



In today's Internet connected world, businesses know that a strong perimeter, as well as proper internal protection is **vital to defending against threats** to corporate security.

Information security assessments should never be limited to just simple operating system and application vulnerability testing. That is why BAI Security provides comprehensive testing in all major key risk areas to ensure that results of every audit **accurately** reflect the security posture of the organization and provide a remediation roadmap to **compliance** and fortification.

BAI Security provides one of the most comprehensive and **cost-effective** Security Audit solutions for regulated and non-regulated industries alike.

Vulnerability Testing: As a core component of any information security audit, BAI Security provides comprehensive vulnerability scanning of all areas associated with your production systems, including the core operating system, applications, and the underlying communication network. There are nearly 10 thousand individual tests conducted during the process. Using proven methodologies developed by BAI Security and based on regulatory standards, the data collected from the scanning process is then correlated and evaluated to determine severity and ensure validity.

Operating System Security Assessment: Unused accounts, active accounts from terminated employees, excessive use of administrative rights, improperly assigned permissions, use of non-standard password expiration and complexity, poor use of security groups, no monitoring of failed logon attempts are all just a few of the key risks identified in this important audit option. The Operating System Security audit takes a detailed look at the design, implementation, administration, and monitoring of servers and core systems to ensure compliance, protection, and business continuance.

Social Engineering Assessment: Social Engineering has long been one of the most common means for hackers to gain vital information about internal systems. Unfortunately, in many environments internal users will divulge sensitive information about systems and/or user-accounts to unauthorized individuals when approached with a cleverly crafted dialog by an outsider to the organization. With this in mind, it is extremely important to periodically evaluate your end-users compliance to security policies prohibiting such discussions without proper authorization or validation. BAI Security offers a non-threatening phone, in-person, and an email-based evaluation process to fully evaluate this area of risk.

Firewall / IDS / IPS Assessment: The Firewall / IDS / IPS audit option is a vital component to any comprehensive audit and is highly recommended due to the importance of these key devices. Installing such devices can provide a false sense of security if not properly implemented. The firewall and IDS/IPS system(s) will be reviewed in detail to ensure proper design, implementation, administration, and monitoring. BAI Security will provide a validation of these protection devices to ensure proper protection, as well as adherence to best-practices and/or regulatory compliance standards.



Telco / Wardialing Assessment: Utilizing common dial-up modems to gain unauthorized access to internal systems has been an early long-standing security vulnerability. Even with the number of modems connected to internal networks dropping, the threat still exists today. Modems are still connected to key network devices for out-of-band management and commonly used for remote access. This testing scans every phone assigned to your organization, determines if a modem exists, evaluates authentication mechanisms, and performs a passive penetration attempt on the device.

AntiVirus Assessment: With the increased frequency and more importantly the growing level of sophistication of viruses in the world today, security professionals recognize that viruses are now a key method for hackers to gain unauthorized access and cause denial of service to businesses. The AntiVirus evaluation will ensure that your antivirus protection is properly designed, implemented, administered, and monitored as necessary to not only protect against common viruses, but to protect against additional security threats that could create a backdoor to corporate systems and/or cause denial-of-service outages.

Wireless Assessment: As the popularity of Wireless LANs increases, so do the security risks. Information such as passwords, dial-in account numbers, WEP keys etc., can be gleaned by hackers through wireless networks in a matter of minutes. This information can be used to gain access to your LAN and computer systems to retrieve confidential company records, customer data, financial data and personal information; all of which needs to be kept secure for business, compliance, and legal reasons. BAI Security can identify current weaknesses and demonstrate best-practice methods of implementing and utilizing this key technology.

VoIP Assessment: The convergence of data, voice and video over the same infrastructure has many benefits that can no longer be ignored. Such as a single IP network to administer, and potentially a substantial cost saving in telecommunications. In turn, voice traffic then incurs the same security risks as any data network with an additional complication in that voice services are time critical. Those implementing or utilizing VoIP strategies need to take into consideration legal and regulatory considerations as well. BAI Security can help by evaluating current implementations and/or provide a security strategy for implementation for new VoIP systems.

Remote Access Assessment: The combination of dialup access, small office/home high-speed Internet service, virtual private networks, mobile computing, and business partner connections have empowered a rapidly growing population of highly mobile, decentralized workers. These technologies have also unfortunately spawned opportunities to create numerous backdoors on many enterprise networks for both inbound and outbound access. Experts in secure and compliant connectivity solutions, BAI Security can evaluate your current remote access implementations and identify weaknesses well before the malicious can take advantage of your heightened connectivity options.

Security Policy Assessment: The Security Policy evaluation and/or development is a vital audit option and provides a streamlined way to ensure your company's Information Security Policies are in sync with industry standards and/or government regulations. It is widely accepted that an organizations information security policies are the cornerstone to an effective and comprehensive security program. BAI Security will review the current IT policy documents for proper content and overlay BAI's own compliant best-practice policies to determine holes in key areas and can provide supplements to the original content as needed.,