system standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The standard is derived from British standard 1799, and for that reason the standard is frequently cited as ISO 17799. It is intended to be used in conjunction with ISO/IEC 27002, the Code of Practice for Information Security Management, which delineates security control objectives and recommends a range of specific security controls.

Organizations may be certified as compliant with ISO/IEC 27001 by a number of Accredited Registrars worldwide, although research did not reflect that any state program has sought certification.

As stated above, ISO 27001 is meant to be used in conjunction with ISO 27002, but both standards are part of the larger suite of security-related standards forming the 27000 series.

Organizations are increasingly adopting 27001 and 27002 due to the standards’ comprehensive approach to information security and the extent to which they provide a checklist covering “security policy, security organization, personal security, physical and environmental security, communications and operations management, access control, acquisition/development/maintenance of information systems, incident management, business continuity management and compliance.”¹

TABLE1: Security Standards (27000 series)

PUBLICATION	CONTENT	PRECEDING/ RELATED STANDARDS	STATUS
ISO/IEC 27000	Vocabulary for the ISMS standards		Under development
ISO/IEC 27001	Standard for ISMS	BS 7799-2	Published in 2005
ISO/IEC 27002	Code of practice for ISMS	BS 7799-1, ISO/IEC 17799	Published in 2007
ISO/IEC 27003	ISMS implementation guide		Planned for late 2008/early 2009
ISO/IEC 27004	ISMS measurements and metrics		Planned for mid-2009
ISO/IEC 27005	Standard for information security risk and management	ISO/IEC TR 13335-3 ISO/IEC TR 13335-4	Published in 2008
ISO/IEC 27006	Accreditation of ISMS certifiers	EA7/03, ISO 17021	Published in 2007
ISO/IEC 27007	Guideline for auditing of management system	(ISO 19011)	Planned for 2009
ISO/IEC TR 27008	Guideline for auditing of controls		Planned for 2011

Source: Gartner (September 2008)

ISO 27001 – What Have States Done?

Many states, including Delaware, Nevada, North Carolina, Tennessee, Washington, and Wisconsin have adopted ISO 27001 as their foundational or baseline security framework. States report that implementation of 27001 frequently takes as much as a year of concerted effort, as associated policies, standards, and controls are established and put in place. While establishing follow-on compliance with the standards is a lengthier process, adoption of ISO 27001 is seen as a critical foundation for the security programs and for positioning programs for subsequent audits.

Other states have policies and standards that are consistent with ISO 27001 and are in the process of looking at the standard more closely in consideration either of adopting it across the board, or assessing gaps in their individual security programs.

FISMA and NIST Guidance

The **Federal Information Security Management Act of 2002 (FISMA)** is a Federal law enacted in 2002 as Title III of the E-Government Act of 2002. The act was designed to bolster computer and network security within the federal government and affiliated parties (such as recipients of Federal monies and government contractors) by mandating yearly information security audits.

FISMA establishes:

- Standards for categorizing information and information systems by mission impact
- Standards for minimum security requirements for information and information systems
- Guidance for selecting appropriate security controls for information systems

- Guidance for assessing security controls in information systems and determining security control effectiveness
- Guidance for certifying and accrediting information systems

Crucial to FISMA implementation has been the National Institute of Standards' (NIST) development of publications that provide detailed information and guidance in each of the preceding categories, to help agencies implement provisions of the Federal legislation. A list of the most significant publications is provided in Appendix B below.

As this brief was researched, NIST released an initial version of Revision 3 of Special Publication (SP) 800-53, the first major update of that document since 2005. SP 800-53 aims to harmonize the security requirements across government information systems, apart from national-security systems. In addition, the document tries to close the gap that exists between information systems in the public and private sectors. It includes a number of changes to the Recommended Security Controls for Federal Information Systems and Organizations, including eliminating security controls and control enhancements that overlap or are no longer needed, incorporating the revised version of the six-step Risk Management Framework, and adding new security control enhancements.

