



An Integrated Approach: ISO 27001 and BITS Shared Assessments Program

*A Perspective of BSI Management
Systems and the Shared
Assessments Program*

April 2008

BITS
1001 Pennsylvania Avenue, NW
Suite 500 South
Washington, DC 20004
(202) 289-4322
www.bitsinfo.org/fisap

BSI Management Systems
12110 Sunset Hills Road, Suite 200
Reston, VA 20190-5902
(703) 437-9000
www.bsiamerica.com

The Santa Fe Group
3 Chamisa Drive N.
Suite 2
Santa Fe, NM 87508
(505) 466-6434
www.santa-fe-group.com

©BITS 2008

Documents created under the Financial Institution Shared Assessments Program may be downloaded at the official Shared Assessments website: www.bitsinfo.com/fisap.

Documents related to ISO 27001 may be downloaded at the BSI website, www.bsiamerica.com, under the “Certification” section.

While retaining copyrights to the Agreed Upon Procedures (AUP) and Standardized Information Gathering (SIG) documents, the Financial Institution Shared Assessments Program makes them freely available to the public for the purpose of conducting self-assessments and third-party security assessments. Licenses for other uses may be available by contacting BITS and The Santa Fe Group. **Please review our Terms of Use prior to downloading, copying, using or modifying the AUP or SIG.**

The Shared Assessments Program is administered by The Santa Fe Group (www.santa-fe-group.com). The Santa Fe Group is a strategic consulting firm that specializes in business strategy, risk management, emerging technologies, and innovation. The Santa Fe Group’s Chairman and CEO is the former Founding CEO of BITS, Catherine A. Allen.

Please direct questions about this document and the Shared Assessments Program to:

Michele Edson
Senior Vice President
The Santa Fe Group
831-637-1879
michele@santa-fe-group.com

BSI (www.bsiamerica.com) is an accredited ISO 27001 certified body and leading global independent business services and standards organization. Please direct questions regarding ISO 27001 and requests for further detail behind the ISO 27001 integration methodology to:

John DiMaria; Certified Six Sigma BB, HISP
Product Manager; ISMS.ITSM,BCMS
BSI Management Systems America Inc.
314-831-7835
john.dimaria@bsigroup.com
inquiry.msamericas@bsi-global.com

This document is intended to assist members of the Financial Institution Shared Assessments Program and others in using the Agreed Upon Procedures and understanding how they relate to industry regulations, as well as to deepen their understanding of the program. This document is provided by BITS, The Santa Fe Group and BSI “as is” and any express or implied warranties are disclaimed. In no event shall BITS, The Santa Fe Group, BSI or the Financial Institution Shared Assessments Program Working Group members be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption), however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this document, even if advised of the possibility of such damage.

TABLE OF CONTENTS

1.0	Industry Perspective.....	5
2.0	Selecting a Standard Integrated Approach for your Organization.....	6
	Controls Must Be Integrated	6
	A “Standard of Care” Must Be Process-Oriented.....	6
	The Standard of Care Must Be Risk-Based.....	6
	The Standard Must Be Relevant.....	6
3.0	Standards and Selection Criteria – ISO 27001 and Shared Assessments	7
4.0	Industry Benefits of AUP Integration.....	9
5.0	Common Shared Controls – ISO 27001 and Shared Assessments	13

The ISO 27001 and BITS Shared Assessments Working Group

Niall Browne (Chair), Yodlee Inc.
John DiMaria, BSI Management Systems
Andrew C. Hout, Citigroup
Christopher Carcich, Citigroup
Ashish Kumar Atri, Churchill & Harriman
Chris Ritterbush, Ernst & Young
Christopher Johnson, Merrill Lynch
Patti Enfanto, Iron Mountain
C.R. Visveswaran, Infosys
Saffet Ozdemir, Wachovia Corporation

1.0 Industry Perspective

Our society has become so reliant on real-time information that the loss or corruption of our information infrastructure would significantly impact global banking systems, as well as many other businesses.

