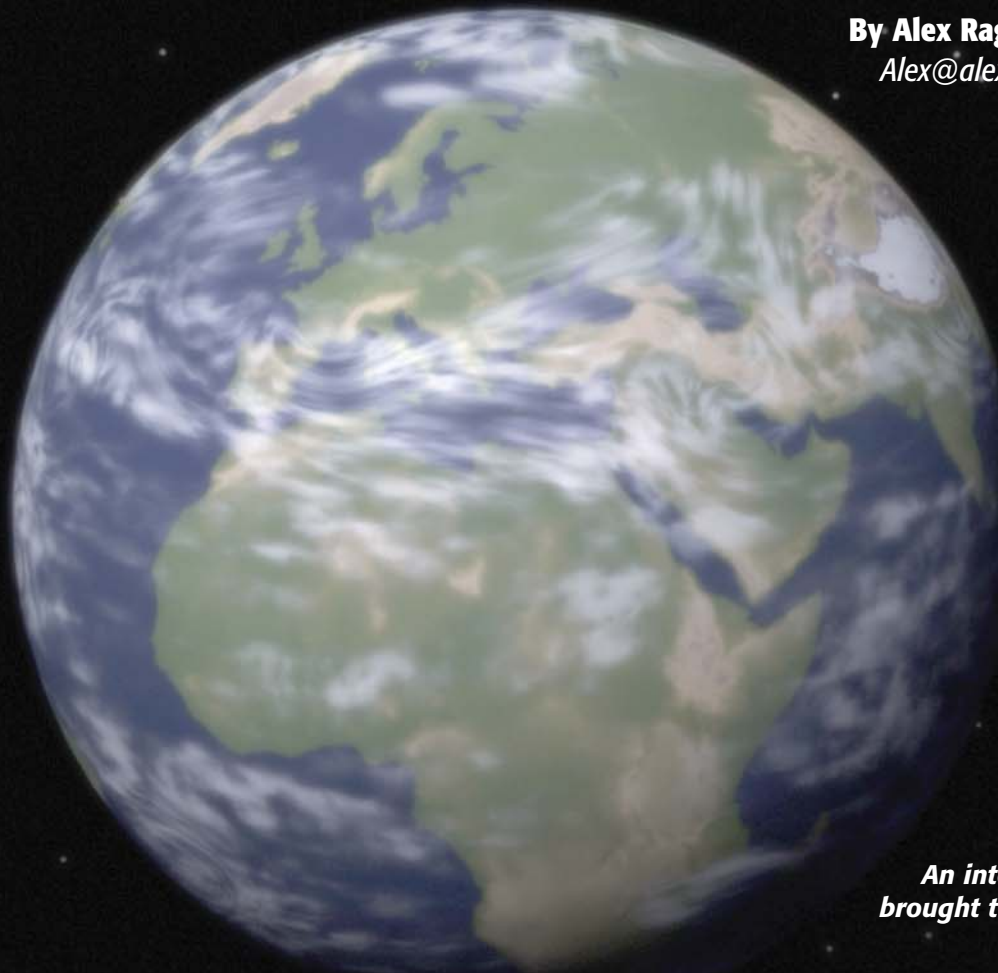


A Brief Guide to the Common Criteria

By Alex Ragen, CISSP
Alex@alexragen.com



*An international article
brought to you from Israel*

On July 1, 2002, the US Department of Defense began to enforce National Security Telecommunications and Information Systems Security Policy (NSTISSP) # 11 (issued in January 2000), which mandates that US government agencies purchase only those IT security products which have been validated in accordance with Common Criteria and/or FIPS 140-1 or FIPS 140-2 as appropriate.

We won't deal with FIPS 140-1 and FIPS 140-2 here except to note that they are Federal Information Processing encryption standards (see <http://csrc.nist.gov/publications/fips/index.html> for more information.). It's the Common Criteria that is the subject of this article.

NSTISSP # 11 made official what had been a recommendation honored more "in the breach than in the observance." IT security vendors who were blindsided by new policy (and to be frank, they should not have been) suddenly found themselves in panic mode, trying to figure out how to get their products certified before their US government sales evaporated.

As a result of NSTISSP # 11, there has been a marked increase in the number of IT security vendors seeking and obtaining Common Criteria certification. But even those who have successfully certified products find the standard and its processes to be esoteric and often confusing.

Should You Be Interested in Common Criteria?

Users/Customers—All other things being equal (and they rarely are), customers should prefer a Common Criteria-certified product to an equivalent one without certification. Not because the Common Criteria-certified product has more or better features, but because the Common Criteria evaluation looks at areas into which the customer has no visibility, the dark corners of the software development process, and provides a high level of confidence that things like configuration management, testing, manufacturing, secure delivery, and even product design are done properly.

