SAS 70 Type II
Overview & Whitepaper

Table of Contents

Overview

Statement on Auditing Standards (SAS) No. 70, *Service Organizations,* is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A service auditor's examination performed in accordance with SAS No. 70 ("SAS 70 Audit") is widely recognized, because it represents that a service organization has been through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes.

In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. In addition, the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 make SAS 70 audit reports even more important to the process of reporting on the effectiveness of internal control over financial reporting. (*For more information see* www.sas70.com*)*

NBD, LLP

Quality Technology Services has engaged NDB, LLP (*Formerly Dupont & Morgan, LLP*) as the exclusive SAS 70 audit provider for QualityTech data center facilities in the continental US. NBD is an international accounting and consulting firm that concentrates on providing high quality, cost-effective services to meet the challenges of today's complex and competitive business environment. NBD's emphasis on SAS 70, in particular their years of experience working in and with data center providers, was an important factor in our decision to engage NDB.

How to obtain a SAS 70 "Engagement Acknowledgement Letter"

Occasionally a QualityTech customer, or prospective customer, will request a statement from our engaged CPA audit firm, NBD, indicating NDB has been engaged to perform a SAS 70 type II audit for a particular data center facility.

An Engagement Acknowledgement Letter covering all facilities being audited is available and can be provided upon request.

How to obtain a SAS 70 "Compliance Letter" or "Audit Complete Letter"

At the conclusion of an audit period for a facility, a letter is prepared by QualityTech management indicating that the facility has undergone a SAS 70 type II audit that includes a brief description of the Service Auditor's Opinion.

Compliance Letters (or Audit Complete Letters) are available and can be provided upon request.

How to obtain a full SAS 70 type II "Service Auditor's Report"

Distribution of any QualityTech SAS 70 type II Service Auditor's Report is highly controlled. The distribution incurs a $1,000 fee, necessitates the signing of an access letter dictating terms of use and disclosure, and is made in hard copy format only. Should a QualityTech customer or prospective customer request a full copy of any SAS 70 Service Auditor's Report, email support@qualitytech.com with the subject "Full SAS 70 Service Auditor's Report Request" and include the following:

> Requestor's Name
> Requestor's Company
> Requestor's Address
> Requestor's Phone Number
> Data Center and Year

QualityTech management believes the nominal charge of $1,000 is not a deterrent for user organizations who intend to "carve out" the findings detailed in the Service Auditor's Report for inclusion into their own yearend statements. The fee is intended to help protect the value of the report contents and limit the exposure of the competitive information contained therein.

In lieu of a full SAS 70 type II Service Auditor's Report distribution, the QualityTech audit team can review in person or via conference call & Webex any complete SAS 70 type II audit report with an existing user organization and/or their auditor. Conference calls are charged at the rate of $125 per hour and in person reviews are performed at a flat rate of $300 with a 2 hour maximum. Note, however, that in person reviews are only performed at the following data center facilities:

> Atlanta, GA (Metro)
> Suwanee, GA
> Jersey City, NJ
> New York, NY

What does it cost to receive multiple distributions of an individual data center's SAS 70 type II Service Auditor's Report?

QualityTech restricts the duplication of any distributed SAS 70 Service Auditor's Report through the language of an "Access Letter" executed by the report recipient organization. In some instances, user organizations have a need for more than one copy of an individual data center's SAS 70 Service Auditor's Report. The schedule below reflects the fee charged for copies of the same report that are for the same data center and same time period:

> First Copy = $1,000
> Second Copy = $500
> Subsequent Copies = $200

QualityTech SAS 70 type II Certified Data Center Facilities

Atlanta, Georgia (Metro)
Jersey City, New Jersey
Lenexa, Kansas – Bond St.
Miami, Florida
New York, New York – Manhattan
Overland Park, Kansas – Foster St.
Santa Clara, California
Suwanee, Georgia

Type I vs. Type II defined

A Type I report describes the service organization's description of controls at a specific point in time *(e.g. June 30, 2007)*. A Type II report not only includes the service organization's description of controls, but also includes detailed testing of the service organization's controls over a minimum six month period *(e.g. January 1, 2007 through June 30, 2007)*.