What is information? Information encompasses a wide range of diverse pieces including computer data, marketing strategies, tax and personnel records, financial data, communications, and business plans. Whether printed, written on paper or stored electronically, whether transmitted by couriers, electronic means or even spoken in conversation, loss of information can be devastating to corporations, governments and countries. In general, the potential financial and reputational consequences of losing information are what motivate individuals and entities to prevent information loss.

The financial services industry is continuously evolving and growing in complexity. Organizations face many challenges and concerns. Issues such as corporate governance, risk management and regulation continue to have an impact on the industry. Customers want more for less, and they continue to be confident that their information is secure.

In the financial industry alone, more than 200 laws, regulations, government bulletins, alerts, and other guidance documents address the information security obligations of financial institutions. Enforcement agencies such as the Federal Trade Commission (FTC) pursue companies whose poor or deceptive trade practices do not match the information security and privacy statements they voluntarily make to the public. Adding to financial institutions' responsibilities, government regulators are beginning to require companies to ensure the security of any corporate information that falls under the control of its supply chain.

New legislation makes it clear that these responsibilities constitute a legal and corporate governance issue for upper management. The threshold for failure to meet security obligations is no longer a security breach. In many cases, laws put the onus directly on financial institution CEOs and boards of directors for any security violations.

Many laws require companies to implement ongoing processes to assess risks, identify and implement appropriate security measures, and be responsive to those risks, as well as to update their processes continuously to address new risks. In most cases, laws do not require the use of specific security measures or standards, nor do they offer any related guidance. Companies are left to decide how they will meet the new requirements, understanding that merely implementing so-called "strong security measures" is not sufficient. To meet today's security requirements, financial institutions must demonstrate due diligence by following internationally proven and accepted standards that show consistency of process and provide maximum protection.

Unfortunately there is no silver bullet or one-size-fits-all industry approach to comply with all applicable laws and regulations, while also meeting client requirements. Instead, financial institutions need a layered, industry-focused approach to compliance.

2.0 Selecting a Standard Integrated Approach for Your Organization

It is not possible to defend a relevant standard of care, or due diligence to a standard of care, unless the following statements are true:

Controls are integrated

In order for controls to work effectively and at minimal cost, management must work across organizational lines and through cross-functional teams, with an integrated set of controls for both security and regulatory requirements.

Management systems of specified key organizational functions of the business must be integrated, as well as infrastructure, business continuity, disaster recovery, records management, fair information practices, HR practices, physical security, financial controls, segregations of duties, vulnerability management, identity and access management, change control, Internet services development lifecycle management, and problem management.

The standard of care is process-oriented

A “standard of care” must be process-oriented for it to be sustainable and manageable. It is one thing to implement a set of controls for the purpose of passing an audit at a point in time. It is quite another to design an effective control environment with continuous monitoring and improvement of all the necessary elements that meet the objectives for information security and ensure compliance with a specific industry’s regulations.

The standard of care is risk-based

Contrary to common industry practice, an organization cannot defend its choice of controls — nor can it have confidence in its ability to mitigate risk — without an understanding of the risks being addressed in the first place. Many of the existing risk assessment tools available today are technology-focused only, making the task at hand cumbersome and addressing only technical risk, vulnerability and threat. By using ISO 27001 certification and the Shared Assessments Agreed Upon Procedures (AUP) methodologies to address financial-sector-specific requirements, firms can facilitate defining business risk and associated risk reduction approaches that simplify and streamline a risk-based approach for defining a comprehensive and integrated standard of care.

The standard must be relevant

The standard must be relevant to the industry in which the organization or client exists. For example:

- BITS Shared Assessments for financial services
- PCI-DSS for credit card processing
- HIPAA for health care
- ISO 27001 as a framework for all industries

3.0 Standards and Selection Criteria – ISO 27001 and Shared Assessments

The International Organization for Standardization (ISO) is an international standard-setting body composed of representatives from various national standards organizations. Founded in 1947, the organization promulgates worldwide industrial and commercial standards. Headquartered in Geneva, Switzerland, ISO has 157 member bodies out of the world's 195 countries.