Vendors—For vendors, Common Criteria usually isn't a matter of choice. Your (potential) customers either insist on Common Criteria certification (for example, US government agencies because of NSTISSP # 11) or they don't (for now).

In any case, it doesn't hurt to learn something about Common Criteria before it is imposed on you, so I invite you to read on.

What is Common Criteria?

Common Criteria is an outgrowth of earlier government-devised standards, such as ITSEC (UK) and the Rainbow Series (US), and provides a mechanism for evaluating and certifying IT security products, as opposed to sites.

Herein lie both the strength and the weakness of Common Criteria. The strength—it's an exhaustive evaluation of a product's capabilities and the environment in which it is developed. A customer can buy a Common Criteria-certified product confident that the product can provide the advertised services in a secure way. The weakness—only the product is certified, not the environment in which it is used. Common Criteria will not protect the customer from using the product in a way that actually reduces site security.

So Common Criteria alone is not enough to guarantee security for a site and its data—what else is new? But Common Criteria does give security personnel the confidence that a product can, *if properly configured and managed*, enhance a site's security.

What Common Criteria Does Not Include

Common Criteria is not quite all-encompassing: it doesn't include encryption. The only reference to encryption in the Common Criteria is to call out FIPS 140-1 and FIPS 140-2.

| Country | Administered by | URLs |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certificate-Issuing Countries | | |
| Australia | Australasian Information Security Evaluation Program (AISEP) Defence Signals Directorate | http://www.dsd.gov.au/infosec |
| Canada | The Communications Security Establishment (CSE) operates the Canadian Common Evaluation and Certification Scheme. | http://www.cse-cst.gc.ca/en/services/common_criteria/common_criteria.html |
| France | Service Central de la Sécurité des Systèmes d'Information | |
| Germany | Bundesamt für Sicherheit in der Informationstechnik | http://www.bsi.de/Common Criteria |
| Japan | Japan Information Technology Security Evaluation and Certification Scheme (JISEC) | |
| New Zealand | Government Communications Security Bureau (New Zealand) | |
| United Kingdom | The Communications-Electronics Security Group (CESG) and the Department of Trade and Industry (DTI) operate the UK IT Security Evaluation and Certification Scheme. | http://www.cesg.gov.uk/ |
| United States | The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) operate the Common Criteria Evaluation and Validation Scheme (Common Criteria EVS) under the National Information Assurance Partnership (NIAP). | NIAP – http://www.commoncriteriaportal.org/ NIST – http://csrc.nist.gov/Common Criteria/ NSA – http://www.nsa.gov CCEVS – http://niap.nist.gov/Common Criteria-scheme |
| Certificate-Consuming Countries (have a national scheme for conducting evaluations but have agreed to accept the certificates produced by the nations listed above) | | |
| Austria | Federal Ministry of Public Service and Sports | http://www.cio.gv.at |
| Czech Republic | National Security authority of the Czech Republic | |
| Finland | Ministry of Finance | |
| Greece | Ministry of Interior | http://www.ipa.go.jp/security/jisec/jisec_e/ |
| Hungary | Ministry of IT and Telecommunication | http://www.ihm.hu/English/ |
| Israel | Standards Institution of Israel | http://www.sii.org.il/ |
| Italy | Autorità Nazionale per la Sicurezza | |
| Netherlands | Netherlands National Communications Security Agency (NLNCSA) | http://www.commoncriteria.nl/ |
| Norway | CHOD Norway/Security Division HQ Defence Command Norway/Security Division | http://www.sertit.no |
| Singapore | Infocomm Development Authority of Singapore (IDA) | |
| Spain | Ministerio de Administraciones Publicas | |
| Sweden | Swedish Board for Accreditation and Conformity Assessment (SWEDAC) | http://www.swedac.se/ |
| Turkey | Turkish Standards Institution | http://www.tse.org.tr/ |

Figure 1: Countries participating in the Common Criteria Recognition Arrangement

Who Uses Common Criteria?

As mentioned earlier, US government agencies now require Common Criteria certification, as do many government agencies in the twenty

other countries that make up the Common Criteria Recognition Arrangement (see Figure 1).

In addition to the CCRA members, some other countries informally require Common Criteria for their government agencies.

In the non-government sector, Common Criteria is rarely required. One exception is the Financial Services Roundtable in the US, which has developed the Common Criteria-based BITS product Certification Program (see http://www.bitsinfo.org/c_certification.html) to ensure that products meet minimum-security criteria established by the financial services industry.

Common Criteria has a built-in mechanism that enables customer groups (such as BITS) to define their own requirements by packaging the pre-defined Common Criteria requirements (and, optionally, customer-defined requirements) in the form of Protection Profiles or Security Packages. The advantage: a level customer-defined playing field that simplifies comparison of competing products. The hope is that Common Criteria will accommodate a rapidly changing security landscape, as both government and non-government groups continue to develop industry-specific Protection Profiles and/or Security Packages.

