PROCESS INTEGRITY AND INFORMATION SECURITY

The Statement on Standards for Attestation Engagements (SSAE) No. 16 and the International Standard on Assurance Engagements (ISAE) 3402 are reporting standards that analyze a service organization's control over information technology and related processes. Successfully complying with these standards indicates that processes, procedures and controls have been formally evaluated and tested.

About SSAE 16 and ISAE 3402

SSAE 16, set up by the Auditing Standards Board of America, is a comprehensive approach to compliance reporting. SSAE 16 closely mirrors and complies with the first international service organization reporting standard — ISAE 3402. Developed to address the global need for third-party reporting standards, ISAE 3402 delivers a unified and transparent reporting tool.

As the standard for reporting on controls at service organizations, essentially replacing the aging Statement on Auditing Standards No. 70 (SAS 70), SSAE 16 and ISAE 3402 offer third-party validation to service providers' customers that the service provider has effective internal controls and safety measures in place, allowing them to deliver process integrity for their customers.

By successfully complying with these standards, service providers can offer customers a valuable tool for planning and streamlining the audit of their financial statements. As the authoritative guidance, SSAE 16 and ISAE allow service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format.

SSAE 16 and ISAE 3402 are primarily used by companies whose jobs impact their customers' finances (e.g., payroll management, data centers, third-party administrators, logistics, fundraising, etc.).

Type 1 versus Type 2 reporting

SSAE 16 and ISAE 3402 Type 1 reporting determines if an organization's controls are designed appropriately. For entities new to the world of reporting on controls, Type 1 reporting is typically a stepping-stone to what is ultimately required by service organizations — Type 2 reporting. Type 2 reports include the same confirmation steps involved in a Type 1 examination in addition to an evaluation of the operating effectiveness of the controls for a period of at least six consecutive months. Type 2 reporting not only includes the service organization's system description, but detailed testing of the design and operating effectiveness of the service organization's controls.

Rise in security and privacy regulations

Reporting standards have become more important in recent years as companies strive to comply with increased regulatory requirements. Following corporate accounting scandals and public concern over the security and privacy of personal information, new rules for the handling and reporting of data have emerged. Additionally, the pervasiveness of outsourcing and externalization among businesses further drives the need for SSAE 16 and ISAE 3402, as service providers are required to demonstrate adequate controls when hosting or processing data belonging to their customers.

The Sarbanes-Oxley Act is an example of legislation that has a strong impact on companies' auditing and reporting processes. Sarbanes-Oxley defines corporate responsibility for financial reporting and specifies that a company's management must issue assessments on the effectiveness of their internal controls and procedures. SSAE 16 and ISAE 3402 address the rules of internal control outlined by this legislation.

Esker's Compliance Level

Esker earned SSAE 16 and ISAE 3402 Type 1 compliance in 2012, and was recently granted SSAE 16 and ISAE 3402 Type 2 compliance by A-lign®, an independent auditing firm, in order to enhance the level of security and assurance it provides to all its on-demand customers.

Companies around the world continue to rely on Esker to host and process their business-critical documents and financial data. These standards deliver transparency to customers, help strengthen trust and give Esker a true competitive advantage, particularly in Europe where Esker is one of the few vendors to achieve dual compliance.

Control objectives

Esker has invested significant amounts of time and technology to obtain compliance based on multiple control objectives, which include:

Organization and administration: Esker's organizational structure provides an appropriate division of responsibilities to effectively communicate and separate the function and duties of providing services (e.g., formal procedures for hiring employees, job descriptions, training requirements, etc.).

Physical security and environmental safeguards: Esker data centers are controlled and restricted-access areas, staffed with third-party security personnel and digital video surveillance equipment ensuring security 24/7. Environmental safeguards include:

- Raised floor architecture to prevent water damage
- Air-conditioning systems with regular controls

- Early warning system fire detection and advanced fire suppression
- A gas evacuation system
- Regularly updated and tested security policies

Logical security: User accounts to log onto the Esker IT systems are unique and nominative, and a complex password policy is enforced. Internal access is restricted to appropriately authorized Esker employees based on their roles.

Application development and change management: All changes, including emergency maintenance and patches, relating to the Esker on Demand platform and supporting infrastructures are properly authorized, tested, implemented and documented. Esker's dedicated development teams write specifications and develop features, corrections and enhancements to all Esker on Demand products.

Incident management: Esker is equipped with an automated administration tool to provide effective incident management. This tool allows Esker to track an incident from its submission until its closure and provides assurance that system problems are properly recorded, analyzed and resolved in a timely manner.

Data management: Esker systems are backed up on a periodic basis based on identified data requirements. Procedures are in place to maintain the confidentiality and integrity of the backup media.

Monitoring and reporting: An automated reporting system continuously monitors the Esker on Demand operations and centralizes events in a monitored dashboard. Customer documents are therefore received and processed correctly and in a timely manner. International teams are organized to provide 24/7/365 monitoring and subsequent reaction.

To support these control objectives, **numerous internal controls** were conducted, such as:

- Data center security
- Infrastructure monitoring
- Logistics access
- Reliable computer operations (backup, reporting, storage and system availability)
- Recruitment

Advantages of SSAE 16 and ISAE 3402

From the service provider perspective

While SSAE 16 and ISAE 3402 reporting can be costly and time-consuming, they have definite advantages for the service providers using them. One of the many benefits is that they provide transparency and build trust with customers by having controls and operations independently verified by an unbiased third party.

From the user organization (customer) perspective

SSAE 16 and ISAE 3402 reports are extremely advantageous to user organizations as they can access a service provider's controls and safeguards. Reports that user organizations receive are full of details describing the service providers' specific controls.

Additionally, these reports offset costs for the user organization due to the fact that they will no longer have to send their own auditors to audit the service provider.

The standards are win-win endorsements for both service providers and their customers, delivering numerous advantages to both parties involved. SSAE 16 and ISAE 3402 give service providers a clear competitive advantage over other organizations that are unable to demonstrate proficiency for internal controls and safeguards. For customers, SSAE 16 and ISAE 3402 reassure them that their information is being managed in a completely secure and transparent manner.

Document Process Automation

Esker, Inc.
1212 Deming Way, Suite 350
Madison, WI 53717
Tel: 800.368.5283 | Fax: 608.828.6001
Email: info@esker.com | Web: www.esker.com

Get Social

Blog: www.quitpaper.com