



Criterion Systems provides full life-cycle security services for our clients in the government, financial services, energy, telecommunications and life sciences market sectors.

Criterion has relationships with leading technology solutions companies such as Microsoft, IBM, Citrix, vmWare, HP, and Access Data.

Criterion has a strong history of delivering some of the most innovative and cost effective security solutions in the marketplace today.

The pace of technology change has outstripped the IT manager's ability to keep up with the security of the enterprise. Product development often becomes a production environment without the benefit of careful review to ensure security holes are closed and affected systems are secure. Above all, customer privacy is at stake. Names, addresses, and even personal financial information are all stored on electronic media, often within reach of the Internet hacker.

### THE ASSESSMENT PROCESS

Criterion Systems consultants apply expert knowledge to the challenges of your business. The electronic marketplace is a networked marketplace, and only Criterion Systems can deliver the right combination of veteran consulting know-how with a firm grasp of the security principles to keep online commerce safe.

Criterion has developed proprietary methodologies to analyze the value proposition for security enhancements. Our experts review a customer's current state for protection of confidential information, review strategies for improved security, and make recommendations for risk mitigation. Our analysis enables decision makers to define how much additional security and how much risk is mitigated for a given investment. The process for qualifying security issues is called a Return of Security Investment Analysis (ROSI), and involves three phases:

- **Gather information** about existing security technology infrastructure, processes, and human assets through technology tools, interviews, document review, hands-on evaluation, and testing.
- **Analyze and quantify the risk** posed by the vulnerabilities identified in terms of both likelihood and impact.
- **Produce a plan** for reducing the risk to an acceptable residual through actionable recommendations.

The output of the ROSI assessment is a report and plan of action that permits the IT manager and business executive to understand the probable impact of the

vulnerabilities on their technology, processes and people as well as the likelihood that the vulnerability will be exploited by an attack. While every organization's needs are different, Criterion Systems security consultants can review the full spectrum of security controls. These include:

- **Personnel:** Staff background, capabilities, training, experience and structure.
- **Physical:** Facility and equipment protection, as well as handling of media or printed matter.
- **Network:** Firewalls, virtual private networks, intrusion detection systems, packet filters, and secure configuration of network elements.
- **System:** Configuration and management of workstation, server, and mainframe operating systems.
- **Application:** Configuration of off-the-shelf and custom developed software.
- **Database:** Management and configuration of data storage and processing.

Each of these areas requires evaluation of technology, process and people necessary to ensure that security and privacy policy is maintained. Criterion Systems security experts possess the experience and know how to evaluate a wide range of vendors and products. Where a novel solution is in use, Criterion Systems consultants have the expertise in secure product development to analyze software and environmental configurations to identify weaknesses and operational pitfalls.

### CRITERION SYSTEMS, INC.

Headquartered in Northern Virginia's technology corridor, Criterion Systems, Inc. specializes in providing strategic, business process, and information technology services to our commercial and government customers. Criterion is managed by a nationally recognized group of senior executives with extensive industry experience, delivering exceptional solutions and value to our customers.

# Cyber Teams



## IAMT

**Information Assurance & Management Team:** Implement a total information assurance program based on a centrally managed corporate model. Our teams provide practical experience in applying risk management, developing policy and procedures, implementing certification and accreditation, and developing and managing IA programs.



## SRT

**Special Response Team:** A specialized team that has the training and experience to perform special operations outside the current abilities of a client. These operations include cyber investigations, digital forensics, and incident response.



## VAT

**Vulnerability Assessment Team:** Deliver solutions based on proven, tested, and implemented methodologies to conduct network security assessments, focusing on protecting the right assets from potential threats with appropriate security measures. Our teams examine the entire enterprise infrastructure for a specific geographic area (site), to include all systems/networks/machines hosted within that site regardless of classification.



8330 Boone Boulevard, Suite 400, Vienna, VA 22182  
TEL 703-942-5800 FAX 703-942-5729  
[www.criterion-sys.com](http://www.criterion-sys.com)