The reality, alas, somewhat belies the hope. While NSA and other government agencies have defined a number of Protection Profiles for firewalls, Trusted Platform Modules, biometrics, etc., and are working on more, the private sector has developed comparatively few. The BITS Security Packages have been around for several years, but so far there are only two certified products. This low level of non-government participation must surely be a disappointment to the powers behind Common Criteria.

Still, don't count Common Criteria out just yet. It's hardly the last word in security standards, but its heavyweight sponsors will ensure that it will be around for a long time.

The Common Criteria Process

A Common Criteria evaluation can be a daunting and expensive experience. The better you understand the Common Criteria from the start, before you sign contracts with an army of consultants, the easier it will all be, and the less you will feel overwhelmed and helpless in the face of the smokescreen of jargon the consultants throw about whenever you ask them to explain why it's taking so long and costing so much money.

Terminology

Common Criteria has a language of its own, and there are some basic terms you should understand.

- ▲ **Target of Evaluation (TOE)** is the [sub]set of the product's features being evaluated. It's not necessary to evaluate the entire product with all its features; a coherent subset is acceptable as long as the product can be configured to implement the subset.
- ▲ **Security Functional Requirements (SFRs)** define security features of the product, for example, that administrators can be denied access to the product after a specified number of failed authentication attempts. SFRs answer the question: "What does the vendor claim that the product does?"
- ▲ **Security Assurance Requirements (SARs)** define assurance features, that is, features that contribute to the customer's confidence that the product installed and running at the customer site is in fact the same version of the product that was evaluated.

Example: the vendor's use of a Configuration Management system to monitor changes to the product during its life cycle. SARs answer the question: "How can I be sure that the product I have installed actually does what the vendor claims it does?"

- ▲ **Evaluation Assurance Level (EAL)** is the level of confidence achieved by the TOE, and is a function of the SARs with which the TOE complies. EALs range from EAL1 to EAL7, with EAL2–EAL4 being the most common.

EALs refer to the level of confidence in the conclusions of the evaluation, and not to the level of security the product provides. In other words, you can have more confidence that an EAL4 product performs as advertised than an EAL2 product, because an EAL4 evaluation examines more aspects of product development (including testing) at a greater level of detail than does the EAL2 evaluation. But an EAL4 product will not necessarily provide more security. This point is commonly misunderstood.

- ▲ **Security Target (ST)** is the central document of the evaluation process.
- ▲ **Protection Profile (PP)** is a document similar to the Security Target, but one that is written by a group of users and defines an imaginary product and an EAL. Not all evaluations involve Protection Profiles.
- ▲ **National Scheme** is the government agency in each country which supervises Common Criteria evaluations and issues certificates.

The Process

The process can be divided into these stages:

1. Preliminaries, such as whether to do the evaluation at all, and if yes, which product (and which of its features) to evaluate, and which EAL to aim for
2. Formal and legal (choosing a consultant and/or a laboratory, deciding in which country to perform the evaluation, signing contracts, etc.)
3. Preparing the first version of the Security Target
4. Holding the start-up meeting, after which the product is listed as "In Evaluation" and US government agencies are allowed to buy the product
5. Preparing and submitting the evidence (documentation and test results)
6. The laboratory's determination that the evaluation is successful, and submission of its report to the National Scheme
7. Certification of the product by the National Scheme

The immediate goal is holding the start-up meeting and getting the product listed in "In Evaluation." Once that is achieved, you can proceed at a more leisurely pace, but you do have to show enough progress from month to month so that the National Scheme does not despair of your ever finishing. If they do, the product's In Evaluation status will be revoked.

Security Target

The Security Target is produced by the vendor, and defines the TOE, the threats it counters, its security objectives, the environment in which it is used, the SFRs and SARs with which it complies, and the EAL. The Security Target is structured as follows:

1. Product Description—name, version, build number, etc.

2. Security Environment, the environment (for better or for worse) in which the TOE will be used:
 - ▼ Threats—the dangers to which the assets are vulnerable
 - ▼ Organizational Security Policies—policies with which the TOE must comply
 - ▼ Assumptions—what can be reasonably assumed to be true of the operating environment (alternatively, what the TOE customer can reasonably demand of the operating environment)
3. Security Objectives, what the TOE customer wants to achieve:
 - ▼ TOE objectives—what the TOE is supposed to achieve
 - ▼ IT Environment—what the other IT products (such as the OS) are supposed to achieve
 - ▼ Non-IT Environment—what the other environmental elements (for example, administrative and training procedures) are supposed to achieve
4. Security Functional Requirements—the SFRs with which the TOE claims to comply
5. Security Assurance Requirements—the SARs with which the TOE claims to comply
6. Security Functions (optional, but usually present)—security functions performed by the product that can be directly mapped to SFRs and to Quality Assurance tests

These are the major issues addressed by the Security Target. The Security Target often addresses additional issues as appropriate, for example, the strength of TOE's encryption or authentication functions.