While ISO is a non-governmental organization, its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most other non-governmental organizations. In practice, ISO acts as a consortium with strong links to governments. ISO standards have come to be the benchmark by which all other standards are measured.

The ISO 27001 standard focuses on the 12 domains of security. It is one of the best known and highly respected of international information security management standards. Its purpose is to help organizations establish and maintain information security management systems (ISMS), and applies to numerous industries including financial, health care, government, and commercial.

While ISO 27001 is used extensively, it is often not the only standard or regulatory requirement an organization may complete. In the case of credit card payments, a company may use ISO 27001 extensively. If the company processes, stores, or transmits payment card data, it would also use and implement the industry-focused PCI-DSS (Payment Card Industry Data Security Standard) as part of its security framework.

Similarly, financial services providers may consider completing the voluntary BITS Shared Assessments Program, which was created by leading US financial institutions with assistance from the Big 4 accounting firms. Shared Assessments has particular industry relevance for financial services.

The BITS Shared Assessments program is based on the AUP assessment tool and Standardized Information Gathering questionnaire, or SIG. Shared Assessments was created by carefully evaluating and selecting the high-value common controls relevant to the financial services industry, adapted primarily from ISO 27001 and also from PCI-DSS and COBIT.

A financial service provider may have, or plan to complete an ISO 27001 certification, or alternatively may utilize ISO 27002 as the common framework for its internal security program. If this is the case, the service provider may cost-effectively complete the Shared Assessments Program, which leverages these common controls.

Similarly, this commonality and mapping of the high-value common controls enables financial institutions to efficiently incorporate Shared Assessments Program results into their internal programs, which typically are linked to the industry standard ISO 27001.

The Shared Assessments Program AUP and SIG are used to document the service provider's management of its information security controls, as explained below.

- **Standardized Information Gathering (SIG) questionnaire:** The SIG is a self-assessment questionnaire developed by Shared Assessments Program members. The SIG is built on the ISO IEC 27002 standard, with additional input from Shared Assessments Program members. All SIG responses are Yes, No, or N/A, making the completed SIG easy to read by machine. The SIG's level of technical detail is unsurpassed in the industry. And as an added benefit, service providers can complete the SIG just once, and then provide the completed SIG to multiple clients in response to

their proprietary questionnaires, reducing the amount of time the service provider consumes completing questionnaires. *Completion Time: 3 days (approx)*

- **Standardized Information Gathering “Lite” (SIG Lite) questionnaire:** The SIG Lite was developed by Shared Assessments Program members to provide a streamlined version of the SIG. It is intended to be used by service providers that are considered low risk, providing clients with a quick view of their controls. The SIG Lite was developed by identifying key controls in the SIG and creating multi-part questions on those controls. All responses in the SIG Lite are Yes, No, or N/A, to allow for straightforward binary analysis by the recipient’s risk management system. The SIG Lite is included in the full SIG. *Completion Time: 1 day (approx)*
- **Agreed Upon Procedures (AUP):** Developed by Shared Assessments Program members with the Big 4 accounting firms acting as Technical Advisers, the AUP provides objective and consistent procedures to be performed under each control area (mapped to ISO 27001) during an onsite assessment. The tests within the AUP are executed by an independent accounting or assessment firm selected by the service provider. The procedures in the AUP are written to follow the American Institute of Certified Public Accountants (AICPA) professional standards AT (Attestation Standard) Section 201, which sets forth attestation standards and provides guidance to practitioners on performance and reporting in agreed-upon procedures engagements. Results of the AUP are provided by the audit or assessment firm directly to the service provider without subjective opinions. In most of the AUP tests, results consist of population, sample size and number of failures within the sample. This allows the recipient financial institution to form its own opinions of the results to satisfy its own risk appetite. Depending on the recipient, AUP results may be used in place of a costly onsite assessment, reducing resources required by both the service provider and the financial institution. *Completion Time: Anecdotal evidence demonstrates that an AUP may be completed in as little as 4 days onsite.*

The end products from the above tools are wholly owned by the service provider executing the SIG, SIG Lite or AUP assessment. They also own the results and distribution. They control who receives the results under their standard non-disclosure agreements.

