
Establishing Audit Guidance for IT Security

Experience of the US GAO's e*Security Laboratory

Keith A. Rhodes, PE, CCP
Chief Technologist
Director, Center for Technology & Engineering

Opening Thoughts

- **Auditing supports government oversight**
- **Security testing supports IT governance**

IT Security Complexity

- A dedicated external adversary;
- An outsider just trying to cause trouble;
- A dedicated internal adversary;
- An insider who does not practice good security;
- The weaknesses built into the common infrastructure (for example, the global telecommunications system);
- Documented and undocumented weaknesses in software environments and products (for example, Microsoft, Oracle, or Cisco), or
- Any combination of the above.

IT Security Audit Questions

- Does the department or agency being audited have security measures in place?
- Are these measures effective?
- Can the effectiveness be proven?

GAO's e*Security Laboratory

- Started in 1997
- Purpose is to conduct comprehensive technical audits of diverse, complex, and interconnected IT environments that support critical agency functions
- Initial investment of \$250,000 (USD)

GAO's e*Security Laboratory

- The laboratory has supported the following audits:
 - The Consolidated Financial Statements of the United States, including the Internal Revenue Service, the Federal Reserve Board, the Bureau of Public Debt, and the Financial Management Service);
 - The Environmental Protection Agency, the Department of Energy, the Department of State, and the Federal Aviation Administration; and
 - In cooperation with inspectors general at the National Finance Center and the Department of the Interior.

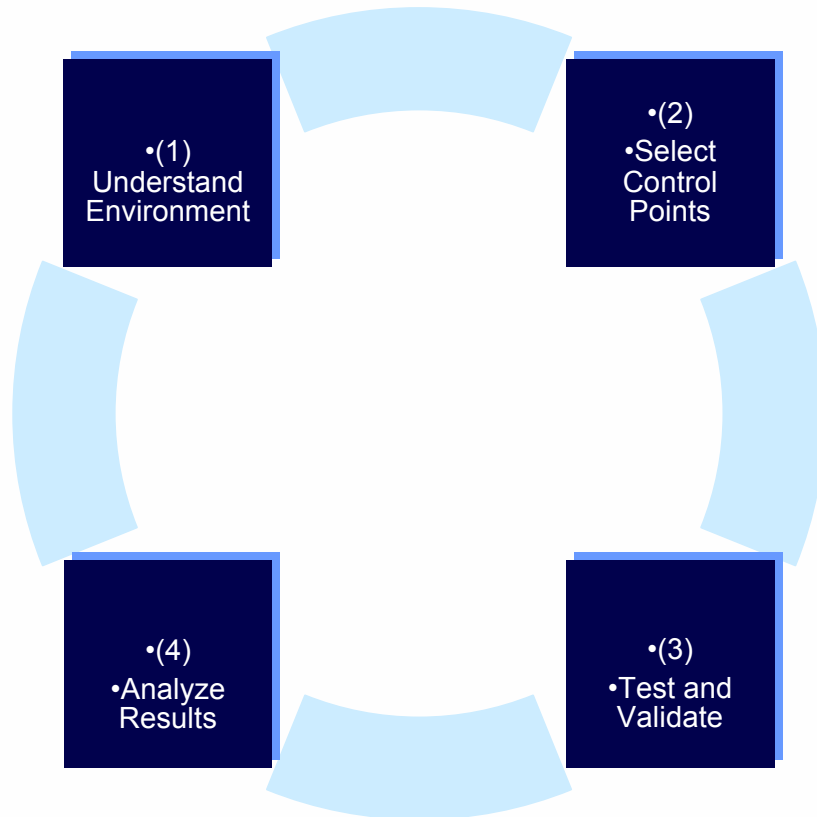
IT Security Audit Guidance

- GAO, *Federal Information System Controls Audit Manual (FISCAM)*;
- Information Systems Audit and Control Association (ISACA), CobiT®;
- U.S. Defense Information Systems Agency (DISA);
- U.S. National Security Agency (NSA);
- U.S. NIST;
- International Standards Organization (ISO) 17799; and
- vendor guidance and industry practices (for example, Oracle, Cisco, and ISS).

