Sponsoring Organization Model for Information Technology Certification Systems

William H. Dashiell, *National Imagery and Mapping Agency*
Arnold Johnson, *National Institute of Standards and Technology*
Phil Brashear, *Electronic Data Systems*

Current acquisition reform trends have challenged acquisition managers to acquire software on time and within budget. The National Institute of Standards and Technology (NIST) Sponsoring Organization Model (SOM) can help acquisition managers and acquisition organizations ensure that the software they acquire fits their needs and is of acceptable quality, which in the long term will save organizations significant time and money. This article sets forth the need for and benefits of an SOM, presents a basic overview of the SOM, and gives three brief example SOM implementations.

Many government information technology (IT) acquisition managers and program managers acquire computer software or contract for the acquisition of special-purpose software to be maintained by the organization acquiring the software. To meet procurement (program) requirements within cost constraints, acquisition managers and program managers need to use all cost-reduction means or resources available. Since conformance to recognized standards is one indication of the completeness and maintainability of software products, conforming software can help hold down costs while meeting program requirements.

Recent Acquisition Reform

In 1996, both the U.S. Congress and the administration initiated efforts to streamline the federal government's acquisition activities by reducing the central management structure and strengthening the authority of each agency's acquisition decisions. As part of this activity, Congress passed the Information Technology Management Reform Act of 1996 (Division E of Public Law 104-106), and President Clinton signed Executive Order 13011, which emphasizes agency management of information technology and new government-wide interagency support activities to improve productivity, security, interoperability, and coordination of government resources. Public Law 104-133 emphasizes federal government use of voluntary industry standards and directs federal agencies to use voluntary standards and to participate in their development.

There is no government-wide requirement for certification of acquired software that is meant to conform to an IT standard nor is there a general requirement that all acquired software be developed using certified tools. However, standardization has enormous implications for maintainability and portability for a program manager, especially since the bulk of software costs are incurred during maintenance (including the porting of software to evolving hardware and operating systems). Therefore, it is important that all acquisition efforts take into consideration the specification of IT standards and the use of development tools (compilers, in particular) that have been tested for conformance to standards.

Good software development practices require that software meet appropriate standards. Some of these standards are maintained by various entities, historically including the NIST, the American National Standards Institute, the Institute of Electrical and Electronic Engineers, and the International Organization for Standardization.

Conformance to software standards is normally established by means of a validation test suite. Based on the successful results of processing these test suites under third-party observation, software products are validated as conforming to the appropriate standard.

Each software purchaser or user must determine whether products with nonconformities are acceptable as meeting their needs. A software validation program may provide the information for a better software selection.

Standardization of testing methods and criteria for conformance to selected IT standards allows developers of IT software to verify conformance to those standards. Verifiable conformance is important to meet procurement requirements, to allow interoperability of various software products, and to allow for the use and sharing of data among various software products. Validation testing by an independent third party, using a standardized conformance test suite, provides the best assurance that the developer has made a significant effort to comply with the appropriate standard.[1]

The Basic Model

Before delving into specific uses and applications of the SOM, it is important to understand the fundamental structure of the model as defined by the NIST. Implementations of the SOM are conformance testing (certification) systems. We will refer to these implementations as SOM certification systems (SOMCSs). An SOMCS (which can be tailored to fit an organization's needs) consists of the

- Sponsoring organization – the organization responsible for the software certification system's management, processes, and funding.
- Test method executive control committee – a committee of testing and process experts taken from all parties involved in the sponsoring organization. They are responsible for establishing the accepted testing methods and the requirements for conformity to a specified standard.
- A certificate-issuing organization – the NIST SOM also allows for multiple certificate-issuing organizations, each sponsoring one or more testing laboratories. This gives the sponsoring organization testing coverage for a wide variety of software types.
- One or more testing laboratories – testing organizations recognized by the certificate-issuing organization as being qualified to test specific types of software against specified standards.

The basic (tailorable) NIST SOM for an IT certification system consists of two parts: a list of suggested functions (Table 1) and a list of suggested roles (Table 2). The contents of both lists were derived from NIST's test development and validation experiences. These lists are not all inclusive. An acquisition organization may require functions and roles not included in the NIST lists or may not require some of the functions or roles. To implement the model, a sponsoring organization chooses required functions and roles, maps the functions to the roles, and assigns specific organizations to the roles.

