The AccessIT Group Mission

At AccessIT Group our mission is to enable our clients' full confidence that their IT security infrastructure will provide them uninterrupted business continuity and productivity.

To meet our mission we strive to maintain technological leadership using structured methods to ensure that complex integration challenges are completed on time and on budget.

We work to design and implement IT security solutions that keep our clients ahead of the curve in the current world of regulatory compliance driven IT security.

From design and implementation to IT security compliance and training, we provide our clients with a single point of contact for all their security needs.

Our Locations

Corporate Office & Training Center
20106 Valley Forge Circle
King of Prussia, PA 19406
610.783.5200
Fax: 610.783.5151

NY Regional Office
112 West 34th Street, Suite 17049
New York, NY 10120
212.946.2886
Fax: 212.208.2620

NJ Regional Office
115 Route 46 West
Building E, Suite 35
Mountain Lakes, NJ 07046
973.316.6016
Fax: 973.394.5602

DC/Baltimore Metro Regional Office
9256 Bendix Road
Suite 306
Columbia, MD 21045
410.782.4800
E-Fax: 410.558.6535

www.AccessITGroup.com / TRM@AccessITGroup.com

TRM

Technology Risk Management

Technology Risk Management (TRM) is the comprehensive practice of proactively guarding intellectual property and critical infrastructures.

www.AccessITGroup.com / TRM@AccessITGroup.com

Vulnerability Assessments

Vulnerability Assessment Services

- External Network Testing
- Internal Network Testing
- Application Testing
- Wireless Testing
- Physical Access
- Demon Dialing

Deliverables

- Vulnerability Discovery
- Root Cause Analysis
- Identify False Positives
- Validate Vulnerabilities
- Provide a Remediation Roadmap
- Technical Summary
- Executive Summary

Vulnerability Assessment and Vulnerability Testing are essential resources within AccessIT Group's TRM Services. Continuously conducting assessments and tests of your high-risk information assets helps to proactively fortify your environment against emerging threats and maintains an effective information security program.

A vulnerability assessment provides insight into the safety and security of your critical assets and information. Our assessment team is comprised of experienced Certified Information System Security Professionals with diverse backgrounds and expertise. Our security professionals use up to date assessment tools, methods and practices to perform a holistic inspection of your network, systems and known points of access.

Assessment testing eposes and examines points of vulnerability in your environment and assesses the potential damage that would result if a threat were to breach your company's gateways. After reporting vulnerabilities, we deliver custom remediation plans for each vulnerability discovered.

Compliancy Audits and Services

TRM offers a wide range of Compliancy Audits and Services including but not limited to:

- Development and Execution of IT Strategy
- Development and implementation of IT cost reduction strategies
- Design and implementation of IT risk management programs including policy, process, internal controls, procedures, metrics, reporting and training
- Facilitation of IT risk assessments
- Design and implementation of IT security & compliance programs including policy, process, internal controls, procedures, metrics, reporting and training
- Design and documentation of IT security policies providing alignment with laws, regulations, compliance requirements and technology.
- Specialization of IT Audits & Compliance reviews (SOX, HIPAA, GLBA, PCI, and DataPrivacy)
- IT due diligence for mergers, acquisitions, divestitures, and joint ventures

Contact our sales team at Sales@AccessITGroup.com and we can customize a compliancy review that best meets your company's needs.

Please visit our website:

www.AccessITGroup.com

Or contact:

TRM@AccessITGroup.com

AccessIT® GROUP, INC.

Application Security

Application Security Services

- Vulnerability Assessments
- Penetration Testing
- Application Architecture Review
- Application Flow Review

Deliverables

- Vulnerability Discovery
- Root Cause Analysis
- Identify False Positives
- Validate Vulnerabilities
- Provide a Remediation Roadmap
- Technical Summary
- Executive Summary

Application Security assessments test known vulnerabilities against an unknown code base. Custom applications may include critical e-commerce websites, internal databases and systems that are considered "custom" or proprietary.

A comprehensive application assessment can provide insight into multiple components. This can include application code vulnerabilities, transport layer issues, application flow vulnerabilities and architecture design flaws.

It is vital that all areas be assessed to ensure that the application does not expose the underlying servers and software to an attack. This includes trusted or malicious users attempting to access, modify or destroy data or services within the system.

Threat Mapping Assessments

What is a Threat Mapping Assessment?

Our Team of Certified Penetration Testers will perform a Threat Mapping assessment of your network. When the goal is to define the potential attack scenarios that have the greatest impact on your company's infrastructure.

How do we perform a Threat Mapping Assessment?

Our Engineers will combine an external and internal vulnerability assessment/penetration test along with configuration data from network firewalls, routers, switches, and host-based firewalls. This will provide a complete overview of your network security posture. We will analyze possible attack scenarios proactively and completely. This complete solution will help discover weaknesses in the network, evaluate the impact of a combination of exploits and recommend changes based on the following:

- Modeling both hosts and network infrastructure devices such as firewalls and routers
- Mapping reachability from attackers to hosts
- Identifying exploitable paths through the network where vulnerabilities are reachable
- Building a clear path of possible attacks including multi-hop attacks

We will provide your company a proactive remediation plan that will prioritize vulnerabilities by placing them in your overall network context and recommending actions that will improve security the most within your overall IT Security Posture.

Please visit our website:

www.AccessITGroup.com

Or contact:

TRM@AccessITGroup.com

AccessIT® GROUP, INC.

Social Engineering

Social Engineering Services

- USB Drops
- Phishing Exercises
- Employee Testing
- Physical Access Controls
- Dumpster Diving

Deliverables

- Vulnerability Discovery
- Root Cause Analysis
- Identify False Positives
- Validate Vulnerabilities
- Provide a Remediation Roadmap
- Technical Summary
- Executive Summary

Social Engineering addresses non-technical intrusions which rely heavily on human interaction. It often involves tricking other people into breaking normal security procedures.

Social Engineering usually involves a deception: trying to gain the confidence of a trusted source by relying on his or her natural helpfulness and weaknesses. Social Engineering techniques include eavesdropping and appealing to the target's vanity or their authority as well as physical security bypass and searching refuse bins for sensitive information.

Our Social Engineering services are offered as part of our comprehensive Technology Risk Management practice to maximize total information security.

Penetration Testing

A penetration test evaluates the security of a computer system or network by simulating an attack from a malicious source. It can be performed through full disclosure of the topology and environment (white box) or with no knowledge of the environment (black box).

The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, known and unknown hardware flaws, operational weaknesses, or technical countermeasures.

The analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner along with an assessment of their impact and a customized remediation plan to mitigate the risk. The intent of a penetration test is to determine the feasibility of an attack and the amount of business impact of a successful exploit, if discovered.

Penetration Testing Services

- External Network Penetration Testing
- Internal Network Penetration Testing
- Application Penetration Testing
- Wireless Penetration Testing
- Physical Access Penetration Testing

Deliverables

- Vulnerability Discovery
- Identify False Positives
- Validate Vulnerabilities
- Provide a Remediation Roadmap
- Technical Summary
- Executive Summary

Please visit our website:
www.AccessITGroup.com
Or contact:
TRM@AccessITGroup.com

AccessIT® GROUP, INC.