

Information Security Risk ASSESSMENT

Given today's dynamic Internet environment and emerging networking technologies, businesses today must strive to maintain comprehensive, proactive, and compliant safeguards of critical company assets.

Risk assessment tools and practices and a sound information security program are paramount for maintaining a company's reputation and data security.

A formal risk assessment process should be the point at which senior management and the security staff come together. Senior management focuses on regulatory compliance, business productivity, and the bottom line. The risk assessment can help articulate the costs of operating with ineffective or inappropriate security controls and meet Sarbanes-Oxley responsibilities.

Secure Enterprise Computing will work with key people from your organization to assess your organization's network security and provide recommendations for improving your overall security posture.

The main objectives of the assessment are communicated as a review of:

- How effectively the organization is maintaining security, integrity, and confidentiality of critical company assets.
- How the organization is protecting against anticipated, reasonable threats or hazards.
- How well the organization is protecting against unauthorized access to information.

Assessment Methodology - Our experienced security engineers will use information gathered through a series of interviews, software tools, our industry experience, and our understanding of industry best practices and standards such as the Code of Practice for Information Security Management (ISO 17799), the NIST Special Publication 800-42 and the FBI/SANS Top 20 Vulnerability List to assess the state of your network.

The evaluation focuses on the following areas:

- Business Continuity
- System Access Control
- System Development and Maintenance
- Physical and Environmental Security
- Compliance
- Personnel Security
- Organizational Security
- Operations Management
- Policy

This assessment measures and analyzes an organization's susceptibility to outside threats by verifying the integrity of the existing security controls.

Our assessment methodology identifies vulnerabilities within the organization, advises on the risk, and provides prioritized recommendations, allowing you to effectively secure operations in today's dynamic environment.

At the end of this assessment, executive management will be provided with:

- An appreciation of the threats to assets
- An articulation of vulnerabilities and weaknesses
- A strategy for prioritized remediation

Our goal is to allow both senior management and information security staff the ability to understand the real risks faced by the organization.