IT Security Audit Guidance

- Reviews Test:
 - Entity-wide Security
 - Access Controls
 - Change Control
 - Segregation of Duties
 - System Software
 - Service Continuity

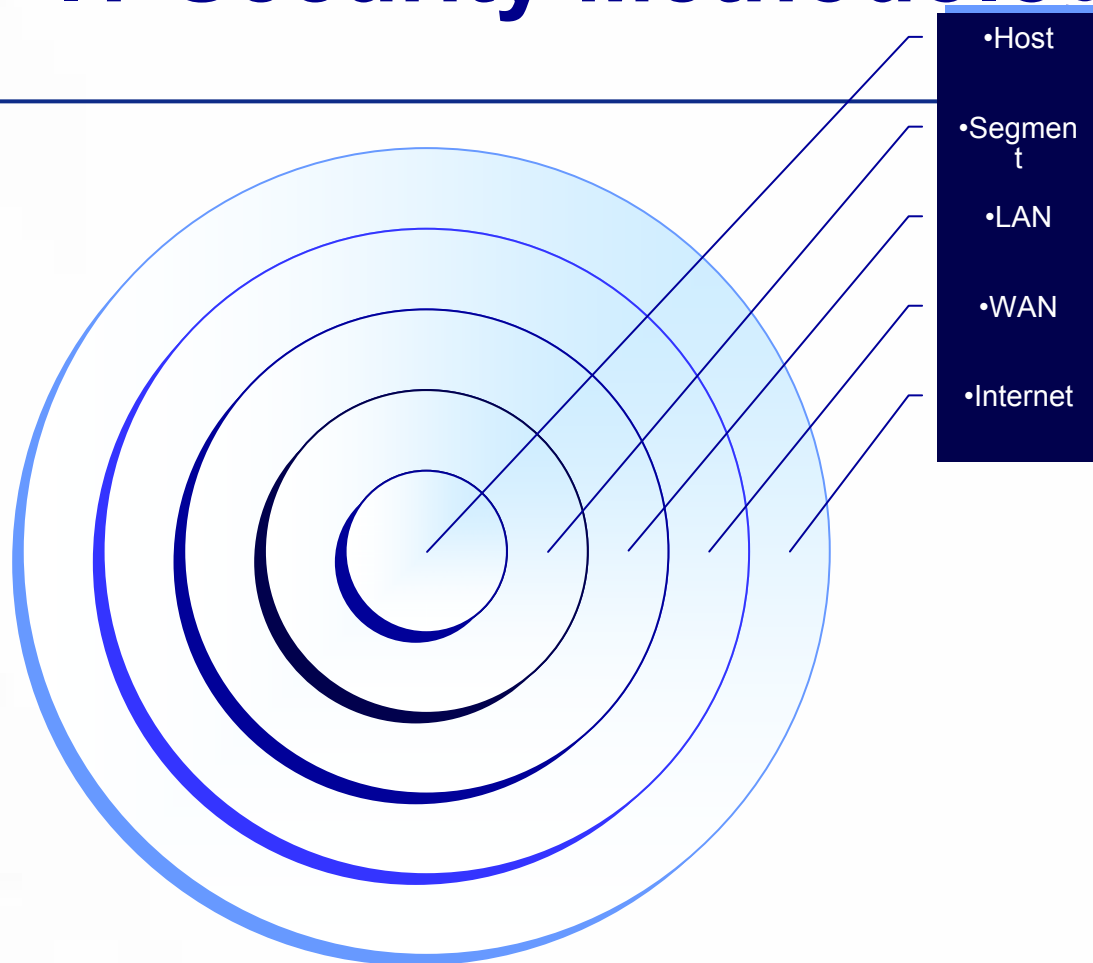
IT Security Methodology



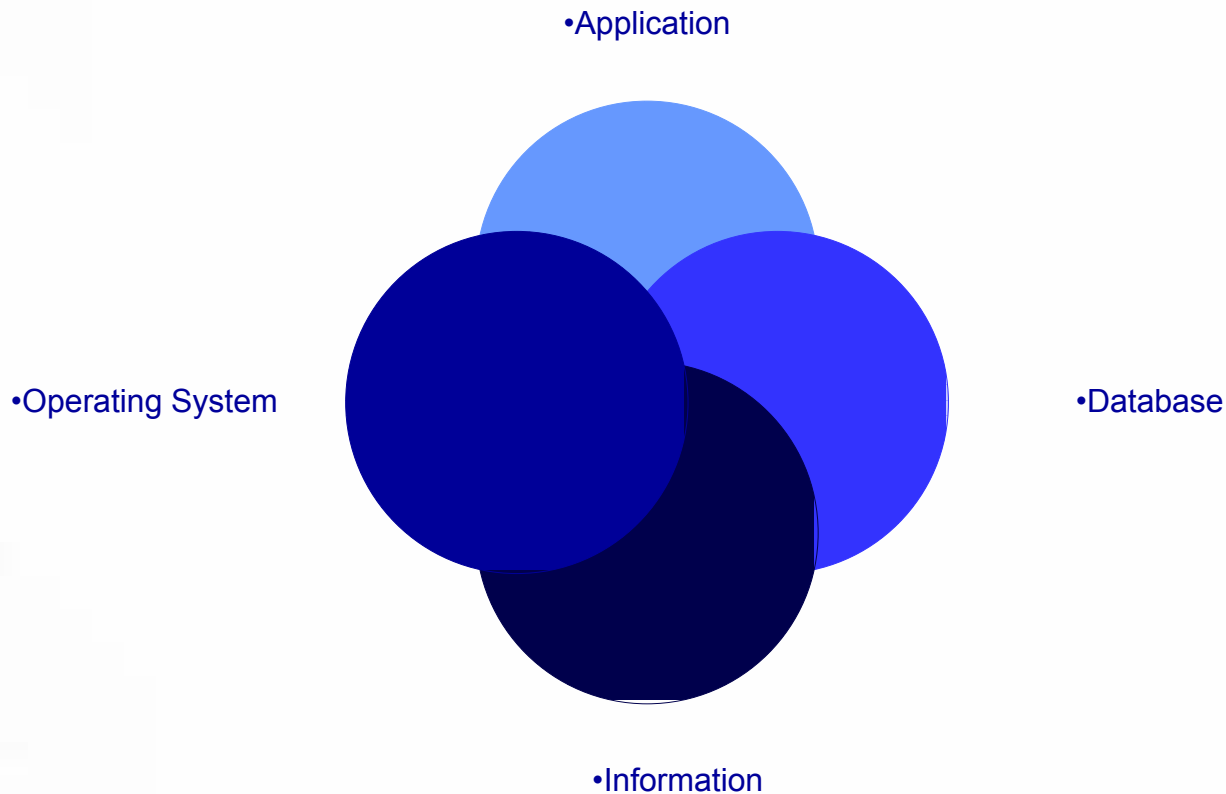
IT Security Methodology

- Reviews included:
 - Ability to Protect
 - Ability to Detect
 - Ability to React
- Reviews covered both **internal** and external threat
- Reviews included both **physical** and logical penetration testing

IT Security Methodology



IT Security Methodology



Findings

Comparison: Flash Memory vs. Paper

USB Drive

Capacity: Up to 2G or about 675,000 pages

Weight: 1 ounce

Portability: Fits on your keychain

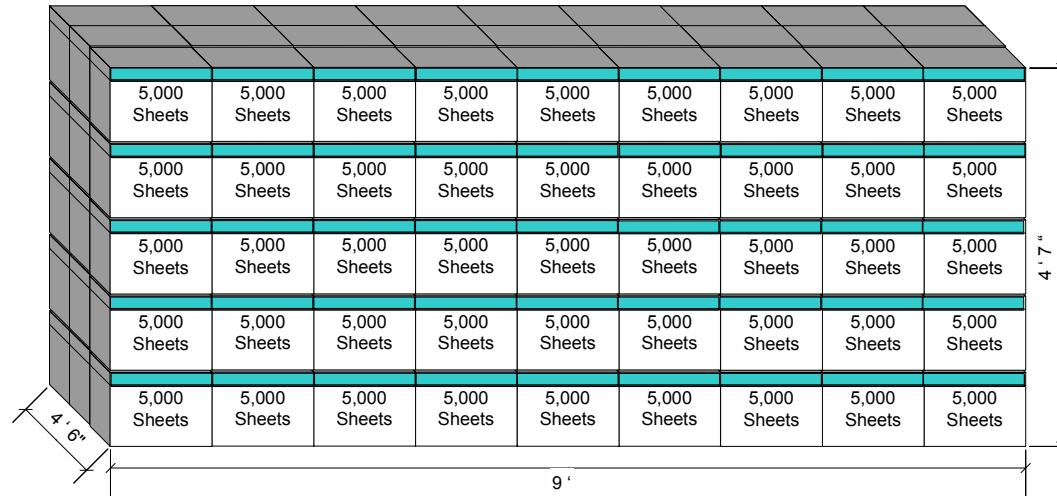


Cases of Paper

Capacity: 135 cases X 5,000 = 675,000 pages

Weight: About 3,375 lbs or 54,000 ounces

Portability: Fits in a tractor trailer



Recommendations

- What is our mission?
- What or who is our adversary?
- What is the critical information?
- How long can we meet our mission without an update to this information?
- How complicated is it to build (or rebuild) this information?

Recommendations

- Computer emergency response teams (CERTs)
 - Protect – via advisories and tools distribution
 - Detect – via network and system monitoring
 - React – via direct countermeasures and cooperation with international and domestic law enforcement

Recommendations

- Vulnerability assessments, both red and blue teaming
 - Not just technology
 - Must sweep public sources (web pages, newspapers, periodicals, phonebooks)
 - Must employ social engineering (help desk, employees, contractors, temps)
 - Must include continuity of operations via contingency planning testing

Closing Thought

- **Assumptions about security are always dangerous**

Contact

Keith A. Rhodes, PE, CCP
Chief Technologist
Director, Center for Technology & Engineering
U. S. General Accounting Office
441 G street, N. W., Washington, D. C. 20548-0001

V: (202) 512-6412
F: (202) 512-6451
E: RhodesK@gao.gov