4.0 Industry Benefits of AUP Integration

Shared Common Industry Controls

By combining the requirements of the AUP with those of ISO 27001 best practices for information security management, businesses can achieve a holistic information security governance standard, along with an ISO certification, which are together more germane to the financial service industry. Using these common industry controls together can create process efficiencies and strengthen internal controls, allowing companies to surpass competitors by completing both assessments. Companies can also use economies of scale to achieve one certification that includes the AUP, thus creating an environment that is ISO 27001-certified along with additional financial industry requirements for a small premium over the cost of two separate silos.

Organizations and corporations that take this hybrid approach of integrating the AUP controls with ISO 27001 controls in their internal control structure programs will strengthen their security posture while demonstrating that they have adequate and effective internal controls over standalone financial type transactions and processes. The result is not only improved integrity but strengthened confidentiality and availability.

Business that combine the AUP and ISO audit steps achieve the information technology governance objectives outlined in COBIT and PCI while eliminating overlap between the two. Combining AUP and ISO audit steps also allows companies to implement the additional prescribed procedures outlined in the Information Technology Infrastructure Library (ITIL) and ISO to achieve a comprehensive internal control structure. This holistic approach can be used as an ongoing measuring tool to verify that financial transactions and security standards are maintained.

Companies that combine the AUP and ISO audits also gain an improved risk-based approach to information security management through an ongoing process of risk assessment and risk mitigation, which helps them to adequately prioritize the implementation of countermeasures, and strengthen their security posture through the AUP's rigorous testing. Organizations are then able to demonstrate that they have good internal controls over financial processes, and, more importantly, that they can help mitigate information security risks by operating under one system rather than two. This approach can complement the Plan, Do, Check, Act (PDCA) process, which is a widely accepted system to drive continual improvement.

Table 1. Example of integrating the AUP testing with the process controls of ISO 27001

H.	Access Control	
	AUP Procedure	ISO 27001 Process Control
H.1	Password Controls	11.3.1, 11.5.1, 11.5.3
H.2	Revoke System Access	11.1.1, 11.2.1, 11.2.4
H.3	Logical Access Authorization	11.1.1, 11.2.1, 11.2.3
H.4	Inactive Accounts	11.5.5
H.5	Controls for Unattended Systems	11.3.2
H.6	Revoke Physical Access	8.3.3, 9.1.2, 11.1.1

Objective and Repeatable – No Potentially Misleading Subjective Opinion

When Shared Assessments was first being developed, one of the guiding objectives was to establish a consistent and independent assessment program that each financial institution could use to evaluate risk exposure relative to its specific vendor risk posture. Numerous industry standards and attestation methods were evaluated, and the agreed-upon procedures model was selected. The primary reasons for selecting this model were:

- It requires the practitioner to be independent from the responsible party (the owner of the subject matter, in this case the service provider). This confirms for the specified parties that the practitioner is not completing the engagement while providing other related consulting services, which could compromise the practitioner's independence.
- There is no opinion or negative assurance provided. This allows each specified party to evaluate the findings in the context of its own risk tolerance.
- The criteria used within the agreed-upon procedures do not create another standard; rather they provide a benchmark that may be consistently measured.
- The criteria used in measurement are objective: regardless of the practitioner, the procedure will yield the same result.
- All control objectives listed in the AUP must be executed if they are applicable to the service provider. If a control cannot be tested, an explanation must be provided in the AUP final report.

The AUP has a distinct advantage over individual vendor assessment programs: it creates an objective, repeatable and sustainable assessment process by design. The AUP component of the Shared Assessments Program does not seek to interpret whether or not a vendor's controls are adequate or inadequate. Instead, the AUP provides objective results based on the exact execution of the AUP, so the assessor/auditor cannot state his or her subjective "opinion" of the control set. The controls are what they are, and the Shared Assessments evaluation is a truly objective vehicle to gather information.

Unique Financial Industry Acceptance, Relevance and Efficiency

Because it was created by leading US financial intuitions through BITS, with the Big 4 accounting firms acting as Technical Advisors, the Shared Assessments Program has a unique level of acceptance and relevance to the financial services industry.