Claiming "Foreign" SFRs

The Security Functional Requirements (SFRs) defined in Part 2 of the Common Criteria are not intended to be exhaustive. A Protection Profile, Security Target or Security Package can define additional SFRs. In fact, the Common Criteria explicitly accounts for this possibility, and defines the tasks the evaluation laboratory must perform when evaluating "foreign" SFRs.

The majority of the claimed SFRs must be standard Common Criteria SFRs. If the vendor wants to claim some functionality not covered by any of the standard SFRs, then custom SFRs can be defined, as long as they are expressed in the standard Common Criteria format.

But of course the question is "Why take on the burden of proving compliance with SFRs that no one seems to have thought of?" One possible reason: the vendor's competitors did so in order to differentiate their own products, and the vendor feels the need to keep up.

Security Target Vs. Protection Profile

A Protection Profile is very similar to a Security Target, and the relationship between a Security Target and Protection Profile can take many forms: a Security Target can claim compliance with any number (including zero) of Protection Profiles, and can specify additional SFRs or SARs, beyond those included in the Protection Profiles with which it claims compliance (if any). Note that it is not possible to claim partial compliance with a Protection Profile.

One issue that people new to Common Criteria sometimes find disturbing is that it's possible to perform an evaluation without a Protection Profile. Why should a vendor be able to write a Security Target himself? What's the point of a standard if nothing is mandatory, if anything goes?

The point is that not anything goes. A Security Target's SFRs and the SARs must be selected from the pre-defined lists in the Common Criteria (except for a small number of foreign SFRs). A vendor can't have a Security Target consisting solely of SFRs like: "The TOE comes in a blue box" and SARs that describe how the vendor ensures that the box is always blue. Common Criteria is flexible but not ridiculous. The Security Target must have some real substance to it.

How Long Will It Take?

If you work quickly and all goes well, you can have the start-up meeting within a few months of signing the contract with the laboratory. After that, think in terms of 6-9 months more for EAL2 and 3-6 months more for each additional level, IF all goes well (did you notice how big that "IF" was?).

In this kind of time frame, it's quite likely that there will be a new version of the product in the market by the time you are done. Because Common Criteria does not have an upgrade process (though they are working on one), you then have a problem: the version you are selling is not the certified version. The "solution" is as follows:

- ▲ During the course of the evaluation, update the version number in the Security Target to the latest version. You can do this as long as the functionality of the evaluated feature set has not significantly changed and the laboratory has not yet begun its penetration testing.
- ▲ Supply the certified version to customers who insist on certification and hope that everybody turns a blind eye when the customer upgrades to the newest version.
- ▲ Go through the certification process for newer version fairly frequently, for example, every other year.

Common Criteria's lack of a fast, simple and economical upgrade process is a real shortcoming, but hopefully it will be resolved sometime in the next year or two.

What's Bad (or Not Yet Good) About Common Criteria?

As you may have concluded by this point, Common Criteria is less than perfect. Some of its shortcomings are:

- ▲ The non-government sector has been slow to adopt Common Criteria.
- ▲ There is at this time no mechanism for upgrading.
- ▲ The specialized tech-heavy jargon and arcane requirements are confusing to ordinary human beings and ensure that Common Criteria documentation is unreadable by non-experts, for example, by customers (who should be able to make sense of a Security Target but often cannot). Sometimes it seems that a lot of documentation effort is expended on making the documentation even more obtuse.
- ▲ The evaluation process, dependent as it is on government employees, is unnecessarily drawn-out, slow, painfully tedious, and very expensive.


More Information

The Common Criteria (available for downloading from the Common Criteria portal at <http://www.commoncriteriaportal.org/>) is divided into three parts:

- ▲ Part One—an overview
- ▲ Part Two—Security Functional Requirements (SFRs)
- ▲ Part Three—Security Assurance Requirements (SARs)

The Common Evaluation Method (CEM), the detailed list of procedures to be used by laboratories in performing evaluations, is available at the same site.

Common Criteria Around the World

An “alphabet soup” of government agencies operate the Common Criteria national schemes worldwide. See <http://www.commoncriteriaportal.org/public/developer/natscheme.html> for current list of the CCRA countries). 

Alex Ragen is a Jerusalem, Israel-based CISSP-certified information security professional (and ISSA member) who has managed numerous successful Common Criteria, FIPS 140 and other evaluations and certifications since 1998, in the US, UK, Australia and other countries. His short book, Manager's Guide to Common Criteria, is available free at <http://www.alexragen.com>.