The central element in the resulting certification system is the sponsoring organization, which plays a key role in establishing and maintaining the system. The sponsoring organization may be any authority that assumes responsibility for the certification system. It may be composed of any combination of the following organizations: consortia, government agencies, or private software industry. Together, they work to broaden the scope of certification recognition.

Use and Benefits of the SOM

How can acquisition managers or program managers take advantage of existing SOMCSs (such as those sponsored by the Air Transport Association, the U.S. Geological Survey, or the Electronic Data Systems (EDS) Conformance Testing Center [explained later in the article]) to make the best software selection? Neither acquisition managers nor program managers use the SOMCS directly but depend on products and results from the SOMCS. For example, acquisition managers can develop better solicitation requirements by requiring the use of products with certificates from existing SOMCSs or can develop their own SOMCS for this purpose. The program manager can use the information provided by an SOMCS to select a tested product that best meets the program's needs, which saves the program money. This "get-it-right-the-first-time" method results in lower software lifecycle costs compared to low-cost software that may not meet all the chosen standard's requirements and therefore may require an inordinate amount of maintenance and modification.

The SOM is applicable to acquisitions or programs in which

- A software product is a deliverable, and a recognized standard exists to which the product should conform, such as C++ compilers, which should conform to the (not yet completed) International Standard or mapping information databases, which should conform to the Topological Vector Profile of the Spatial Data Transfer Standard.
- A software product is to be used in the development of a deliverable, and the government must maintain the deliverable, such as delivery of a command and control software system to be developed using standardized programming languages or delivery of a design specification in which all schematics are to be delivered in a format conforming to the Computer-Aided Acquisition and Logistics Support profile of the Computer Graphics Metafile (CGM) standard.

In these cases, the solicitation should specify that all such software products be tested by a certification system based on the SOM. If the acquiring agency is a sole or joint sponsor of an SOMCS, the solicitation can specify their SOMCS as the source of certificates.

The benefits of using an SOMCS include

- (First case, above) the assurance that delivered software products have been subjected to standardized testing procedures, using known test instruments, under the supervision of a disinterested third party. This provides acquisition managers with a set of objective assessments on which to base a procurement decision.
- (First case, above) some assurance that government use of delivered software products will have predictable results (as promised by the relevant standard).
- (First case, above) assurance that government employees who use delivered software products will not have to be retrained to use non-standard features.
- (Second case, above) assurance that deliverables developed using the

Table 1. *Certification system functions.*

Establish policies and procedures.
Recognize certificate-issuing organizations.
Resolve technical and procedural issues.
Approve content and use of the test suite.
Issue validation certificates.
Maintain a public list of validated products.
Recognize testing laboratories.
Maintain conformance test suite.
Conduct conformance testing.

Table 2. *Certification system roles.*

IT Standard Committee
Sponsoring Organization
Test Suite Developer/Maintainer
Advisory/Control Board
Certificate-Issuing Organization
Technical Reviewers/Experts
Testing Laboratory
Users of SOM Products
Validation Customer

tested software products can be modified as needed, using either the tested software products or other products known to conform to the same standard.
- (Second case, above) assurance that deliverables have known interface characteristics, e.g., data sharing, and that software using those interfaces will have specified behaviors as specified by the relevant standard.

Solicitation Wording

Because of Public Law 104-133, software procurement solicitations should contain requirements for conformance testing of IT products when the delivered products are expected to conform to an IT standard or when they are used to develop products to be delivered to and maintained by the acquiring organization. Major benefits are the existence of a software standard against which to compare when the software does not function properly and the increased assurance that the software will be maintained by the vendors and that interfaces with other conforming software will function as expected by the standard. Specific procurement activities have the authority to determine the demonstrated degree of conformance (either zero nonconformities or some limited number of nonconformities exposed by testing).

