

Draft for Discussion  
Quality Assurance and Configuration Management Requirements  
March 7, 2007

At the December 2006 TGDC Plenary, the TGDC agreed that the ISO 9000/9001 standards should provide the framework for VVSG07 requirements dealing with quality assurance. In that context, this paper presents, for discussion, a draft set of such requirements. Some attempt is made to use the format of the current draft VVSG07 document, e.g., green for the actual requirements, Source, DISCUSSION, and Applies to fields, etc.

Unresolved Issue:

A key principle in the application of the ISO 9000/9001 standards is that adopting organizations apply the principles of the standards throughout their organizations, and throughout their product life cycles. In particular, the good practices called for by the standards should begin before, and encompass, the entire design and development of vendor products. This is usually accomplished by requiring that the quality manual, which describes the scope and details of the organization's quality procedures, be developed, delivered, and approved by an appropriate authority *before* work on a new product begins.

The question here is how this goal can be accomplished in the context of voting system certification. One of the perceived weaknesses of the quality assurance procedures specified in the VSS and the current VVSG is that the vendor is only required to deliver the details of his QA procedures as part of the Technical Data Package, that is, at the time the voting system is submitted for certification. At that point, even if deficiencies were discovered in the procedures, it may be too late to do anything about them.

We've attempted to address this issue in requirement IV.1.1-A:

All voting system vendors shall develop and present to the EAC a complete Quality and Configuration Management Manual. This presentation shall occur during the Manufacturer Registration process as specified in the EAC Testing and Certification Manual, and before the start of the design and development process for the given voting system.

The EAC's Manufacturer Registration process would be the obvious place for the presentation of the Quality and Configuration Management Manual. The problem is that the EAC Testing and Certification Manual doesn't specify a time frame for this event. In the extreme case the registration could occur the day before the vendor delivers his product for testing. It would then be impossible to determine whether or not the policies and procedures in the QA/CM Manual had been, in fact, adhered to throughout the design and development stages. Our strawman solution is to be explicit and require that this be done "before the start of the design and development

process." However, this has the effect of specifying a time frame on the Manufacturer Registration process, i.e., adding a nontrivial requirement to the EAC manual, which may be outside the scope of the VVSG. If this approach is taken, we might have to request a modification to the EAC Manual. An alternative would be to drop the "before" condition. The second sentence of the requirement would then be simply "This presentation shall occur during the Manufacturer Registration process as specified in the EAC Testing and Certification Manual," In this approach, we could add an informative discussion that advises that the Manual should be delivered before the start of design and development.

The alternative would eliminate the immediate problem, but the cost might be a reduction in the benefits we hope to realize in adopting the ISO framework in the first place.

# Volume III – Product Standard

## 1. Quality Assurance and Configuration Management Requirements

The quality assurance and configuration management requirements discussed in this section help assure that voting systems conform with the requirements of the VVSG. Quality Assurance is a vendor function with associated practices that is initiated prior to system development and continues throughout the maintenance life cycle of the voting system. Quality Assurance focuses on building quality into a system and reducing dependence on system tests at the end of the life cycle to detect deficiencies, thus helping ensure that the system:

- Meets stated requirements and objectives;
- Adheres to established standards and conventions;
- Functions consistent with related components and meets dependencies for use within the jurisdiction; and
- Reflects all changes approved during its initial development, internal testing, qualification, and, if applicable, additional certification processes.

Configuration management is a set of activities and associated practices that ensures full knowledge and control of the components of a system, starting with its initial development progressing through its ongoing maintenance and enhancement, and including its operational life cycle.

### 1.1 Standards Based Framework for Quality Assurance and Configuration Management

The requirement in this section establishes the quality assurance and configuration standards that voting system vendors shall conform to. The requirement to develop a Quality and Configuration Management manual, and the detailed requirements on that manual, are contained in Volume IV.

