Global Information Assurance Certification Paper

Common Criteria or ISO17799

By Lucille Santillo

It has always fascinated me that we, as a free society, have so many choices to review before we can make a purchase. Looking at the many different types of personal computers and networking equipment that are available, I wonder if they can measure up to the same security standards?

As I began research, I questioned whether I had the right information to make a good decision. I needed something to get past the smoke and mirrors of the "Account Executives" and glossy brochures. Reviews from the different trade papers and magazines help but one really wants something more official.

This is where a good, respected Security Standard is needed. I discovered that there are two very good security standards--Common Criteria (International Standard 15408) and the British ISO17799.

In this paper, I will try to give a brief description of each in an effort to understand what they are. I have compiled this into a chart to determine their similarities and differences.

While searching, I found that information on Common Criteria was free, readily available and easy for me to understand.

In contrast, a company called C & A Systems Security LTD seemed to be the only source of information on ISO17799. They have an informative website giving a general description of ISO17799.

(Please check the glossary for descriptions of some of the terms in this table.)

	Common Criteria	**ISO17799**
What is it?	Common Criteria (CC) • Identifies and evaluates security features of both computer products and systems. • Is a joint effort of NIST, NSA and security organizations in Canada, France, Germany, the Netherlands, and the United Kingdom. In 1999, it became known as International Standard 15408 and the latest version is CC version 2.1. CC caused the need for a group called National Information Assurance Partnership (NIAP) to combine the activities of	It began in the United Kingdom as BS 7799 in 1995, as a comprehensive set of controls comprising best practices in information security. It was significantly revised and improved in May 1999 becoming known as ISO 17799.

	NIST and NSA This group is chartered to establish cost-effective evaluation of security-capable IT products.	
What is its purpose?	CC: *For consumers* • Provides a level of confidence that the products they are evaluating were measured equally. • Helps them determine whether the product meets their security requirements or, at least, will allow them to know what their risks are. *For Developers* • Provides a standardized set of product security requirements to follow in designing and building a product. • Helps to determine the type of support they will give their product. *For Evaluators:* • Standards to test products against. • Helps to determine which evaluations can be performed and input in forming specific evaluation methods.	ISO17799 is to be used as a comprehensive standard range of controls needed for most situations involving Products and Systems.

What are the parts of this standard?	*Part 1 Introduction and General Model* ***Defines:*** • General concepts for security evaluations • Requirements through constructs (called PPs, STs and packages) that help identify objectives for specifications of products and systems.	• **Business Continuity Planning** Deals with interruptions to business activities and to critical business processes from the effect of major failures or disasters.

	Part 2-Security Functional Requirements This part tackles the responsibilities of explaining the security requirements using a catalog. The catalog includes the following: • Classes are groups consisting of families of requirements, all relating to a common security focus. (e.g., identification and authentication). • Families are groups of components, all relating to specific security objectives but having some differences (e.g., user authentication). • Components are selectable requirements that may be included in PPs, STs, or packages (e.g., unforgettable user authentication). *Part 3 Security Assurance Requirements* Also organized in a catalog format, this part contains a set of assurance components to use in standardizing the expressing of the assurance requirements for products and systems. An evaluation criterion is defined for PPs and STs.	A product by C & A Systems LTD called Cobra, could be a real aid in helping with BCP. They offer a 15 day trial copy which is well worth checking out. • **System Access Control** Covers various kinds of access control and their detection to aid in protecting information, networked and mobile services. • **System Development and Maintenance** Includes objectives to ensure security is built into operational systems and IT projects. Development of maintenance procedures for application systems that have Security in mind. Protect the confidentiality, authenticity and integrity of information. • **Physical and Environmental Security** This section deals with access and compromise but with the physical business premises in mind. • **Compliance** Covers avoiding violations of the law and the organizational security policies and standards.

	But here is the best part that shows real cooperation between the organizations—seven Evaluation Assurance Levels (EALs), which are predefined packages of assurance components that make up the CC scale for rating confidence in the security of IT products and systems are defined. If the product was previously evaluated under the concepts defined by the TCSEC or ITSEC or CTCPEC, all is not lost because the EALs were developed with the goal of preserving the concepts of assurance drawn from their source criteria. This is good news for the consumer and manufacturer alike. Some products you purchased or built won't automatically fail to meet the new security standards.	Covers maximizing the effectiveness of system audits and minimizes any interference with it. • **Personnel Security** Discusses the need for Security Awareness for all users to minimize the risks of human error, theft, fraud or misuse of facilities. • **Security Organization** Guides one with Security responsibilities within the company, at processing facilities and when the information processing has been outsourced to another organization. • **Computer & Network Management** Objectives are to plan a facility with: 1) Correct and secure operation of the facilities; 2) Minimize the risk of system failures; 3) Protect the integrity and availability of software and information; 4) Preventing damage and loss to assets and interruptions to business activities including information exchanged between organizations. • **Asset Classification and Control** Deals with maintaining appropriate protection of corporate and

		information assets. • **Security Policy** Covers providing management direction and support for information security.

Glossary of terms:

Name	Abbreviation	Standard**	Definition
Evaluation Assurance Level	EAL	CC	One of seven rigorous packages of assurance requirements from CC Part 3. A level of confidence in the security functions of an IT product or system.
The National Institute of Standards and Technology	NIST	CC	Is an agency of the U.S. Department of Commerce's Technology Administration. NIST strengthens the U.S. economy and improves the quality of life by working with industry to develop and apply technology, measurements, and standards.
National Security Agency	NSA	CC	It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information.
Package	None	CC	A reusable set of either functional or assurance components combined together to satisfy a set of identified security objectives.
Protection Profile	PP	CC	Is an implementation-independent statement of security needs for a set of IT security products. Contains a set of security requirements
Security Target	ST	CC	Statement of security claims for a particular IT security product or system. Like the PP but includes product-specific detailed information.

**The description of the parts of the ISO17799, although clear, does not really touch on any of the terms one might need to be familiar with.

Sources of information:

http://www-08.nist.gov/cc/info/cc_bulletin.htm by Eugene F. Troy, NIST-ITL 11/24/98
http://csrc.nist.gov/cc/ccv20/ccv2list.htm Common Criteria Version 2.1/ISO IS 15408 last updated: 9/19/2000
http://www.abanet.org/scitech/ec/isc/stonebumer Using Common Criteria Protection Profiles by Gary Stonebumer, Computer Security Division, NIST 4/9/99
http://www.radium.ncsc.mil/tpep/library Common Criteria last updated: 6/9/99

http://www.securityauditor.net/ ISO17799 Compliance & Positioning. Sponsored by C&A Systems Security Ltd-Risk Analysis & ISO 17799 Specialists.
www.iso17799software.com C & A Systems Security LTD