In a Type I report, the service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date, and (2) whether the controls where suitably designed to achieve specified control objectives.

In a Type II report, the service auditor will express an opinion on the same items noted above in a Type I report, and (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

How does QualityTech benefit from being SAS 70 type II certified?

QualityTech receives significant value from having a SAS 70 engagement performed. A Service Auditor's Report with an *unqualified opinion* issued by an Independent Accounting Firm, such as NBD, differentiates QualityTech from its peers by demonstrating the establishment of effectively designed control objectives and control activities. A Service Auditor's Report also helps QualityTech build trust with its user organizations.

Without a current Service Auditor's Report, QualityTech may have to entertain multiple audit requests from its customers and their respective auditors, thus placing unnecessary strain on QualityTech management and resources. A Service Auditor's Report ensures that all QualityTech customers and their auditors have access to the same information that, in most cases, satisfies the user organization's auditor's requirements.

Background text taken from www.sas70.com

QualityTech SAS 70 engagements are performed by control oriented professionals who have experience in accounting, auditing, and information security. A SAS 70 engagement allows QualityTech to have its control policies and procedures evaluated and tested (in the case of a Type II engagement) by an independent party. Very often this process results in the identification of opportunities for improvements in many operational areas.

How do user organizations benefit from QualityTech's SAS 70 type II status?

User organizations that obtain a Service Auditor's Report from QualityTech receive valuable information regarding QualityTech's controls and the effectiveness of those controls. The user organization receives a detailed description of QualityTech's controls and an independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively for the defined audit test period (in the case of a Type II report).

QualityTech recommends user organizations provide a SAS 70 type II Service Auditor's Report to their own auditors. This will greatly assist the user organization's auditors in planning the audit of the user organization's financial statements. Without a SAS 70 type II Service Auditor's Report, the user organization may incur additional costs in sending their auditors to QualityTech to perform their own audit procedures.

When is a "Service Auditor's Report" available?

QualityTech SAS 70 type II Service Auditor's Reports typically cover a 10 month period beginning January 1 and, barring any unforeseen circumstances, are generally available approximately 8 weeks after the completion of any specific facility's testing period. For a January 1 through October 31 testing period, a report is typically available by December 31.

By engaging in this generally accepted SAS 70 practice, publicly owned QualityTech customers may review and include QualityTech's SAS 70 type II Service Auditor's Report in their own yearend financial statements, further enhancing the value of QualityTech's Service Auditor's Report to user organizations and their auditors.

How to obtain a "Management Representation Letter" for the remaining 61 days of the year after a 10-month audit

Management Representation Letters for each facility indicating 'No material change, for the controls in operation on October 31, occurred during the period of November 1 through December 31' are available and can be provided upon request. In the event material changes take place in any facility during the 61 days subsequent to the audit, a Management Representation Letter detailing the material change(s) and the justification for the change(s) will be made available and provided upon request.

QualityTech SAS 70 type II audit scope and control objectives

QualityTech's SAS 70 type II audit scope includes every operational unit of the organization except for finance. Accounting, inventory, logistics, payroll, cash management, etc. are all components of a financial audit; however, they are not in scope for a SAS 70 type II audit.