1.1-A Voting system vendors shall implement a quality assurance and configuration management program that is conformant with the recognized ISO standards in these areas:

- ISO 9000:2005
- ISO 9001:2000
- ISO 10007:2003

*Source:* New requirement

*Applies to:* Voting system

## **1.2 Configuration Management Requirements**

This section specifies the key configuration management requirements for voting system vendors. The requirements include those of equipment tags and configuration logs. Continuation of the program, in the form of usage logs, is the responsibility of State and local officials.

### **1.2-A Identification of Systems**

Each voting system shall have an identification tag that is attached to the main body.

*Source:* New requirement

*Applies to:* Voting system

#### **1.2-A.1 Secure**

The tag shall be tamper-resistant and difficult to remove.

*Source:* New requirement

*Applies to:* Voting system

#### **1.2-A.2 Contents**

The tag shall contain the following information:

- The voting system model identification in the form of a model number and possibly a model name. The model identification identifies the exact variant or version of the system
- The serial number that uniquely identifies the system
- Identification of the vendor, including address and contact information for technical service, and vendor certification information
- Date of manufacture of the voting system.

*Source:* New requirement

*Applies to:* Voting system

### **1.2-B The Voting System Configuration Log**

For each voting system manufactured, a Voting System Configuration Log shall be established.

*Source:* New requirement

*Applies to:* Voting system

## DISCUSSION

The Log is initialized by the configuration data supplied by the vendor. From that point on, it functions like a diary of the system. Entries are made by election officials whenever any change occurs. Every exception, disruption, anomaly, and every failure is recorded. Every time the cover is opened for inspection or a repair or maintenance is performed, an entry details what was done, and what component was changed against what other component, as well as any diagnosis of failures or exceptions.

### **1.2-B.1 Contents**

The Log shall contain the following information:

- The information on the system tag described in Requirement 1.3-A.2
- The identification of all critical components of the system
- The complete historical record, as developed by the vendor per Requirement 1.2-A.12, of all critical parts, components, and assemblies included in the voting system.

*Source:* New requirement

*Applies to:* Voting system

### **1.2-B.2 Storage**

The Log shall be kept on a medium that allows the writing, but not the modification or deletion, of records.

*Source:* New requirement

*Applies to:* Voting system

# Volume IV – Standards on Data to be Provided

## 1. Quality Assurance and Configuration Management Program

### 1.1 Quality and Configuration Management Manual

#### 1.1-A Develop and Present

All voting system vendors shall develop and present to the EAC a complete Quality and Configuration Management Manual. This presentation shall occur during the Manufacturer Registration process as specified in the EAC Testing and Certification Manual, and before the start of the design and development process for the given voting system.

*Source:* New requirement

##### 1.1-A.1 Processes and Procedures

The Manual shall detail the vendor's Quality Assurance and Configuration Management processes and procedures required by the VVSG. These processes and procedures shall conform with all requirements of the VVSG and the standards listed in 1.1-A.

*Source:* New requirement

##### 1.1-A.2 A Binding Commitment

The Manual shall declare that meeting the requirements of the entire VVSG is a binding commitment for the entire vendor organization.

*Source:* New requirement

##### 1.1-A.3 Project Plan

The Manual shall provide for the formulation of a project plan for the design and development of a voting system. It shall require the project plan to be clearly and unambiguously documented.

*Source:* New requirement

##### 1.1-A.4 Quality Check

The Manual shall require the project plan to include, at a minimum, one quality check during and at the end of the design phase, and one quality check during and at the end of the development phase. The project plan shall define the progress that is required before each quality check can be passed.

*Source:* New requirement

## DISCUSSION

A "quality check" is the sum of the activities Design and Development Review, Design and Development Verification, and Design and Development Validation, as defined in ISO 9001 Sections 7.3.4. through 7.3.6.

### **1.1-A.5 Problem Log**

The Manual shall require the vendor to maintain a log in which all difficulties encountered during the design and development phase for a voting system are required to be recorded. The log shall be available for inspection by the test lab.

*Source:* New requirement

## DISCUSSION

"Difficulties" are any occasions when it is recognized that changes in past design decisions or in the project plan are necessary to complete the project.

