

Third Party Assessments: FAQs

What is a third party assessment?

A third party assessment is an audit performed on controls put in place by third party service providers. It is designed to manage the risk associated with the outsourcing of services that support critical business functions.

Why are third party assessments performed?

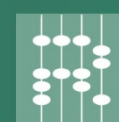
Certain legislation requires companies to implement ongoing processes to assess risks, identify and implement appropriate security measures, and be responsive to those risks. They must also update their processes continuously to address new risks. In most cases, laws do not require the use of specific 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.

What is a SAS 70?

A SAS 70 is an audit which reports on the controls at a service organization. SAS 70 stands for ‘Statement of Auditing Standard # 70.’ It was created by the American Institute of Certified Public Accountants (AICPA) of the United States.

Is SAS 70 changing?

Yes! The AICPA will be issuing a new standard for reporting on controls at a service organization. While the release date is not yet known, we do know that the new standard will differ from the current SAS 70 standard. The new standard will presumably be called SSAE 16. SSAE 16 updates and replaces the traditional SAS 70 audit, addressing the modern evolution of globalization of outsourcing trends and regulatory concerns as well as the convergence toward one set of International Financial Reporting Standards (or IFRS). SSAE 16 is similar to the ISAE 3402 (see below), but has been tailored for the U.S. business environment. Reznick Group can help you smoothly transition from a SAS 70 to the new reporting requirements of SSAE 16.



**Reznick
Group**

ACCOUNTING • TAX • BUSINESS ADVISORY

What is a BITS Shared Assessment?

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. BITS helps sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. It provides intellectual capital and addresses emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' efforts involve representatives from throughout its member institutions, including CEOs, CIOs, CISOs, and fraud, compliance and vendor management specialists.

The BITS Shared Assessment is a way for service providers to streamline the assessment process while raising the bar on security in their industry. Substantial economies can be achieved through an industry-developed process, driving continuous improvement and bringing consistency to audit practices. Many third-party service organizations have found that a Shared Assessment is a more efficient, less costly, and faster way to provide an industry-standard report on their security, privacy, and business continuity processes. Following the BITS Shared Assessment AUP (or Agreed-Upon Procedures) methodology, and using a robust and comprehensive set of assessment tools, Reznick Group's approach offers a common-sense solution for reporting on controls.

What is ISAE 3402?

ISAE 3402 is a global assurance standard for third party reporting. The intent of the global standard is to converge existing country specific standards (e.g. SAS 70 in the United States) into one common reporting standard. ISAE 3402 was designed to better meet the needs of service organization users and demands for a more global set of standards for reporting on controls at international third-party service organizations. Whether this is your first controls assessment or you are transitioning from another controls reporting approach, Reznick Group has experience performing assessments at international third-party service organizations.

What is Sarbanes-Oxley (SOX)?

SOX (section 404) mandates that all publicly-traded companies establish internal controls and procedures for financial reporting. This includes documenting, testing and maintaining procedures to help ensure effectiveness. The purpose of the bill is to reduce the possibility of corporate fraud by strengthening procedures and requirements for financial reporting.

What is PCI?

The PCI (Payment Card Industry) compliance standard was created by major credit card issuers to help protect personal information and ensure security when transactions are processed using a payment card. All members of the payment card industry (merchants, card companies and financial institutions) must comply with the standard if they want to accept credit cards. There are 6 rules related to PCI standards:

1. 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

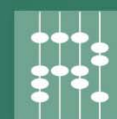
Whether you are a small retailer, a regional merchant processor, a payment gateway, or a global financial institution, Reznick Group offers services to help you achieve all aspects of your PCI compliance requirements.

What are SysTrust® and WebTrust®?

The SysTrust® service is an assurance service that was jointly developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). It is designed to increase the comfort of management, customers, and business partners with systems that support a business or particular activity. In a SysTrust® engagement, the practitioner evaluates and tests whether or not a specific system is reliable when measured against three essential principles: availability, security, and integrity. SysTrust® is based on the common framework of the Trust Services Principles and Criteria.

WebTrust® is a seal of best practices, and a new service jointly developed by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA). It enables consumers and businesses to purchase goods and services over the Internet with the confidence that vendors' web sites have historically met specific high standards for privacy, security, business practices, transaction integrity and more.

By passing independent verifications, an organization demonstrates its commitment to sound controls. The verification enables the organization to display the SysTrust® or WebTrust® seal on its website. These seals communicate the organization's commitment to security, availability, processing integrity, confidentiality, and privacy criteria that are amongst the highest in the world. The SysTrust® or WebTrust® seal can give your business a competitive advantage.



**Reznick
Group**

ACCOUNTING • TAX • BUSINESS ADVISORY