

New International Standards:
ISO-17799
and
The Common Criteria

A presentation to ISACA
Vincent LeVeque
June 20001

Why Standards?

- Solid, objective criteria for assessing organizational practices
- More credibility than personal judgment
- Ability to benchmark practices
- Essential for public and private regulation
- Target for vendors to build new products
- Facilitate RFP by product purchasers
- Can you trust your trading partners?

Past History

- The “Orange Book” – Trusted Computer Security Evaluation Criteria
- GSSP – Generally Accepted System Security Principles
- Various regulations and guidelines for financial services industry
- CobiT
- FIPS (e.g. FIPS-140 for crypto hardware)

Two Basic Types

- Product Evaluation
 - Does this product provide the security features it promises?
 - What is the quality of the product's security? Can it be easily broken?
 - Is the product secure enough to use in my environment?
- Practice Evaluation
 - Are we following accepted good security practice?
 - Are the controls in place to maintain security?
 - Do we have enough security for our business

Product Evaluation

- Provides credible evidence that the product:
 - Has the advertised security features (“functionality”)
 - These features cannot be broken (“assurance”)
- Used by:
 - End using organizations, to evaluate purchase
 - Vendors, to provide guidance in product design and development

Products : Functional vs. Assurance Level

- Functional
- Assurance
- Tied together in TCSEC “Orange Book”
- Specified and evaluated independently in Common Criteria



The Common Criteria Process

- Protection Profiles
- Evaluation Assurance Levels
- Security Targets
- Target of Evaluation



Common Criteria Functional Levels

- Flexible
- Developed by governments, industry associations
- Expressed as Protection Profiles
 - A common consumer need for security requirements
 - A set of requirements, independent of any specific product
- Must themselves undergo evaluation



Some Current Protection Profiles

- Packet Filter firewall
- Application proxy firewall
- Transaction-processing system
- Commercial “Discretionary Access Control”
- And of course, all the old “Orange Book” categories have their corresponding CC PP.



Common Criteria Assurance Levels

- How well does the product meet the Protection Profile?
- Expressed as an Evaluation Assurance Level (EAL)



Common Criteria Assurance Levels

- EAL1 – Functionally Tested
- EAL 2 – Structurally Tested
- EAL 3 – Methodically Tested and Checked
- EAL 4 – Methodically Designed, Tested, and reviewed
- EAL 5 – Semiformally Designed and Tested
- EAL 6 – Semiformally Verified Design and Tested
- EAL 7 – Formally Verified Designed and Tested



Who Does CC Evaluation?

- Commercial Labs in various participating countries
- In the USA:
 - Arca Systems
 - Booz Allen Hamilton
 - CSC
 - Netigy
 - SAIC
 - Etc.

Now for Practice Evaluation

- How does the organization manage and use security? How is data protected?
- Focus is on policies, procedures, and standards
- Some examples:
 - GSSP
 - Surveys and benchmarks
 - Regulatory Requirements
 - British Standard 7799

BS7799/ISO-17799

- Overview
 - One of several internationally recognized standard practices for ensuring quality by different organizations in different geographical areas.
 - Analogous to ISO 9000 for general organizational controls.
 - Provides guidelines to assure integrity, availability, and confidentiality of information assets, through management controls.

BS7799/ISO-17799

- Focus areas (10 key controls):
 - A documented information security policy
 - Allocation of information security responsibilities within the organization
 - Information security education and training
 - Security incident reporting and response
 - Virus detection and prevention controls
 - Business continuity planning
 - Control of proprietary software copying
 - Critical record management processes
 - Protection of personal data (privacy)
 - Periodic compliance reviews

BS7799/ISO-17799

- Certification process
- Like ISO 9000?
- Stages
 - BS7799-1 Code of Practice
 - BS7799-2 Specification of Information Security Management Systems
 - ISO standard
- Master “checklist” of security items
- Requires prior risk analysis to determine checklist item applicability to YOUR organization

Standards and the Audit Process

- Product standards generally less useful, unless mandated
 - Some product standards “stick”, others fall into disuse
 - Note vendor “abuse” of Orange Book C2 rating
- ISO-17799/BS-7799 should prove more useful
 - Internationally recognized “catalog” of controls
 - Can be tailored, based on organization’s specific needs
 - Literature suggests use similar to SAS70 as third party assurance

More Information

- Common Criteria
 - <http://www.commoncriteria.org>
 - <http://www.radium.ncsc.mil/tpep/library/ccitse>
- ISO-17799/BS7799
 - <http://all.net/books/standards/bs7799.html>
- Comparison of the two:
 - <http://www.sans.org/infosecFAQ/standards/iso17799.htm>