

Area	SAS 70	SSAE 16	AT101 - Attest Engagements	AT601 - Compliance Attestation	ISAE 3402	ISO 27002/3
Effective	For reporting timeframes up until June 14, 2011. Superseded by SSAE 16.	For reporting timeframes ending on or after June 15, 2011. Early adoption allowed.	For reporting timeframes ending on or after June 1, 2001.	For reporting timeframes ending on or after June 1, 2001.	Effective for reports covering periods ending on or after June 15, 2011.	Has been issued since October 2005 however, it is due to be updated
Management Assertion	Not Required	Required	Only required for reports on Management's Assertion	Required, unless the engagement is required by law.	Required	Not required per se, Management does need to develop the Information Security Management System (ISMS) and supporting policies as well as the Statement of Applicability (SoA) which defines scope and the Risk Treatment Plan (RTP)
Who should consider	Service Organizations with a reporting timeframe currently in progress that will end before June 14, 2011 that have clients and prospects primarily based in the United States.	Service Organizations who have international clients may want to early adopt. Service Organizations that have reporting timeframes ending on or after June 15, 2011. Service Organizations who have an established controls framework and assessment process who may see early adopting as a competitive advantage.	Entities that wish to report on controls over a specified set of objectives.	Entities that wish to obtain a report on compliance to specified requirements and/or report on the effectiveness of the entity's internal control over compliance.	Service Organizations whose clients or prospects are primarily not US based companies or whose clients have non US affiliates or subsidiaries. Applies to service organizations that provides a service to user entities that is likely to be relevant to the user entities' internal control as it relates to financial reporting.	All organizations using complex information systems environments
Opinion Scope	Opinion on Description/Design of Controls is as of the report date. Opinion on Operating Effectiveness covers the timeframe of the report.	Opinion evaluates Management's Assertion for the entire period. Opinion on Description of Systems covers the entire audit period.	Opinion is based on a defined criteria or an assertion by Management. Opinion is issued for a high level of assurance (Examination). A negative assurance letter is issued for a level of moderate assurance (Review).	Examination: Opinion is based on the entity's compliance with specified requirements or the entity's assertion about compliance with specified requirements. Agreed-Upon Procedures: No opinion.	Opinion evaluates Management's Assertion for the entire period. Opinion on Description of Systems covers the entire audit period.	Certifiers opinion on meeting the requirements of the certification for the information system management solution
Users of the Report	Limited to Management, Board of Directors, and User Organizations and their auditors	Limited to Management, Board of Directors, and User Organizations and their auditors	May be for general use (not restricted)	For Examination: A statement restricting use to specified parties may be included. For Agreed-Upon Procedures: Limited to specified parties.	Limited to Management, Board of Directors, and User Organizations and their auditors	Certification may be used as a public statement
Timeframe of the Report	May be as of a certain date (type 1) or cover a timeframe typically between six months and one year (type 2).	May be as of a certain date (type 1) or cover a timeframe typically between six months and one year (type 2).	May be as of a certain date, cover a timeframe, or cover multiple periods (comparative statements).	May be as of a certain date or cover a timeframe.	May be as of a certain date (type 1) or cover a timeframe typically between six months and one year (type 2).	The report is as of a point in time. Once certified, the certification is valid for a period of three years. Annual audits for verification of compliance are required.
Report Includes	1. Service Auditor's Report 2. Management's Description of Controls 3. Tests of Operating Effectiveness (type 2 only) 4. Other information (not required)	1. Service Auditor's Report 2. Management's Assertion 3. Management's Description of the System 4. Tests of Operating Effectiveness (type 2 only) 5. Other information (not required)	1. Service Auditor's Report 2. Subject Matter or Management's Assertion	1. Service Auditor's Report 2. Subject Matter or Management's Assertion	1. Service Auditor's Report 2. Management's Assertion 3. Management's Description of the System 4. Tests of Operating Effectiveness (type 2 only) 5. Other information (not required)	Stage 1 • Informal review of Information Security Policy, Statement of Applicability (SoA), and Risk Treatment Plan (RTP) Stage 2 • Formal audit of the ISMS Stage 3 • Follow-up audits to confirm compliance is maintained
Information Being Reported On	Description of control objectives and related controls, including complementary user entity controls. Description of aspects of the service organization's control environment, risk assessment process, information and communications systems, control activities and monitoring controls.	"Description of Systems" : Includes descriptions required for SAS 70 as well as the following descriptions: Description of the services provided, including classes of transactions processed; Description of the procedures by which services are provided, including transaction initiation, authorization, recording, processing and correction; Description of the capturing of significant events and conditions other than transactions; Description of the process used to prepare reports or information provided to user entities.	Report may be on Subject Matter or an Assertion by Management.	Compliance with specified requirements. May be financial or nonfinancial.	Internal controls over services provided that are likely to be relevant to the user entities' financial reporting.	The adherence to ISO standards for the ISMS for areas within the SoA defined systems at an organization.
Internal Audit Function	Use of Internal Audit work is permitted.	Use of Internal Audit work is permitted. However, the service auditor is required to describe the work performed by the internal audit function, as well as the procedures used to test that work. (When internal auditors provide direct assistance to the service auditor and that assistance is planned and supervised by the service auditor, the assistance need not be disclosed.)	Use of Internal Audit work is permitted.	Use of Internal Audit work is permitted.	Use of Internal Audit work is permitted. However, Use of Internal Audit work for direct assistance is not permitted.	Certifying lead auditor needs to review primary evidence
Evidence	Evidence obtained in prior engagements regarding design or operation of controls may be used to reduce the amount of testing.	Evidence obtained in prior engagements regarding operation of controls may not be used to reduce the amount of testing, even if supplemented with current year evidence.	Evidence obtained in prior engagements regarding design or operation of controls may be used to reduce the amount of testing.	Evidence obtained in prior engagements regarding design or operation of controls may be used to reduce the amount of testing.	Evidence obtained in prior engagements regarding operation of controls may not be used to reduce the amount of testing, even if supplemented with current year evidence.	Evidence obtained in prior engagements regarding operation of controls may not be used to reduce the amount of testing, even if supplemented with current year evidence.
Subservice Organization	Inclusive or carve-out method may be used.	Inclusive or carve-out method may be used. When using the inclusive method, the subservice organization must provide a description of controls and control objectives, written assertion, and letter of representation.	N/A	N/A	Inclusive or carve-out method may be used.	N/A
Anomalies	Sample testing deviations may not be labeled as anomalies.	Sample testing deviations may not be labeled as anomalies.	Sample testing deviations may not be labeled as anomalies.	Sample testing deviations may not be labeled as anomalies.	Sample testing deviations may be labeled as anomalies. The auditor may conclude that a deviation is not representative of the population.	Deviations must be explained