

ISO 27001: the Standard for Due Care



Network Computing Architects, Inc.

The International Standard for ISMS

Businesses are increasingly aware of the need to address governance, risk, and compliance. However, most organizations are challenged to adopt an integrated approach to these three areas.

ISO 27001 is a certifiable, international standard to produce evidence that sufficient controls are in place to address these areas for management, auditors, and customers. ISO 27001 defines this approach as an Information Security Management System or an "ISMS."

Aligning your business with risks and technology

Using a standardized framework provides a consistent and clear mapping of business objectives, applicable risks to the organization and resource expenditures regarding risk management, avoiding expectation gaps or communication issues between management and security operations personnel. A properly-defined ISMS will provide budgetary guidance regarding applicable risk and your organizations needs against a measured baseline of your organization's currently implemented and managed controls.

Demonstrate compliance with legal and contractual obligations

The value of a standardized framework can demonstrate compliance to auditors. ISO 27001 is an internationally recognized standard approach that encompasses all current and emerging compliance and regulatory requirements, clearly mapping the measured controls against specific compliance objectives. This allows the framework to provide continuous visibility, on both a practical and compliance level, into the interplay between defined business objectives, risk management, documented control design and ongoing control operations.

Increasing effectiveness through a repeatable and measurable approach

ISO 27001 is a management system requiring continual process improvement for information security. An organization must monitor and improve based on objective measurements. By granularly measuring risk and control effectiveness the system can be tuned on defined acceptable levels of risk. The repeatable processes establish a control library that can be leveraged to address compliance in a unified approach. This unified approach reduces cost of implementation and operating controls to address your governance, risk, and compliance requirements.

ISO 27001 DEMONSTRATES INDEPENDENT ASSURANCE OF:

- Corporate governance
- Business continuity
- Laws and regulations are observed
- Meeting contractual obligations
- Organizational risks are identified, assessed and managed
- Formalized information security processes, procedures and documentation
- Senior management commitment to information security
- Continuous monitoring of performance and improvement

Reasonable Assurance is a concept of proportional security that is weighted to the individual businesses requirements for asset protection. Every information asset has a value that can be quantified by its level of Confidentiality, Integrity of the information, and Availability requirements. Reasonable assurance creates management confidence by accurately prescribing Information Security within a business.

Through the guidance of implementing an Information Security Management System (ISMS) based on the British Standard Institute's (BSI) ISO/IEC 27001:2005, NCA works with each client to achieve Reasonable Assurance that their business risks are mitigated.

ISO 27001: the Standard for Due Care

About NCA

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.

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 Consultant

British Systems Institute (BSI), the certification body for an ISO 27001:2005, has set up an Associate Consultant Program 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.

Protecting your data with care

At NCA we are strongly committed to fulfilling the vision of being the industry leader in providing premier security consulting services and building Information Security management Systems (ISMS). Our commitment is demonstrate by being the only ISO 27001 Associate Consultants in the United States to be ISO 27001:2005 certified (IS 506700).

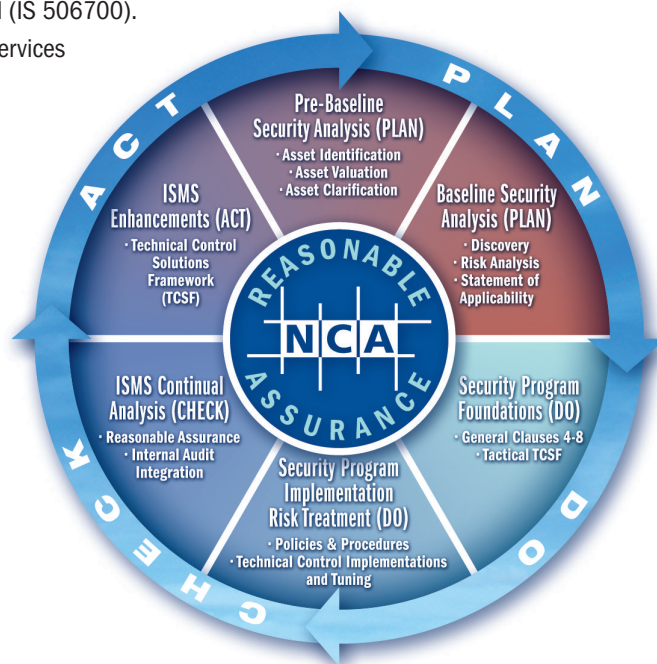
NCA demonstrates the care to protect our client's data through the same services and products that we recommend to our clients.

ISO 27001 service offering

NCA can help your organization achieve ISO 27001 certification to demonstrate independent assurance of governance, risk, and compliance.

NCA's service offerings encompass a complete security management program guiding you from initiation to certification.

NCA has developed partnerships with industry experts to automate of many of the controls and requirements of ISO 27001.



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

MANAGEMENT FRAMEWORK