A wide array of state programs that are recipients of Federal funding are increasingly and more formally subject to FISMA requirements.

FISMA/NIST – Implications for the States

Though it is designed specifically for government information security programs and applies most directly to Federal agencies, a wide array of state programs that are recipients of Federal funding are increasingly and more formally subject to FISMA requirements. These have directly impacted unemployment insurance, Medicare and Medicaid services, homeland security, IRS, and social security-related programs.

For these reasons, several states, including Kansas, Michigan, Minnesota, and Tennessee have chosen NIST standards, particularly 800-53, as the base framework for their security programs. Auditors in those states are using NIST checklists in the course of regular auditing.

Conversations with other state CISOs, CIOs and other security professionals reflect that, while there is some uncertainty or unevenness about the extent to which FISMA/NIST standards are being applied, it is increasingly likely that FISMA compliance will be explicitly extended to all recipients of Federal funds.

In the environment that will exist as Federal economic recovery act monies are provided to states, the likelihood is even greater that FISMA will play a larger role in security auditing and compliance at the state level.

States that have adopted ISO 27000 series standards typically have cross-walked the series' policies, standards, and controls to FISMA/NIST standards, and federal guidance is available to assist this effort.

PCI DSS Payment Card Industry Data Security Standard

PCI DSS stands for **Payment Card Industry Data Security Standard**, and is a worldwide security standard created by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa through the Security Standards Council (SSC) established by those companies in 2006. The PCI security standards are technical and operational requirements placed on organizational entities that process card payments to prevent credit card fraud and hacking and mitigate other security vulnerabilities and threats. The standards apply to all organizations that store, process or transmit cardholder data, which obviously includes an increasingly larger number of state agencies transacting with businesses, with citizens, and with other government entities.

The following are the six primary control areas comprising the Payment Card Industry security standard:

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

Related requirements for each of the base control areas are detailed in Appendix B below.

PCI standards have also been extended through separate Personal Identification Number (PIN) Entry Devices requirements and Payment Application Data Security standards. The latter have become increasingly critical as more and more businesses and public agencies conduct business through web-based applications. The PCI SSC has also released several supplemental documents that clarify various requirements, including:

Information Supplement: Requirement 11.3 Penetration Testing; Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified; and Navigating the PCI SSC—Understanding the Intent of the Requirements.

The PCI Security Standards Council is responsible for managing PCI security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council. Non-complying companies that maintain a relationship with one or more of the card brands, either directly or through an acquirer risk losing their ability to process credit card payments and being audited and/or fined.

PCI and State Government Transactions

State governments are under constant pressure to deliver both in-person and online services that often include payment card mechanisms. States are faced with the choice of developing internal solutions or outsourcing, but in both instances there are significant risks in getting financial processing wrong. States must strongly consider requiring certification of third party vendors they contract with. Additionally, they should strive to meet PCI requirements in their internal development processes.

Most states have moved strongly to ensure that credit card processing applications they employ are PCI-compliant, by integrating PCI-DSS requirements into existing security policies, standards, and controls. As noted above, credit card processing is often handled through third party contracts, and states require PCI compliance and adherence through those contracts.

Most states have moved strongly to ensure that credit card processing applications they employ are PCI-compliant...



COBIT

Control Objectives for Information and related Technology, COBIT, is an open, international standard originally published in 1996 by the IT Governance Institute and the Information Systems Audit and Control Association (ISACA). Now in version 4.1, COBIT is a set of best practices for information technology designed to provide managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control for private-sector companies or public agencies.

The COBIT Framework is organized into four domains, thirty-four high-level control objectives, and 318 detailed control objectives. The framework follows a general plan-do-check-act structure. The primary COBIT domains comprise the following (please see Appendix B for the associated, high-level control objectives):

1. Plan and Organize
2. Acquire and Implement
3. Deliver and Support
4. Monitor and Evaluate

COBIT and State Programs

Since its introduction in the mid-nineties, COBIT has been used by state and federal auditors in the analysis and assessment of IT systems and their operation, and as such, it predates several of the security standards frameworks covered in this brief. Many states, among them Kansas, Minnesota, North Carolina, and Oklahoma, report that state auditors use COBIT as the primary audit framework in assessment of their IT security programs, with the implication that CIO familiarity with COBIT requirements is vital there.

