Realtime publishers
"Leading the Conversation"

The Essentials Series

IT Compliance Volume II

sponsored by

SECURE® COMPUTING

by Rebecca Herold

Using Certified Products to Improve Compliance

by Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI ***April 2007***

What Does "Certified" Really Mean?

Over the past few years, there have been a slew of security certifications that have sprung up professing to validate that the security product you are buying has been independently vetted to validate that it is trustworthy and will not create more vulnerabilities than it closes if you implement it within your enterprise. Table 1 provides a listing of a few of the better-known such certifications.

Certification	What It Means
Common Criteria (CC) Certification	From the Common Criteria site (http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf): "The CC presents requirements for the IT security of a product or system under the distinct categories of functional requirements (CC Part 2) and assurance requirements (CC Part 3). The CC functional requirements define desired security behaviour. Assurance requirements are the basis for gaining confidence that the claimed security measures are effective and implemented correctly."
ISO/IEC 27001 Certification	From BSI Global (http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030126472&recid=253): "BS ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) and specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system (ISMS) within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations. The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. If an organization already has an operative business process management system (e.g. in relation to ISO 9001 or ISO 14001), it is preferable in most cases to satisfy the requirements of this International Standard within the existing management system."
NSS Group Certification	From NSS (http://www.nss.co.uk/aboutnss.htm): "The NSS Group awards are recognised world-wide as being the most desirable and essential when it comes to security products. Vendors consider the awards to be a crucial step in any security-related marketing campaign, whilst feedback from readers of the reports indicates that participation in an NSS Group test and/or one of the NSS Approved awards is a prerequisite for any security product in order to be considered for purchase."
FIPS-140	From NIST (http://csrc.nist.gov/cryptval/): "Security requirements cover 11 areas related to the design and implementation of a cryptographic module Within most areas, a cryptographic module receives a security level rating (1-4, from lowest to highest), depending on what requirements are met. For other areas that do not provide for different levels of security, a cryptographic module receives a rating that reflects fulfillment of all of the requirements for that area."
Cybertrust Certification	From Cybertrust (http://www.cybertrust.com/media/data_sheets/cybertrust_ds_certifications.pdf): "Created in 1997, Cybertrust offers the most mature certification program in the industry, with the largest customer base. We have programs to certify your enterprise, perimeter or locations. Or we can help you build your own certification program to ensure your partners, vendors and business units are meeting your standards."

CIS Software Certification	From CIS (http://www.cisecurity.org/trademarks.html): “The CIS Software Certification Mark signifies that a security software product has been: (1) tested to accurately measure and report the conformity of computer configurations with the technical settings and actions defined in the CIS Security Benchmark and (2) awarded Certification by CIS.”
BITS Certification	From BITS (http://www.bitsinfo.org/c_certification.html): “The BITS Product Certification Program tests technology products used to deliver financial services at unbiased and professional facilities against minimum-security criteria established by the financial services industry.”

Table 1: Sample security certifications.

However, there has also been much discussion and wide debate about how useful these certifications are. The value of these certifications really depends upon the scope of the certification, the goal the organization has for getting a certification, and the true independence of the certifying organization. Each of these certifications is achieved through its own evaluation process for certification.

Does Certification Really Mean You Have a Better Product?

In general, it is always a good thing to know that there has been an independent review of a security product prior to committing to the purchase. The key is to ensure qualified and truly non-biased reviewers performed the certification process, and that the certification was not obtained just by paying enough money for it.

I am skeptical of many vendor-specific certifications; some seem as though the only real benefit is to the vendor that is offering the certification as another revenue stream for their company, which weakens their objectivity. After all, if a vendor wants to sell as many of their certifications as possible to bump up their revenue, they are likely to not be as stringent as an organization—such as one of those providing certification for the Common Criteria—that is providing certification as a way to provide an internationally accepted methodology to validate the security of software.

Different Certifications = Different Meanings

A growing number of commercial firms and independent consultants offer impartial security assessment or audit services for software applications and systems. They range from a series of reviews, tests, and assessments throughout the software life cycle to focusing on post-development penetration testing, vulnerability scanning, and software security audits. Some software security testing tool vendors also offer testing and certification services, but the caveat is that the tests must be performed using their tools. Accredited vendors who use the independent security assessment methodologies, such as the Common Criteria, will provide assurance that they are using proven and accepted international methodologies to validate the security of software.

Other security certifications exist that are very specific to a particular security issue, such as FIPS-140 certification of cryptographic software. Cybertrust provides multiple certifications, including one for application security, one for the enterprise, and another for the network perimeter. Center for Internet Security (CIS) is a non-profit organization that uses benchmarking practices to evaluate security for systems and networks. BITS is for use only within the financial industry and strives to establish a validated set of security practices for banking and financial services with what they indicate is a simpler certification process than that of the Common Criteria.

As they apply to all types of organizations and are based upon accepted international standards and methodologies, let’s look more closely at the Common Criteria certification to validate the security of products, and the ISO/IEC 27001 certification to provide validation for the vendor organization itself.

Common Criteria

If a product is Common Criteria certified, does that mean it is completely secure? Not necessarily.

> ✎ The criteria are “common” in that they are shared internationally as the result of agreement among a number of countries that formerly had differing security criteria.

