** Information Security **
ISO 15408 Common Criteria Certification Explained

Introduction

The Common Criteria (CC) program is an international alliance that has established procedures for evaluating the security of information technology (IT) products and systems. This program, called the CC Project, was started in June 1993 with the sponsoring organizations - the United States, Canada, France, Germany and United Kingdom - combining separate criteria into a single set of IT security criteria. After a number of trial evaluations and extensive public review, CC Version 2.1 was produced in August, 1999. This set of Common Criteria is referred to as International Standard 15408, or ISO 15408. A product or system that has successfully completed testing and validation can receive **ISO 15408 Common Criteria Certification**.

The extent to which the IT product or system has been assessed for compliance with ISO 15408 Common Criteria is measured using Evaluation Assurance Levels (EALs). There are seven predefined assurance packages, on a rising scale from EAL1 to EAL7. EAL1 to EAL4 certification applies to security technologies designed for Commercial Off-The-Shelf (COTS-platform) office equipment, such as facsimile, printers and digital copier/multifunctional products. For example, Ricoh's DataOverwriteSecurity System Type A & B kit has received EAL3 certification. This assures consumers that the targeted security functionality – three-pass overwrite of hard drive data - is appropriate to meet a given threat and that it has been correctly implemented.

With that said, let's review frequently asked questions about Common Criteria.

Q. ***Who administers the Common Criteria program?***

A. The Common Criteria program is administered by the National Information Assurance Partnership (NIAP), a government initiative that meets the security testing needs of IT decision makers and manufacturers. A collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), NIAP leverages both agency's extensive experience to research and develop IT security requirements, including evaluation test methods, tools, techniques and assurance metrics.

Q. ***What is the primary goal of NIAP?***

A. NIAP's primary goal is to help increase the level of trust IT decision makers have in their information systems and networks through the use of cost-effective security testing, evaluation and validation programs. In doing so, NIAP promotes the development of technically sound security requirements for U.S. and international IT products and systems.

Q. ***Who conducts the testing and validation for ISO 15408 Common Criteria?***

A. Security testing and validation is conducted by a Common Criteria Testing Laboratory (CCTL), an independent, experienced private-sector laboratory accredited by NIAP. NIAP employs the National Voluntary Laboratory Program (NVLAP) at NIST to ensure that security testing laboratories meet the highest standards for technical competence and integrity. For a list the NAIP-approved Common Criteria Laboratories, visit:

www.niap.nist.gov/cc-scheme/testing_labs.html.

Q. ***What role does NIAP's Common Criteria Evaluation and Validation Scheme play?***

A. The CCEVS, also called Validation Body, is the program developed by NIST and NSA as part of the National Information Assurance Partnership (NIAP). CCEVS establishes an organizational and technical framework to evaluate the trustworthiness of IT products and Protection Profiles (PP[1]) for conformance to ISO 15408 Common Criteria. This Validation Body is also responsible for approving private sector security testing laboratories.

[1] A Protection Profile (PP) is an implementation independent statement of security requirements that is shown to address threats that exist in a specified environment, for example, a hospital may wish to purchase an IT system to address its security requirements relative to patient records.

Q. *Has the international community embraced Common Criteria?*

A. Yes. The international community has embraced Common Criteria through the Common Criteria Recognition Arrangement (CCRA) whereby the signers have agreed to accept the results of CC evaluations performed by other CCRA members.

Q. *Which countries are Common Criteria Recognition Arrangement (CCRA) members?*

A. The governmental organizations listed below constitute the CC Project Sponsoring Organizations. These organizations worked closely on the CC Project to produce a Mutual Recognition Arrangement for IT security evaluations.

Country	CCRA Scheme Title
Australia	Australian Information Security Evaluation Program (AISEP) Defence Signals Directorate
Canada	Communications Security Establishment
Germany	Bundesamt für Sicherheit in der Informationstechnik
France	Service Central de la Sécurité des Systèmes d' Information
Japan	Japan Information Technology Security Evaluation and Certification Scheme (JISEC)
New Zealand	Government Communications Security Bureau
United Kingdom	Communications-Electronics Security Group and Department of Trade and Industry
United States of America	National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS)

Note: To see the list of participants in the Recognition Agreement, and links to respective sites, visit: **www.niap.nist.gov/cc-scheme/mutual-rec.html**.

Q. *Which nations accept certifications from Common Criteria Recognition Arrangement (CCRA) members?*

A. Countries that do not have a national scheme for conducting evaluations, but have agreed to accept certifications produced by the nations listed above, are as follows:

Austria	Federal Ministry of Public Service and Sports
Finland	Ministry of Finance
Greece	Ministry of Public Order / National Information Service
Israel	Ministry of Industry and Trade
USCi from Italy	Presidenza del Consiglio dei Ministri Autorità Nazionale per la Sicurezza CESIS III Reparto
The Netherlands	Ministry of the Interior and Kingdom Relations
Norway	HQ Defence Command Norway/Security Division
Spain	Ministerio de Administraciones Públicas
Sweden	SWEDAC (Swedish Board for Accreditation and Conformity Assessment)
Hungary	Ministry of IT and Telecommunication
Turkey	Turkish Standards Institute

Q. *Which Ricoh products are ISO 15408 Common Criteria certified?*

A. As the list of Common Criteria-compliant Ricoh products and systems is continually updated, we suggest you contact your authorized Ricoh sales representative or visit www.ricoh-usa.com for more information. Simply click the *Solutions* link, then *Security Solutions*.

Q. *How do organizations use ISO 15408 Common Criteria Certification?*

A. ISO 15408 Common Criteria Certification is used as third-party validation that the security features of a given product or system will operate as advertised, thus is a valuable "proof source" for any organization concerned with building a secure infrastructure. Another key benefit to ISO 15408 Common Criteria is that the certified solution can often assist public and private enterprises in compliance with the following:

- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Defense Security Service (DSS)
- Defense Information Systems Agency (DISA)

Web Resources:

National Information Assurance Partnership (NIAP)	www.itl.nist.gov
National Institute of Standards and Technology (NIST)	www.nist.gov
National Security Agency (NSA)	www.nsa.gov
Ricoh Corporation	www.ricoh-usa.com