As a framework, the concerns of COBIT are essentially a superset of those relating specifically to security, and some organizations have adopted COBIT guidelines as part of their IT governance process. COBIT

guidelines are frequently employed in combination with both NIST and ISO security standards.

SAS 70

SAS 70, more formally, Statement on Auditing Standards No. 70, Service Organizations, is an auditing standard created by the American Institute of Certified Public Accountants (AICPA) in 1992. SAS 70 defines standards used by auditors to assess the internal controls of service organizations and prepare service auditor's reports. Service organizations are entities providing services that impact the control environment of their customers. Examples of service organizations are insurance and medical claims processors, trust companies, hosted data centers, application service providers (ASPs), managed security providers, credit processing organizations and clearing-houses. Auditors follow AICPA standards for fieldwork, quality control and reporting and issue a formal report to the service provider that includes the auditor's opinion once the audit is completed.

SAS 70 audits consist of two types. A Type I audit assesses the service organization's description of controls placed in operation and the suitability of the design of the controls to achieve the specified control objectives, as the latter are defined by the service provider. A Type II service auditor's report includes the information contained in a Type I service auditor's report and also includes the service auditor's opinion on whether the specific controls were operating effectively during the period under review.

SAS 70 and Enterprise IT Shops

The majority of state enterprise IT agencies are structured in a similar fashion and operate as internal service providers to state agencies and other public entities on a chargeback basis, user fee or comparable model of delivering services. The agencies are "customers" that

purchase data center, network, e-mail or telecommunication services under a published rate or pro rated assessment method. Because of this business model, State CIOs are more familiar with the SAS 70 audit process, recommendations and reports.

SAS 70 audits have become the standard compliance audit for assessing internal controls for data centers and managed services. As a shared services organization, the state CIO agency may have service level agreements or third party agreements with external providers. From a security perspective, these should have procedures to protect data and applications. In addition, as a service provider, state CIOs must account for services and billing charges to the agency customer.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the Federal government in 1996. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers, with the overall goals of protecting the privacy and security of health information and promoting the efficiency of the health care industry through use of standardized electronic transactions.

HIPAA's Security Rule covers health plans, healthcare clearinghouses, and healthcare providers. Health plans are defined as any individual or group plan that provides or pays the cost of health care, which includes the Medicare and Medicaid programs operated at the state and federal levels. The Rule establishes three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, various security standards are identified, and for each standard, both required and addressable implementation specifications are delineated. The rule

includes eighteen standards that cover thirty-six implementation specifications. Required specifications must be adopted and administered as dictated by the Rule. Addressable specifications are more flexible.

The Centers for Medicare and Medicaid Services defines the following steps for complying with the Security Rule:

- Assess current security, risks, and gaps
- Develop an implementation plan
 - Review the Security Rule standards and specifications
 - Review addressable implementation specifications
 - Determine security measures
- Implement solutions
- Document decisions
- Reassess periodically.

The Security Rule required covered entities to be in compliance with the rule no later than April 2005, though smaller health plans were given an additional year to comply.

HIPAA and State Health-Related Agencies

As in the case of PCI-DSS standards, HIPAA is an example of a set of requirements that is applicable to a particular niche in state government programs – those dealing with patient health records – rather than an across-the-board set of requirements. As a consequence, HIPAA impacts health and human services agencies more directly than others, although there are linkages outside those programs which place HIPAA requirements on other agencies. At the same time, impacted health and human services programs must view HIPAA security as a fundamental business requirement: given the extent to which such programs are supported by federal funding, HIPAA compliance has an extremely high priority within those programs.