Historically, the ISO standards have been the foundation upon which industry builds solid management systems. ISO 9001 was the catalyst for AS 9001 for Aerospace, QS 9000 and TS 16949 for automotive. ISO 27002 and ISO 27001 were the catalysts for the National Institute of Standards and Technology (NIST) government sector Federal Information Security Management Act (FISMA), and, more recently, the Shared Assessments Program AUP and SIG.

The Shared Assessments Program provides a unique opportunity for financial institutions and service providers to utilize assessment controls that are rooted primarily in the ISO/IEC 27002, and also in PCI-DSS and COBIT. Since these controls are either developed from or mapped to the ISO/IEC 27002 standard, the consumer of these assessment documents is assured that the controls are addressed during the assessment. With the broad acceptance of the ISO/IEC 27002 standards, most organizations have already mapped their internal policies and controls to this standard, allowing them to easily see the difference between their policies and the controls tested by the Shared Assessments Program.

In the past, financial service providers that completed an industry standard assessment would often find after

presenting the results to a financial institution that only limited sections were considered relevant, or that specific areas of interest to the client had not been examined. The true industry value of Shared Assessments is in its efficiency, as it examines specific areas of interest to financial intuitions, allowing both the AUP and the SIG to be executed with minimal time and cost, while providing maximum effectiveness and relevance. Other industries, too, are using Shared Assessments because of the program's depth of inspection of critical common controls.

Shared Assessments as a Business Enabler

For financial institutions, one of the key criteria in selecting a service provider is often the degree of confidence in the provider's proven level of security. The effort required to initially and periodically review the service provider's controls is often considerable and costly, both for the financial institution and the service provider.

The Shared Assessments program was designed by financial institutions to ask only applicable questions and request only necessary information, so it can be used for both initial evaluations and periodic reviews. Because it is a formalized process, Shared Assessments allows financial institutions to quickly and easily determine the level of risk. The service provider will typically complete the AUP and SIG annually.

Service providers can provide Shared Assessments data to financial institutions prior to contract signing, allowing financial institutions to evaluate the service provider controls sooner and in depth. The program's efficiency speeds the engagement process, making it a key business enabler for the service provider.

Common Adaptive Security Model

Complex corporate governance, evolving risk management methodologies and constantly changing regulations continue to have a significant impact on the financial industry. Corporate governance and risk management are constantly evolving within corporations based on industry technology developments, management models, standardization and threat identification.

Each institution approaches this constantly changing environment differently. The AUP allows them to *adapt* their current corporate governance and risk management models to a "common" statement of controls specific to the financial industry. This allows financial institutions the freedom to evolve their security models and keep pace with changing industry requirements and standards without having to communicating changing criteria to their vendors.

Sampling Methodology Predefined by the Big 4 Accounting Firms

One of the key factors of an evaluation process is determining the size of the sample to examine, as well as the sampling methodology. If the sampling methodology is too narrow or restrictive then the picture will be incomplete; if the sampling is too broad the assessment can become cost prohibitive and bloated. Often the sampling is constricted by the negotiated price of the assessment. But if two assessment or audit firms are theoretically to execute the same assessment, and all the variables are identical apart from one assessment using a sample size of one and the other thirty, the results could vary significantly. The financial institution would not be able to truly determine the actual level of risk or have confidence in the evaluation process.

With the AUP, the sampling size has been predefined by using a methodology common to the Big 4 accounting firms, and acceptable to financial institutions. This allows a far more complete, consistent and accurate risk picture to emerge.

The table below reflects the sample size for a population using the random sampling selection technique.

