



NetAUDIT™ Security Assessment for ISO/IEC 17799:2005 Security Standard

Measuring security controls against ISO standard for SOX, GLB, and other assessment requirements

How do you know if you have done enough?

Organizations today employ a wide range of security controls to manage risk of loss to information systems and facilities. Although no company can be 100% secure, most strive to implement the controls that are relative to significant threats. But how do you know if you have done all that is commercially reasonable to address foreseeable security events?

Regulations such as SOX and GLB have put in place minimum security control requirements that mandate proactive measures be taken to ensure the confidentiality, integrity and availability of protected information. How do you prove to internal/external auditors that you have met the regulatory requirements of security and followed best practices?

The rising number of recent security events among high profile businesses indicate that the size of the organization does not dictate full-proof security. How do you demonstrate due-diligence in securing your company to your board,

shareholders, customers, and employees?

NetAUDIT ISO/IEC 17799 Assessment

NetAUDIT is Spohn's security assessment service for identifying threats, risk, vulnerabilities and commercially reasonable improvements. NetAUDIT deploys proven people, processes and tools to assess the effectiveness of a company's security controls against security best practices.

ISO/IEC 17799 is the internationally-recognized standard for enterprise security best practices. It documents a comprehensive set of security controls any business can implement to prepare for and address foreseeable events. By using ISO/IEC 17799 within NetAUDIT, you can be confident that you have used an Internationally recognized "Best Practices" for security to protect your enterprise, provide proof of regulatory compliance and demonstrate due-diligence.

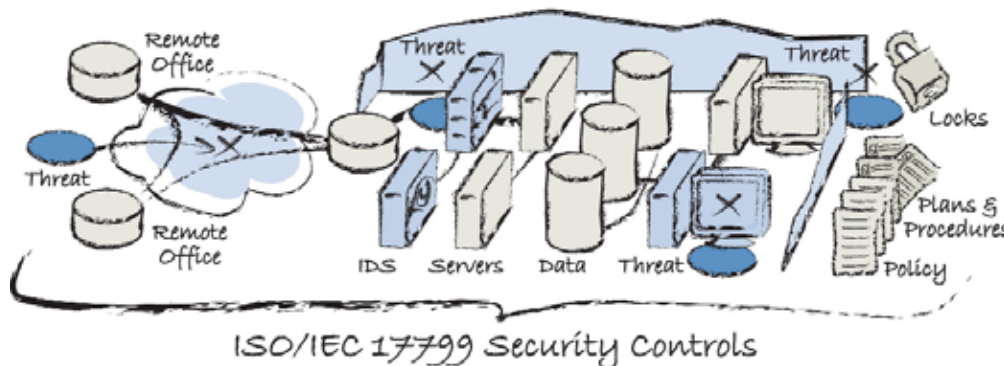
Tailor NetAUDIT ISO/IEC 17799 to meet specific assessment requirements

NetAUDIT can assess an organization

Benefits

- Meet security requirements of Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLB) and other regulations
- Determines effectiveness of security controls compared to an Internationally recognized security standard (Best Practice)
- Demonstrates due-diligence in an organization's efforts to identify threats, weaknesses, vulnerabilities, and gaps in compliance
- Provides proof of compliance with security requirements for most legislation
- Builds confidence with stakeholders, shareholders, board members, and employees
- Fits within standard framework for risk management

Figure 1: Enterprise security controls are measured against ISO/IEC 17799 standards, checked for gaps and regulatory compliance, and assessed for vulnerabilities



against the entire ISO/IEC 17799 security standard. However, this approach may be more detailed than some companies need as ISO/IEC 17799 is comprised of 133 unique security controls across eleven domains:

- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Informational Systems Acquisition, Development and Maintenance

- Information Security Incident Management
- Business Continuity Management
- Compliance

As an alternative, companies can select a subset of security controls applicable to their organization for assessment against the related ISO/IEC 17799 security standard.

Spohn's assessment may be custom tailored to meet specific requirements necessary for your organization, using any combination of domains and related controls. This assessment can be designed to meet multiple regulatory and due-diligence requirements.

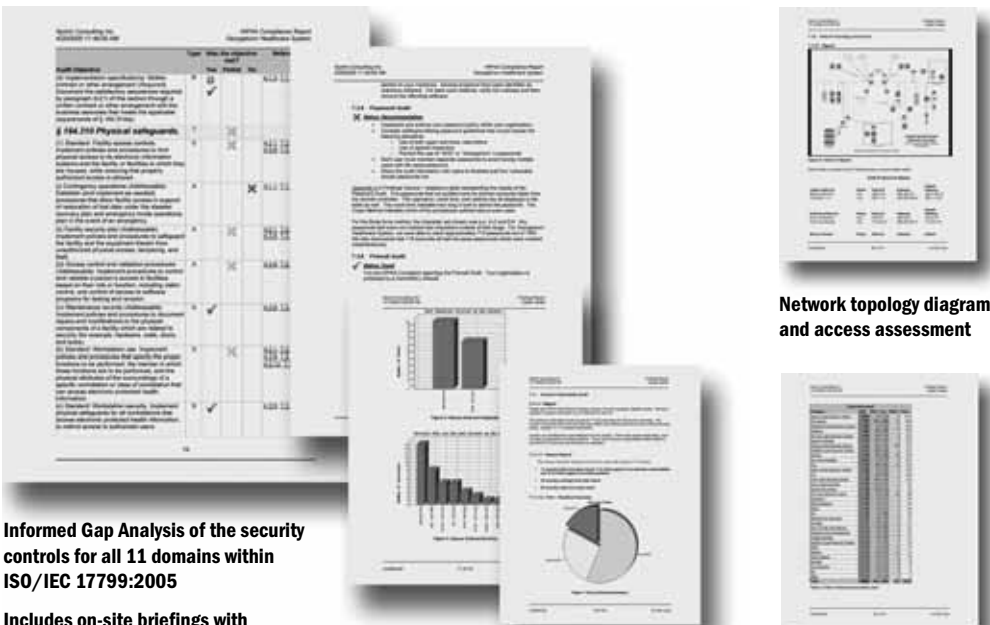
Figure 2: NetAUDIT ISO/IEC 17799 Security Assessment provides comprehensive analysis, documentation and remediation recommendations for determining and planning commercially reasonable improvements to security

Features

- **Internationally recognized as the most comprehensive standard for security**
- **133 unique security controls are inspected**
- **Tailorable to meet company-specific security control assessment requirements**
- **3 volume deliverables provided in printed bound copies and in digital Adobe® PDF and Microsoft® Word format on CD-ROM**
- **Executive-level report provides summary of findings and recommendations**
- **Indepth finding reports provide security, IT management and implementation teams detailed inspection results and technical data including vendor neutral recommendations for remediation**

NetAUDIT ISO/IEC 17799 Security Assessment is a member of a suite of security services for corporate due diligence and regulatory compliance.

For further information please contact our corporate office at 512.685.1000



Informed Gap Analysis of the security controls for all 11 domains within ISO/IEC 17799:2005

Includes on-site briefings with executive and technical staff to review findings and recommendations

Network topology diagram and access assessment

External vulnerability test and findings assessment



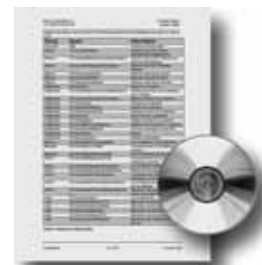
Vulnerabilities scan listing issues, scores and results



Physical security controls are assessed and photographed



Findings report with vendor-neutral recommendations



Findings & Recommendations with CD-ROM database