

A3I Security Solutions Scope

Information Technology Security Assessment

NetCentric Technology's A3I Security Solutions is a comprehensive review and evaluation of the technology, people and processes that provide for an organization's information security. Security is equal to managing risk. Controls are the technologies and processes that are designed and implemented to minimize risks. NetCentric Technology's A3I Security Solutions is designed to determine whether or not various technical, operational and management controls are present and to evaluate those controls for their effectiveness in protecting the confidentiality, integrity and availability of a corporation's information assets.

A3I Security Solutions from NetCentric Technology examines an organization's strategic direction and initiatives with respect to security requirements. We evaluate the effectiveness of existing security systems and processes in addressing actual business requirements for securing information assets. We determine what immediate threats and risks exist and evaluate whether the current security environment can protect against today's risks while supporting future needs and goals of the business.

The Scope of the A3I Security Solutions Includes a Review and Evaluation of the Following Critical Areas:

SECURITY POLICIES, PROCEDURES, OPERATIONS AND MANAGEMENT

- Information Security Policy Document
- Security Organization
 - Information Security Infrastructure
 - Security of 3rd Party Access
 - Outsourcing
- Asset Classification and Control
 - Accountability for Assets
 - Information and Data Classification
- Personnel Security
 - Security in Job Definitions
 - User Training and Awareness
 - Security Incident Response Procedures
- Business Continuity Management

PHYSICAL AND ENVIRONMENTAL SECURITY

- Secure Areas
 - Physical Security Perimeter
 - Physical Entry Controls
 - Office/Room/Facility Security
- Equipment Security
 - Equipment
 - Power Supplies
 - Cabling
- General Environmental Controls

ACCESS AND AUTHENTICATION CONTROLS

- Business Requirements for Access Control
- User Access Management
- User Responsibilities
- Network Access Control
- Operating System Access Control
- Application Access Control
- Monitoring System Access and Use
- Mobile Computing and Remote Access

NETWORK AND SYSTEMS ARCHITECTURE, CONFIGURATION AND MANAGEMENT

- Security Requirements
- Network Architecture Review and Analysis
 - Internet Perimeter Analysis
 - Remote Access Points
 - Core Internal Systems Analysis
- Network Perimeter Vulnerability Testing
 - Firewall Scans
 - Router Scans
 - Intranet Scans
 - Web Server Scans
 - Modem Scans
- Internal System Vulnerability Testing
 - Individual Server and Operating System Scans (Database, Application, Domain, Messaging and Core Services Servers)

ELECTRONIC EXCHANGE INFORMATION

- Electronic Commerce Security
 - Authentication
 - Authorization
 - Security of Information in Transit
- Electronic Mail security
- Anti-Virus Protection Against Malicious Software
- Internal Usage/Content Monitoring

TECHNOLOGY OPERATIONS MANAGEMENT

- Operating Procedures Documentation Review
 - Change Controls
 - Incident Management: Identification/Containment/ Eradication/ Recovery/Follow-Up
- Information Backup Strategies and Procedures
- Operations Housekeeping
 - Log File Review and Maintenance
 - Media Handling and Security
 - System Documentation

