

SAS 70 vs. an ISO 27001 ISMS



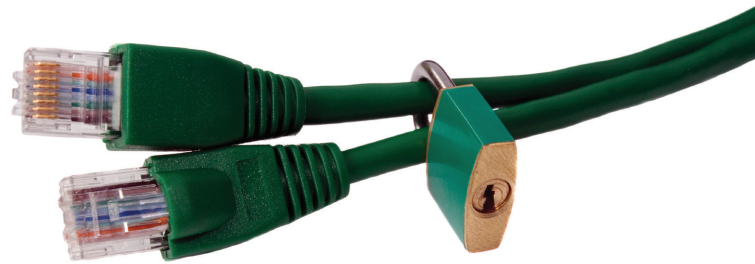
Network Computing Architects, Inc.

A compliance comparison to SAS 70

Many organizations are asked to provide assurance of information security, information technology, and controls to clients, business partners, or other third parties. Previously, the SAS 70 Service Auditors Report was used to meet these requirements. Over the last several years, the ISO 27001 standard has been leveraged within many organizations to provide business assurance.

What is SAS 70?

SAS 70 is an auditing standard designed to enable an independent auditor to evaluate and issue an opinion on a service organization's controls. The audit report can be shared with the service organization's customers and their respective auditors. The service organization is responsible for describing its control objectives and control activities that would be of interest to user organizations and the respective user auditors.



What is ISO 27001?

Information is a critical asset to the operation and perhaps even the survival of your organization. ISO27001 is a standards-based approach for building Information Security Management Systems (ISMS) that was developed, and is supported internationally, by members of the International Organization for Standards (ISO). ISO 27001 evolved from British Standard (BS) 7799 and is intended to provide a framework for managing information security.

Why an ISMS?

Given that the ISO 27001 standard requires ongoing management and enhancement, the P-D-C-A (Plan-Do-Check-Act) must be followed not only for what is in place today, but for future changes as well. Information is critical to the operation and perhaps even the survival of your organization. Being certified to ISO 27001 will help you to manage and protect your valuable information assets.



SAS 70 vs. an ISO 27001 ISMS

How Network Computing Architects Can Help!

NCA is a Pacific Northwest regional consulting firm that has been in business for over 15 years and specializes in providing information security management solutions and services. The primary objective of the NCA's professional services practice is to assist our clients with minimizing the likelihood that threats and risk will exploit vulnerabilities to critical assets. In order to be effective at this task, we have to first analyze, assess and audit the client's Information Security components to ensure that we obtain enough knowledge of their unique environment to act as a trusted advisor. As a trusted advisor, NCA works with our clients to identify their available information security budget and appropriate use of that budget.

Some of NCA's services include; Asset Identification, Security Analysis, Vulnerability Assessments, Security Program Development, Penetration Testing, Security Architecture and Implementation Services for controls such as firewalls, VPN's, SIEM's, encryption, IPS, Web and Mail gateways.



NCA's ISO 27001

NCA achieved ISO 27001:2005 certification in December of 2007. The scope of NCA's ISMS is client confidential information within the Information Security Practice.



ISO 27001- 012 1207

ISO 27001 Associate Consultancy

British Systems Institute (BSI), the certification body for an ISO 27001:2005, has set up an Associate Consultant partnership program in which to refer clients who are seeking ISO 27001 certifications. BSI offers Associate Consultancy status to organizations that they believe have a credible and acceptable service in terms of value and performance to consult other organizations in developing an ISMS.

NCA is the first associate consultant in the United States to achieve their own ISO 27001 Certification.

Comparison Between SAS 70 and ISO 27001

METHODOLOGY	SAS 70	ISO 27001
Intended Use	Audit Guidance for Minimum Requirements	Management Requirements
Assurance Method	Service Auditors Report	International Certification
Scope	Financial focus (statements & related systems)	Enterprise focus for any and all forms of information or systems
Stance	Reactive	Proactive
Risk Model	"Maximum" risk, then reduce	Identify, Measure & Address
Control Definition and Measurement	Tested in "Type 2", but not addressed in "Type 1"	Required by ISMS
Continuous Improvement	Not Addressed	Continuous Updates, Plan-Do-Check-Act



Network Computing Architects, Inc.

855 106th Ave NE | Bellevue WA 98004 | 877-566-9622

Spokane WA 425-766-6706 | Portland OR 888-968-5434

Los Gatos CA 408-342-9900 | Las Vegas NV 702-457-7990

www.NCAnet.com

COMPLIANCE COMPARISON