From the point of view of enterprise security programs, the challenge is to ensure that HIPAA compliance efforts are harmonized with other security standards



and controls that are established at the enterprise level. Given different levels of emphasis and financial support for security requirements, the possibility exists that health and human services agencies can operate outside the larger frame of reference, but it is also the case that HIPAA compliance efforts can be well-integrated into broader security standards and have a synergistic effect on enterprise security initiatives.

It should be noted that as this brief was prepared, a penalty of \$2.25 million was assessed against the drugstore chain CVS by the Federal Trade Commission, for violations of HIPAA requirements relating to the disposal of protected patient information.

FERPA

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Schools or public agencies that receive student data may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools or agencies must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification is left to the discretion of each school or agency.

FERPA, State Departments of Education, and the CIO

Within states, departments of education and post-secondary oversight agencies are most directly impacted by FERPA privacy requirements. It is also true, however, that data breaches at public universities involving student records and personal information are alarmingly prevalent, as the log of data breaches at privacyrights.org attests. To the extent that student data flows into state systems, either from postsecondary institutions or local school districts, data exposure risks are present wherever security controls are inadequate. State CIOs must be mindful of this, as well as the brand damage that follows from exposure of student data. CIOs should also be aware that the American Recovery and Reinvestment Act (ARRA) provides \$250 million in competitive grant funding for modernization of statewide longitudinal data systems.

The Federal Department of Education has issued "Recommendations for Safeguarding Education Records." The department chose to include in this notice recommendations that included references to guidance issued by NIST and the Office of Management and Budget (OMB). An Educause Security Task Force commented in May 2008, that while it shared the department's concerns about cybersecurity, it was concerned that focus on government approaches may be misinformed and encouraged the department to consider resources developed by the task force (e.g., see Effective IT Security Practice Guide). The task force further cautioned DOE that "the inclusion of recommended safeguards causes considerable confusion about the department's intentions and future plans."²

Sarbanes-Oxley

The Sarbanes-Oxley Act (SOX) was enacted by the Federal government in 2002 in response to a number of major corporate and accounting scandals, most prominently that of the Enron Corporation. SOX establishes new, enhanced standards for all U.S. public companies, and though as such it is not directed at government, it has nonetheless had a significant impact on internal accounting controls in public agencies through its focus on management oversight of how fiscal information within agencies is created, accessed, stored, processed, and transmitted within automated as well as manual record systems.

Among the Act's principal reforms are these elements:

- Creation of an independent public company accounting oversight board
- A heightened level of corporate governance and responsibility measures
- Expanded corporate, financial, and insider disclosure requirements, and
- A range of new penalties for fraud and other violations.

SOX Relevance to State Programs

Within the Federal government, a counterpart to Sarbanes-Oxley requirements was passed in the form of OMB Circular A-123 in December 2004. The circular was addressed to all Federal chief financial officers, chief information officers, and program managers, and the fiscal transparency and accountability requirements imposed on private sector companies by Sarbanes Oxley have effectively been replicated at the Federal level.

In the current environment of increasingly stricter rules surrounding such transparency, it behooves state CIOs to acquaint themselves with the impacts that SOX has had on their private sector counterparts and more specifically, on the fiscal controls within their organizations.

The "New Kid in Town" – Consensus Audit Guidelines (CAG)

From the foregoing discussion, the complexity of the environments in which state security programs are maintained should be readily apparent. If more proof were needed, a significant new set of guidelines, the Consensus Audit Guidelines (CAG) from the Center for Strategic and International Studies appeared as this brief was nearing completion. The guidelines were developed during 2008 by a consortium of federal agencies and private organizations that included the Department of Homeland Security, the National Security Agency, the SANS Institute, and MITRE Corporation.