The Common Criteria is the most widely referred to international standard for evaluating software products and systems with significant security functionality. In the U.S., the Common Criteria consists of a two-step process:

1. Evaluation by an approved laboratory/vendor and then,
2. Validation by the government.

The assignment of Evaluation Assurance Level (EAL) ratings 1 through 4 is done by the National Information Assurance Partnership (NIAP) and EAL levels 5 through 7 are generally done by the National Security Agency (NSA). A number of countries have a reciprocity agreement for EAL levels 1 through 4.

> ✎ EAL is the numerical rating assigned to the target of the evaluation (such as a specific application or system) that reflects the depth of the assurance requirements met during the evaluation. Each EAL corresponds to a set of requirements covering the complete development of a product as it corresponds to a given level of security strictness. Common Criteria lists seven levels, with EAL1 being the most basic, least restrictive, and cheapest to implement and evaluate. EAL7 is the most stringent and most expensive. Higher EAL levels do not necessarily mean the software has "better security;" it means the security has been more extensively validated.

The Common Criteria contains:

- Enumeration of security functionality and capabilities, such as authentication and logging
- EAL 1 (low) through 7 (high), calling for increased levels of documentation, formality, and testing as the level numbers increase
- Consistent methods that must be followed by those doing the evaluation and certification

✎ The Common Criteria provides a global security standard that can assure those using them of consistent testing rigors and demonstrated levels of security capabilities.

Knowing that a security software product has obtained a Common Criteria certification provides assurance that it was truly independently analyzed. Be sure you are aware of the scope of the certification, and remember that the higher the EAL level, the more security validation that occurred to obtain certification.

Common Criteria certification tells the organizations using them that the applications and systems:

- Have been engineered to protect the applications and systems from compromise and unauthorized use
- Were tested and validated to the EAL level indicated; with the higher levels meaning more validations and testing occurred
- Were engineered according to a specific protection profile standard consisting of a standard minimum set of security requirements

✎ A protection profile is an independent set of security requirements for a specific category of IT products that meet specific consumer and user needs.

📖 For a list of CC evaluated products see http://www.commoncriteriaportal.org/public/consumer/index.php?menu=5.

ISO/IEC 27001 Certification

Whereas Common Criteria certifies the security capabilities of software and systems, ISO/IEC 27001 certification certifies the information security program and practices of an organization. ISO/IEC 27001 provides an international standard for organizations to use to establish, implement, operate, monitor, review, maintain, and improve upon their clearly defined Information Security Management System (ISMS).

> 🕮 An ISMS includes the organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources.

An ISMS encompasses the entire information security program and must integrate with and relate to all other parts of the enterprise. ISO/IEC 27001 lists the various organizational functions required for security certification, including a list of required documents that must be maintained and provided for review during the certification process.

ISO/IEC 27001 applies to all types of organizations. The prescribed ISMS must be established to be appropriate for the organization's risk level and overall risk management processes. ISO/IEC 27001 certification provides validated assurance that an organization has implemented the part of their security program that is encompassed by the scope of the ISMS certification in compliance with their own documented program. Authentic ISO/IEC 27001 certification can only be performed by accredited certification organizations and auditors.

> 🕮 As of March 2007, 3350 organizations throughout the world had achieved ISMS certification. See http://www.iso27001certificates.com/ for more information about those with ISMS certification along with a listing of accredited ISMS auditors and organizations.

Certification Assists with Compliance Efforts

The independent review of the security worthiness of software products and the associated product vendors is becoming so important that it is starting to show up more often within requests for proposals (RFPs) for vendor security products. Because virtually all organizations must now provide documented proof that they are appropriately safeguarding information to effectively minimize risks to an acceptable level to meet related compliance requirements, the certification helps to demonstrate that the organizations are following a standard of due care with regard to their software choices.

Not only must organizations implement secure applications for regulatory compliance, they increasingly must do so to comply with the requirements of their business partners. This compliance goes beyond just describing the security products they are using; it requires that the organizations provide documented proof that they have acceptable security in place. One such method of providing this proof is by using a certified security product.

> ✎ As organizations face compliance obligations and are expected to implement internationally accepted standards to safeguard information assets, there will be more emphasis on certification and accreditation of security prior to applications or systems implementation.

The most effective way to ensure secure applications and systems is through a continuous assessment process to manage risk and compliance with standards and regulations. Throughout the world, ISO/IEC 27001 has become the de facto standard for defining at a high level an effective ISMS. The Common Criteria product certification is becoming more widely pursued and recognized, especially as more organizations require such certification to use the products.

> ✎ The U.S. Department of Defense agencies mandate that security products considered for purchase must be Common Criteria certified.

Certified security products provide independent validation that software applications and systems satisfy specific security requirements relevant to a number of regulations and business partner contracts. Certain certifications, such as the Common Criteria, provide documentation and, in effect, an audit trail of the engineering considerations—from requirements to full evidence of compliance. They provide the justification of why certain security processes were, or were not, implemented and provide documented descriptions of how they were judged to be successfully effective. Such documentation and evidence can be very helpful when trying to demonstrate compliance to a regulatory auditor and could cut the time of the audit dramatically.