

A3I Security Solutions Approach

Tailorable Processes

Guided by the formalized framework outlined in the scope of the A3I Security Solutions, the specific tasks associated with a security assessment vary based on the complexity of each individual business. Our A3I Security Solutions methodology is based on Department of Defense "Defense in Depth Strategy", National Security Agency (NSA) Information Assurance Technical Framework and knowledge of commercial security best practices. The tailorable processes used by NetCentric to gather data to identify your organization's risks are listed below:

- **Interview key management personnel ("owners" of systems and technologies)** - assess specific security needs and expectations
- **Interview key information technology personnel** - assess implemented security practices and perceived expectations
- **Evaluate existing security policy documentation** - documentation is examined to assess the focus and goals of a company's security posture
- **Evaluate known regulatory requirements defined by required external entities** - recognize mandatory and optional security procedures
- **Evaluate network topology for "security conscious" design practices** - evaluate from a physical and logical design level for vulnerabilities
- **Evaluate intranet accessibility** - evaluate established internet access technologies, which are key enforcement points for any security system
- **Perform perimeter network scans** - scan to reveal services and or configurations that present a security risk on perimeter equipment
- **Perform perimeter penetration testing** - "ethically hack" to expose undesired responses from perimeter equipment
- **Perform host content vulnerability testing** - Implement sophisticated scanning tools to reveal security risks on specific network hosts
- **Perform database vulnerability testing** - Run sophisticated scanning tools to reveal security risk to specific network databases and their content
- **Perform network element vulnerability testing** - Run sophisticated scanning tools to reveal security risks on specific network elements including firewalls, routers, and switches
- **Develop Security Risk Assessment** - perform a risk assessment that develops and assigns risk levels to identified vulnerabilities given an organization's security posture and processes
- **Develop Security Architecture Blueprint** - Provides a roadmap for an organization to proactively manage and reduce these security risks through product solutions, training, process improvements and policy development
- **Implement** - Provide engineering support in securing your business processes and provide continuous security engineering services to minimize your risks



NetCentric Technology, Inc.