The Consensus Audit Guidelines focus on addressing known attack techniques and delineate twenty controls that Federal agencies commonly employ to protect against them. Of those twenty, fifteen can be addressed through automatable means, and the remainder require human intervention. The guidelines have been immediately heralded within many Federal civilian and defense agencies, presumably for their simplicity and risk-responsive character, but there have also been criticisms of them in light of FISMA/NIST requirements that would be unmet should these be the only points of emphasis. During the current thirty day comment period for the draft guidelines, they are being mapped against ISO, HIPAA, PCI, and SOX requirements.

The impact that CAG may have on state programs is unclear.

The Consensus Audit Guidelines focus on addressing known attack techniques...

It's About Risk Management: Action Items for State CIOs

The rapidly evolving digital infrastructure carries with it a correspondingly dynamic range of security threats that state security professionals must constantly contend with to maintain the integrity and availability of government services. The standards and guidelines described in this brief were created to assist CISOs and other security administrators in this effort and to reduce the risk and vulnerabilities to the greatest extent possible.

To benefit from the standards and guidelines, it is imperative that CIOs:

- **Understand the complexity of overlapping standards**
- **Select a foundational standard while expecting to reference others as needed**
- **Start the “as is” assessment to identify existing gaps**
- **Incorporate the standard by reference in the state’s security architecture**
- **Understand related vertical standards and potential impacts on the enterprise as they evolve**
- **Develop strong working relationships with state auditors**
- **Monitor, test, and quantify compliance levels, to ensure that standards and controls are working and effective**
- **Work untiringly to educate the state workforce about the role of security standards and their own responsibilities under those standards**

While informing themselves, making sometimes difficult choices between standards, and executing the follow-on policies, standards, and controls are significant challenges to CIOs and their CISOs, there are no short-cuts to securing state IT systems and the services they provide.

Appendix A: Bibliography and Additional Resources

Descriptions of each of the standards or guideline in this document are drawn from Wikipedia entries on each topic. The latter typically provide additional detail for each standard and should be consulted for further background.

See:

Wikipedia, ISO/IEC 27001,
http://en.wikipedia.org/wiki/ISO/IEC_27001

Wikipedia, Federal Information Security Management Act of 2002,
http://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002

Wikipedia, PCI DSS,
http://en.wikipedia.org/wiki/PCI_DSS

Wikipedia, COBIT,
<http://en.wikipedia.org/wiki/COBIT>

Wikipedia, Statement on Auditing Standards No. 70: Service Organizations,
http://en.wikipedia.org/wiki/Statement_on_Auditing_Standards_No._70:_Service_Organizations

Wikipedia, Health Insurance Portability and Accountability Act,
http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

Wikipedia, Family Educational Rights and Privacy Act,
http://en.wikipedia.org/wiki/Family_Educational_Rights_and_Privacy_Act

Wikipedia, Sarbanes-Oxley Act,
http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act

“How to make the most of ISO/IEC 27001” by Carsten Casper. Gartner Research Note G00161458, September 2008.

Recommended Security Controls for Federal Information Systems – NIST Special Publication 800-53, Revision 1: December 2006. (Appendix G Security Control Mappings provides a crosswalk mapping between ISO 17799, NIST 800-26, GAO FISCAM, and other Federal standards.
<http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf>

NIST Introductory Resource Guide to Implementing the HIPAA Security Rule [PDF] October 2008
<http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>

Core PCI DSS, PCI Security Standards Council 2009,
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

The Centers for Medicare and Medicaid Services provides a series of publications designed to introduce and guide implementation of the HIPAA Security Rule at http://www.cms.hhs.gov/EducationMaterials/01_Overview.asp#TopOfPage

HIPAA ISO Mapping:
http://www.wedi.org/cmsUploads/pdfUpload/WEDIBulletin/pub/Copy_of_ISO_HIPAA_MatrixFeb05final.pdf

SANS Reading Room Article also includes cross-walk: The HIPAA Final Security Standards and ISO/IEC 17799. Sheldon Borkin, 2003
http://www.sans.org/reading_room/whitepapers/standards/the_hipaa_final_security_standards_and_iso/iec_17799_1193