During every QualityTech SAS 70 type II audit testing period, NDB identifies approximately 200 controls, presented by QualityTech management, which result in the testing of thousands of individual attributes. Detailed below is a list of control objectives included in SAS 70 type II audits of QualityTech data center facilities as applicable:

E1 (1.0)-Organization and Administration (Executive Tone)
> *Controls provide reasonable assurance that management instills a positive and effective corporate tone, organizational goals and objectives are discussed on an outline basis, and corporate policies and procedures are documented and distributed accordingly.*

HR1 (1.1)-Organization and Administration (Human Resources)
> *Controls provide reasonable assurance that employees hired are qualified individuals assigned to duties compatible with their skill sets.*

CCP (2.0)-Client Contract Process
> *Controls provide reasonable assurance that the client contract process is fulfilled according to various requirements, including the completion of necessary documentation, and carried out in a timely and complete manner.*

CPP (2.1)-Client Provisioning Process
> *Controls provide reasonable assurance that the client provisioning process is implemented, managed, and administered as contracted.*

IPP (2.2)-Internal Provisioning Process
> *Controls provide reasonable assurance that the internal corporate provisioning process is implemented, managed, and administered as contracted internally.*

IM (3.0)-Incident Management (Client Facing)
> *Controls provide reasonable assurance that incident management/support services are provided to clients for properly monitoring, evaluating, and supporting managed services and systems, ensuring availability and timely problem resolution.*

IM (3.1)-Incident Management (Internal)
> *Controls provide reasonable assurance that incident management/support services are provided to the internal organization for properly monitoring, evaluating, and supporting managed services and systems, ensuring availability and timely problem resolution.*

CCM (4.0)-Change Control Management (Client Facing)

Controls provide reasonable assurance that configuration/change management activities for client facing Network Services, Systems, Monitoring Services, Mass Storage, Security Services, and Facilities are authorized, approved, administered, implemented and documented.

CCM (4.1)-Change Control Management (Internal)

Controls provide reasonable assurance that configuration/change management activities for internal Network Services, Systems, Monitoring Services, Mass Storage, Security Services, and Facilities are authorized, approved, administered, implemented and documented.

LS1 (5.0)-Logical Security (Policies/Procedures & Passwords/Rules)

Controls provide reasonable assurance that Logical Security policies and procedure are documented and distributed to all employees, and password complexity rules are in place for all systems, network, and application devices throughout the organization.

LS2 (5.1)-Logical Security (Provisioning & Access Rights)

Controls provide reasonable assurance that new and existing employees are properly provisioned onto company-wide systems, network and application devices, and access rights are commensurate with roles and responsibilities within the organization.

LS3 (5.2)-Logical Security (Access Removal & Termination Procedures)

Controls provide reasonable assurance that terminated employees are properly removed from all systems, network and application devices throughout the organization.

NS1 (6.0)-Network Security

Controls provide reasonable assurance that data transmissions are complete, accurate and secure, and all systems are configured to prevent and detect unauthorized access attempts and attacks.

COP (6.1)-Computer Operations

Controls provide reasonable assurance that data files are backed up in a timely and complete manner, back up logs are generated for appropriate review, and critical system maintenance activities are undertaken on a regular basis.

CG (7.0)-Corporate Governance

Controls provide reasonable assurance that a documented Corporate Governance initiative is implemented and utilized throughout the organization.

PS2 (8.0)-Physical Security

Controls provide reasonable assurance that logical and tangible physical access to computer equipment, storage media, corporate resources and business premises are limited to properly authorized individuals.

ES2 (9.0)-Environmental Security

Controls provide reasonable assurance that critical mechanical and electrical computer equipment, storage media, corporate resources and business premises are protected from environmental risks and threats.

ES3 (9.1)-Facility Inspection and Documentation

Controls provide reasonable assurance that all critical mechanical and electrical components are routinely inspected, complete with documentation, and all other major infrastructure components supporting the daily operations of the data center are observed and documented accordingly.

SAR (10.0)-Shipping and Receiving Activities

Controls provide reasonable assurance that shipments received are examined and handled accordingly, recorded appropriately, and stored in specific areas.

ER (11.0)-Emergency Response

Documented emergency response initiatives exist for assisting the facility in planning, preparing for, and undertaking any emergency activities as needed.

BCM (12.0)-Business Continuity Management

Documented Business Continuity Management initiatives exist for assisting the facility in planning, preparing for, and undertaking any business continuity activities as needed.