

## CRITICALITY-BASED, INTEGRATED VULNERABILITY ASSESSMENT (CIVA)

Capabilities-based versus Compliance-based Reviews

### What do these typical compliance-oriented security survey checklist items mean to you?

Compliance-oriented checklist item:	...Ask yourself:
Have management and staff responsible for managing the threat and vulnerability assessment process received <b>adequate</b> training?	What does "adequate" mean?
Does a System Security Plan exist?	How effective is it?
Have security-critical facilities been identified?	What determines facility criticality?

### Capabilities-based Reviews

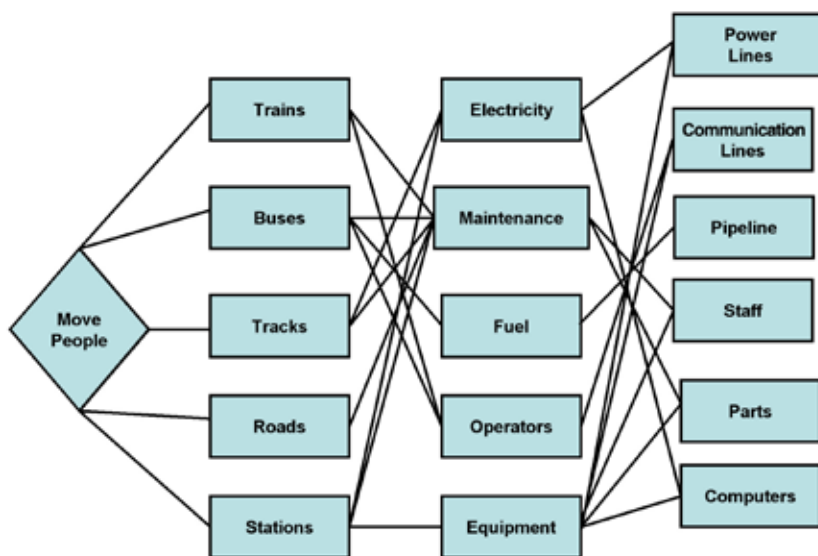
The ENSCO CIVA process focuses on the critical aspects of your operation, looking at the process or system vulnerabilities. We do this by combining the traditional pieces of a criticality assessment with a vulnerabilities assessment and using personnel knowledgeable in not only physical security and information technology practices, but also your industry. Our analysts all have more than 20 years of experience in their respective fields. They focus on the capabilities of your security system, not just the parts that comprise the system. Because ENSCO has been conducting assessments since 1985, we understand that the answer you obtain from a checklist is not the whole picture. We use a proven assessment methodology, averaging 15-20 assessments per year, on everything from critical command and control facilities, to ports and dams, to hospitals and commercial manufacturers.

### Criticality-based Reviews

Understanding the critical parts of your operation is vital to ensuring continued operations and to prioritizing protective actions. Our approach diagrams your business process to identify key components and interrelationships.

### Integrated Operations—and Vulnerabilities

ENSCO understands that vulnerabilities do not exist in isolation, and that vulnerabilities in one area can be mitigated or exacerbated by operations in another area. For example, access control systems that fail in the unlocked configuration in the event of a power outage, create an avoidable vulnerability.



**Checklist compliance is not enough.  
The overall capabilities of the security system matter!**

(continued on reverse side)



Innovation Starts Here

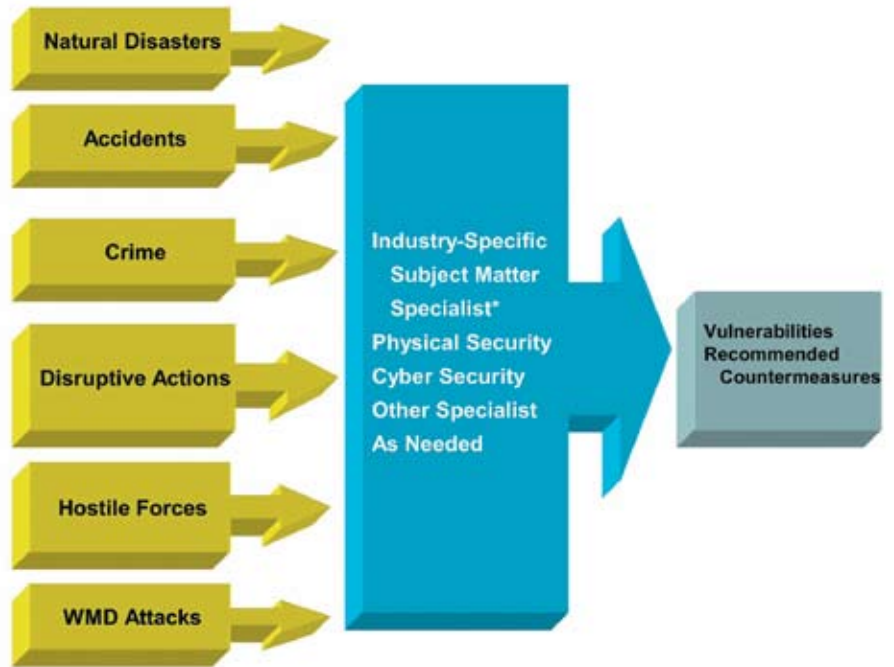
**CORPORATE HEADQUARTERS**  
3110 Fairview Park Drive, Suite 300  
Falls Church, VA 22042-4501  
703-321-9000 • 800-ENSCO-VA  
info@ensco.com • www.ensco.com

## Single Point Vulnerabilities

A single point vulnerability is defined as a single piece of equipment (or aggregation of several pieces of collocated equipment) or process, that, if destroyed or disrupted, will result in the loss of the system's mission. Examples of single point vulnerabilities include:

- Technical control facility
- ADP and LAN centers
- Control and operations centers
- Power distribution
- Power generation
- UPS/power conditioners
- Communications lines
- Air intake and exhaust
- Fuel/storage lines
- Train control systems
- Switching/internal distribution
- Cooling water pumps and manifolds
- Rail bridges and tunnels

ENSCO's methodology identifies the most critical and vulnerable parts of your operation, allowing you to focus corrective measures on the areas that will provide you with the greatest return on investment.



\*This position varies with the entity under consideration.



For more information, please contact:

Jim Byers  
Deputy Director,  
Security Services Group  
703.321.4607  
byers.james@ensco.com

Thomas Plutt  
Deputy APA Division Manager,  
Security Systems Group  
703.767.9736  
plutt.thomas@ensco.com

05.0161

EXPERIENCED, PROVEN, FLEXIBLE