“Consensus Audit Guidelines,” SANS,
<http://www.sans.org/cag>

Appendix B: More Information

FISMA/NIST

NIST publications include the following key security-related documents:

- *FIPS Publication 199, Standards for Security Categorization of Federal Information and Information System* (Completed)
- *FIPS Publication 200, Minimum Security Requirements for Federal Information and Federal Information Systems* (Completed)
- *NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems* (Completed)
- *NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems* (Completed)
- *NIST Special Publication 800-37 Revision 1, (initial public DRAFT) Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach* (Completion August 2008)
- *NIST Special Publication 800-39, (second public draft) NIST Risk Management Framework* (Completion April 2008)
- *NIST Special Publication 800-53 Revision 2, Recommended Security Controls for Federal Information Systems* (Completed)
- *NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems* (Completed)
- *NIST Special Publication 800-59, Guide for Identifying an Information System as a National Security System* (Completed)
- *NIST Special Publication 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories* (Completed)

Payment Card Industry Data Security Standards – Control Areas and Specific Requirements

The following are the six primary control areas comprising 12 specific requirements of the PCI DSS:

1. Build and Maintain a Secure Network
 - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
 - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
2. Protect Cardholder Data
 - Requirement 3: Protect stored cardholder data
 - Requirement 4: Encrypt transmission of cardholder data across open, public networks
3. Maintain a Vulnerability Management Program
 - Requirement 5: Use and regularly update anti-virus software
 - Requirement 6: Develop and maintain secure systems and applications
4. Implement Strong Access Control Measures
 - Requirement 7: Restrict access to cardholder data by business need-to-know
 - Requirement 8: Assign a unique ID to each person with computer access
 - Requirement 9: Restrict physical access to cardholder data
5. Regularly Monitor and Test Networks
 - Requirement 10: Track and monitor all access to network resources and cardholder data
 - Requirement 11: Regularly test security systems and processes
6. Maintain an Information Security Policy
 - Requirement 12: Maintain a policy that addresses information security

COBIT Domain and Control Objectives

The COBIT Framework is organized into four domains, 34 high-level control objectives, and 318 detailed control objectives. The framework follows a general Plan-Do-Check-Act structure. The domains and control objectives are as follows:

Plan and Organize

- P01 Define a strategic IT plan.
- P02 Define the information architecture.
- P03 Determine technological direction.
- P04 Define the IT processes, organization, and relationships.
- P05 Manage the IT investment.
- P06 Communicate management aims and direction.
- P07 Manage IT human resources.
- P08 Manage quality.
- P09 Assess and manage IT risks.
- P10 Manage projects

Acquire and Implement

- AI1 Identify automated solutions.
- AI2 Acquire and maintain application software.
- AI3 Acquire and maintain technology infrastructure.
- AI4 Enable operation and use.
- AI5 Procure IT resources.
- AI6 Manage changes.
- AI7 Install and accredit solutions and changes.

Deliver and Support

- DS1 Define and manage service levels.
- DS2 Manage third-party services.
- DS3 Manage performance and capacity.
- DS4 Ensure continuous service.
- DS5 Ensure systems security.
- DS6 Identify and allocate costs.
- DS7 Educate and train users.
- DS8 Manage service desk and incidents.
- DS9 Manage the configuration.
- DS10 Manage problems.

- DS11 Manage data.
- DS12 Manage the physical environment.
- DS13 Manage operations.

Monitor and Evaluate

- ME1 Monitor and evaluate IT performance.
- ME2 Monitor and evaluate internal control.
- ME3 Ensure regulatory compliance.
- ME4 Provide IT governance.

Appendix C: Endnotes

¹“How to make the most of ISO/IEC 27001” by Carsten Casper. Gartner Research Note G00161458, September 2008.

²“Security Task Force Submits Comments on Proposed FERPA Rules”; Educause, May 29, 2008; <http://connect.educause.edu/blog/vvogel/securitytaskforcesubmitsc/46810?time=1237980745>