But why would one knowingly purchase software with known nonconformities? The NIST SOM requires that a Validation Summary Report be written for each validation effort. The Validation Summary Report is produced by a testing laboratory and contains the results that are observed from validation testing of a specific software product under test. Acquisition managers and program managers who review the Validation Summary Report for software that fits their requirements may find that the nonconformities exist in functional areas that are irrelevant to their program's needs. For example, they may be seeking a standardized application language compiler for an embedded system that has no need for text input and output. In this case, a nonconforming compiler that does not support text input and output may provide the best value—a potential for significant savings.

The NIST has developed suggested wording for acquisitions for which zero nonconformities are allowed or acquisitions for which limited nonconformities are allowed. (http://sdct-sunsrv1.ncsl.nist.gov/~ftp/vpl/validwrd.htm). Those acquisition managers and program managers whose needs require full conformance should select the zero nonconformities wording.

In addition to allowing variations in the number of nonconformities, the suggested solicitation wording allows acquisition managers and program managers to select one of three validation options: *delayed validation, prior validation,* and *prior validation testing (with errors)*.

Delayed validation allows IT suppliers to offer products that may not have been tested prior to contract award but must be tested during the contract period. This option would allow an acquisition manager to purchase a software product being developed (perhaps state of the art) and know the product will be assessed for conformance to the standard during the contract period. The risk is that the software may not meet the requirements of the standard, and, therefore, the procurement manager may negotiate a better price.

Prior validation requires product suppliers to have their products validated with zero nonconformities prior to contract award. Here, the acquisition manager and the program manager have the greatest assurance that the product meets the standard.

Prior validation testing (with errors) requires that the products be tested prior to being offered in response to the solicitation request and allows for testing results exhibiting nonconformities. Those exhibited nonconformities, summarized in a Validation Summary Report, may not be important to the program needs or software users and may represent a cost savings to the acquisition manager and the program manager.

Extrapolation from Validation Results

With ever-shrinking budgets, it is not feasible to directly test all candidate IT products for conformance, since formal validation can be expensive, time-consuming, and resource-intensive. Acquisition managers may decide to extrapolate information from the test results published by the certificate-issuing organization based on additional research, demonstrations, or warranties by the IT product supplier. It must be kept in mind that a validation certificate attests only to the successful testing of a product in a particular environment (hardware and system software). One cannot assume that the conformance of a product in a particular environment implies the conformance of a different version of the product (even from the same implementer) or the same version in a different operating environment. It is the acquisition manager and the program manager's responsibility, not an outside organization's, to review the certificate-issuing organization's Validated Product List and determine the applicability of these validations to the needs of the acquisition manager and the program manager. The applicability and usefulness of a validation certificate should be based on the size and timing of the procurement.

SOM Example Implementations

The NIST Directory of Conformance Testing Programs, Products and Services (http://www.itl.nist.gov/div897/ctg/ctdhome.htm) lists some existing testing services, including the following current implementations of the NIST SOM. The descriptions below illustrate some of the variations possible in implementing the model.

Government Agency with Commercial Certificate-Issuing Organization

The U.S. Geological Survey (USGS), an agency of the Department of the Interior, sponsors a certification system (Figure 1) for IT products that implement the Spatial Data Transfer Standard, Topological Vector Profile (SDTS TVP).

This standard specifies formats for the transfer of spatial data among different computer systems. The USGS, with assistance from the NIST, has developed a test suite to validate products that implement SDTS.

The USGS (http://mcmcweb.er.usgs.gov/sdts/conform.html) has recognized the Conformance Testing Center (CTC) at EDS (http://eds-conform.com/SDTS.html) as both a certificate-issuing organization and a testing laboratory for the SDTS TVP certification system.

Trade Association with Commercial Testing Laboratory

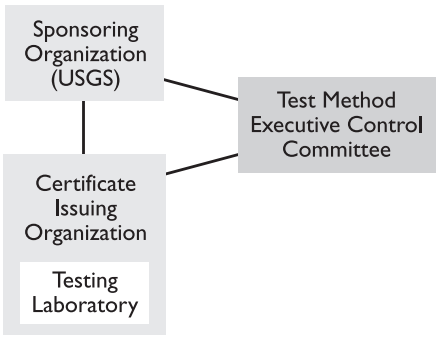
The Air Transport Association (ATA), a trade association, has established a certification system (Figure 2) for products that implement the CGM ATA Profile (as defined in ATA 2100 Specification, Graphics Exchange).