Table 2. Sample size for a population using the random sampling selection technique

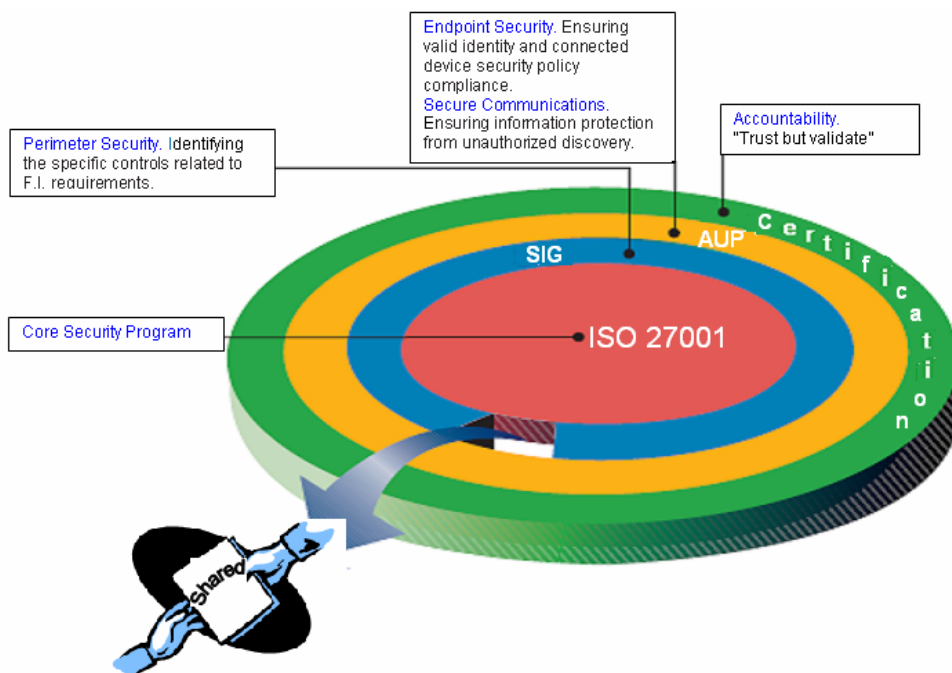
Population	Sample Size
$X > 300$	30
$2 < X < 300$	The greater of 10% or 3
$X < 3$	All

Multiple Solutions for Various Business Cycles, Sizes, and Organizations

Companies can choose from three levels of assessment under the Shared Assessments Program: the SIG, the SIG Lite and the AUP, introducing significant flexibility to the assessment process. Smaller service providers with less risk may complete the SIG Lite, which is composed of 50 questions. Service providers seeking a more comprehensive assessment may complete the full SIG and/or the AUP.

Organizations using ISO 27001 may ask “What is the value?” of Shared Assessments, since the SIG was created using the ISO 27002 controls. The value is in the program’s “layered approach” (see Figure 1 below). ISO 27001 provides the “road map” and controls for a holistic information security system. The SIG is more specific to the financial services industry, so it provides a self-assessment that can facilitate creating an SOA (Statement of Applicability) required in ISO 27001. In some cases, the SIG can provide a supplemental control that may serve the business better and therefore be substituted for one or more of 133 controls in ISO 27001.

Figure 1. The Shared Assessments Program’s layered approach



5.0 Common Shared Controls – ISO 27001 and Shared Assessments

A comprehensive mapping of the Shared Assessments AUP controls to ISO 27001 as well as PCI-DSS version 1.1 and COBIT version 4.1 is published in the Shared Assessments Program white paper “The Financial Institution Shared Assessments Program Industry Positioning and Mapping Document.” The document can be downloaded on the BITS website at <http://www.bitsinfo.org/FISAP/Forms/V3WP.pdf>.

Table 3 below provides a sample from the white paper mapping a single AUP (C.2) to ISO 27001.

Table 3. Sample mapping of an AUP to ISO 27001, from the Shared Assessments white paper

C.	ORGANIZATION OF INFORMATION SECURITY	AUP	ISO 27001	Control Objective	Control
C.2		<i>DEPENDENT SERVICE PROVIDER AGREEMENTS</i>	<i>ORGANIZATION OF INFORMATION SECURITY</i>	Confidentiality agreements	6.1.5
				Contact with authorities	6.1.6
				Identification of risks related to external parties	6.2.1
				Addressing security when dealing with customers	6.2.2
				Addressing security in third party agreements	6.2.3