The NIST CGM Interpreter Test Suite is used to validate interpreters for the CGM ATA. The NIST CGM ATA interpreter test service is expected to be terminated in 1998, when the ATA establishes a CGM testing program. The ATA, serving as both sponsoring organization and certificate-issuing organization for its certification system, has solicited for testing laboratories (http://www.itl.nist.gov/div897/ctg/graphics/cgm.htm).

Commercial Sponsoring Organization

In reaction to the withdrawal of the NIST and the Ada Joint Program Office (AJPO) from validation of language processors (compilers), EDS operates a compiler certification system (Figure 3)

Figure 1. *SDTS TVP certification system.*



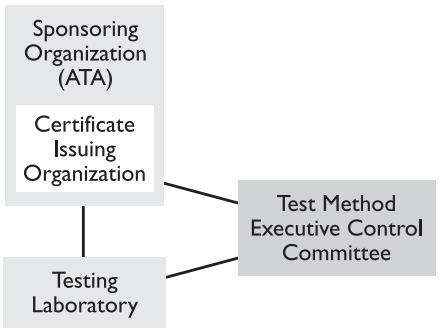


Figure 2. *ATA CGM certification system.*

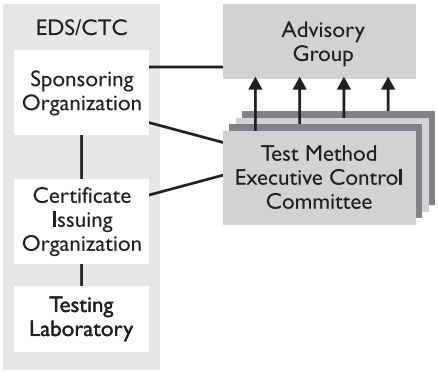


Figure 3: *EDS CTC compiler certification system.*

as an implementation of the NIST SOM. This system provides validation testing services and issues certificates for Ada 83 and 87, Ada 95, C, COBOL 85, and FORTRAN 77 compilers as well as Structured Query Language processors. In most cases, the test suites used for these validations are the ones that the NIST and AJPO have used in the past. Plans to test C++ compilers are underway (http://eds-conform.com).

As Figure 3 shows, EDS CTC fulfills all three major roles: sponsoring organization, certificate-issuing organization, and testing laboratory. A test method executive control committee is established for each standard, with the majority of the members drawn from the validation customers and organizations implementing the standard. Each test method executive control committee advises EDS CTC on policy and procedures specific to validations for its standard as well as controlling the test suite and resolving validation issues related to that standard. An advisory group provides advice on the overall certification system policy and procedures. Each test method executive control committee names one of its validation customer members to serve on the advisory group.

The EDS CTC certification system has only one testing laboratory, which is operated by the CTC. However, procedures are in place to recognize other testing laboratories and to issue certificates in accordance with their recommendations.

Conclusion

Government acquisition reform emphasizes decentralized control of procurement. At the same time, there is a strong trend to privatize functions previously performed by the government. These forces increase both the power and the responsibility of the acquisition manager and the program manager. In particular, these managers are empowered to take advantage of SOMCSs to ensure the acquisition and use of software that conforms to standards. Doing so can significantly reduce development and maintenance costs while resulting in more reliable systems with predictable behavior. ◆

About the Authors

William H. Dashiell is a computer scientist at the Department of Defense National Imagery and Mapping Agency. He has worked on the development of software testing by statistical methods using binomial models, coverage designs, mutation testing, and usage models. He has contributed to the development of conformance and testing protocols for federal, national, and international information technology standards. He has a bachelor's degree in business administration and education, a master's degree in education technology, and a doctorate in mathematics education from the University of Maryland. He also has a master's degree in computer science from Hood College in Maryland.

National Imagery and Mapping Agency
Washington Navy Yard, Building 213

SNIT Mail Stop N-61
1200 First Street, S.E.
Washington, D.C. 20303-0001
Voice: 202-863-3516

Arnold Johnson has spent more than 20 years managing the development and operation of testing and certification programs spanning 10 federal and international IT standards including negotiating six bilateral or multilateral international agreements for mutual recognition of test results. He is currently the NIST program manager for the National Information Assurance Partnership, a joint initiative by the National Security Agency and NIST to foster the development of tests, test methods, tools, and commercial testing laboratories to evaluate the quality of IT security products.

National Institute of Standards and Technology
Information Technology Laboratory
Building 820, Room 517
Gaithersburg, MD 20899
Voice: 301-975-3247
E-mail: arnold.johnson@nist.gov

Phil Brashear is a senior systems engineer at EDS in Dayton, Ohio, where he leads the EDS Conformance Testing Center and the maintenance of the Ada compiler validation test suite. He previously directed compiler validation efforts at CTA Incorporated from 1989 to 1997. From 1986 to 1989, he performed compiler validations and directed test suite enhancements at SofTech, Inc. Prior to 1986, he was a member of the mathematics and computer science faculties at Eastern Kentucky University. He has a bachelor's degree in mathematics education from the University of Kentucky, a master's degree in mathematics from Northwestern University, and has completed the course work and examinations for a doctorate in mathematics at the University of Georgia.

Phil Brashear
EDS Conformance Testing Center
Dayton, Ohio
E-mail: phil.brashear@acm.org

Additional Reading

1. ISO/IEC Guide 2, *General Terms and Their Definitions Concerning Standardization and Related Activities.*
2. ISO/IEC Guide 25, *General Requirements for the Competence of Calibration and Testing Laboratories,* 3rd ed., 1990.
3. ISO/IEC Guide 28, *General Rules for a Model Third-Party Certification System for Products*.
4. ISO/IEC Guide 38, *General Requirements for the Acceptance of Testing Laboratories.*
5. ISO/IEC Guide 39, *General Requirements for the Acceptance of Inspection Bodies.*
6. ISO/IEC Guide 40, *General Requirements for the Acceptance of Certification Bodies*, currently under revision, April 1995.
7. ISO/IEC Guide 42, *Guidelines for a Step by Step Approach to an International Certification System.*
8. ISO/IEC Guide 43, *Development and Operation of Laboratory Proficiency Testing.*
9. ISO/IEC Guide 44, *General Rules for ISO/IEC and IEC International Third-Party Certification Schemes for Products.*
10. ISO/IEC Guide 56, *An Approach to the Review by a Certification Body of Its Own Internal Quality System.*
11. ISO/IEC Guide 60, *Code of Good Practice for Conformity Assessment*.
12. ISO/IEC Technical Report 13233, "IT – Interpretation of Accreditation Requirements," ISO/IEC Guide 25, *Accreditation of IT and Telecommunications Testing Laboratories for Software and Protocol Testing Services*, Nov. 30, 1995.
13. Rada, Roy, "Who Will Test Conformance?" *ACM Communications*, January 1996.
14. *Test Method Control Procedures Model, Workshop on Harmonization of Programming Languages and Graphics Validations*, March 15-16, 1994, NIST, Computer Systems Laboratory.

Note

1. Two concepts must be emphasized. First, validation (conformance) testing does not warrant that the product tested is free of nonconformities, even if all tests are passed. Second, validation testing is not intended as a means of performance benchmarking.

WebTALK: A New On-Line Discussion Forum

CROSSTALK is based on the premise that sharing information is the fastest way to learn. The software engineering field, still in its infancy, is still trying to define itself–no other industry can serve as a model for the process and techniques needed to produce good software. Trial and error is still the predominant, but we hope doomed, method.

With that in mind, we hope you will share your ideas about software development–or your reaction to ideas presented in *CROSSTALK*–via a new feature on our Web site: WebTALK, an on-line forum that affords you the opportunity to engage in some cross talk of your own. The discussions are formatted as threads to make conversation as easy as a mouse click. Access WebTALK from *CROSSTALK*'s home page (http://www.stsc.hill.af.mil/CrossTalk/crostalk.html).

Your ideas count. Be heard!