### **1.1-A-6 Critical Parts**

The Manual shall specify rules that define what parts and components of the voting system are to be considered as critical. A part or component shall be defined as critical if its failure may

- cause a faulty display of options
- cause an uncertainty if voter's choice has been recorded
- cause a false recording of vote cast
- cause the change of stored votes
- cause the false transmission for polling station totals
- cause injury to voters or staff
- provide an opening for tampering
- violate a voter's privacy
- cause a false accumulation of polling station totals
- cause a false transmission for regional totals
- give the appearance of irregularity.

As used here, "components" shall include software modules.

*Source:* New requirement

### **1.1-A.7 Testing Statements for Every Part**

The Manual shall require that the design and development process of a voting system produce statements for every part, assembly, and component, whether to be manufactured

by the vendor or obtained elsewhere, that impacts conformity to the VVSG. These statements shall define verifiable requirements against which the part, assembly, or component can be tested at the end of its manufacturing process, or upon delivery, as appropriate. The requirements shall be defined in such a way that any part, component, or assembly that meets the requirements will provide the functionality and reliability required of it for the voting system to meet the overall functionality and reliability requirements specified in the VVSG.

*Source:* New requirement

#### **1.1-A.8 Inspection Processes for Every Part**

The Manual shall require that the design and development process define or identify processes by which all parts, components, and assemblies of a voting system can be tested for compliance with requirements developed under Requirement A.7.

*Source:* New requirement

#### **1.1-A.9 Testing Statements for the Entire Voting System**

The Manual shall require that the design and development process of a voting system produce a statement that defines verifiable requirements against which any voting system can be tested at the end of its manufacturing and assembly process in such a way that passing the test provides assurance that the voting system meets all requirements defined in the VVSG.

*Source:* New requirement

#### **1.1-A.10 Inspection of all Purchased Parts**

The Manual shall require that all purchased parts, assemblies, and components are tested according to the testing requirements developed under Requirement A.7 and the processes developed under Requirement A.8 before they are incorporated into a voting system. The records shall be maintained until such time as the certification of the voting system model is revoked.

*Source:* New requirement

#### **1.1-A.11 Inspection of all Manufactured Parts**

The Manual shall require that all manufactured parts, assemblies, and components are tested according to the testing requirements developed under Requirement A.7 and the processes developed under Requirement A.8 before they are incorporated into a voting system. The records shall be maintained until such time as the certification of the voting system model is revoked.



*Source:* New requirement

#### **1.1-A.12 Records of all Critical Parts**

The Manual shall require that for each part, assembly, and component, whether purchased or manufactured by the vendor, that has been defined as critical, records shall be kept that document the complete history of the part, assembly, or component. The records shall include the source of raw materials, the processes used in the manufacture, the time when critical manufacturing steps were taken, the organization or person that performed each critical manufacturing step, and the persons who performed the required inspections. The records shall also include documentation of any failures, discrepancies or anomalies that might have occurred during manufacture, of any actions taken to correct the failure, discrepancy or anomaly, and of the final determination that the problem has been corrected. These records shall be available for inspection.

*Source:* New requirement

#### **1.1-A.13 Technical capability for monitoring**

The Manual shall require the vendor to identify and maintain the technical capability to monitor the in-service performance of all voting systems sold throughout their life cycle.

*Source:* New requirement

### **DISCUSSION**

For the purpose of this and subsequent Requirements in this section, the term life cycle of a voting system model shall be defined as the time period from the delivery of the first voting system of that model to the time when the certification of the model is revoked.

#### **1.1-A.14 Technical Capability for Developing and Implementing Remedies**

The Manual shall require the vendor to identify and maintain the technical capability to develop and implement remedies that are suitable to correct any defects that led to in-service difficulties in all voting systems sold, throughout the life cycle of the voting system model.

*Source:* New requirement

#### **1.1-A.15 Financial capability to provide the product support**

The Manual shall require the vendor to identify and maintain the financial capability to provide product support as defined in Requirements A.13 and A.14 throughout the life cycle of the voting system model.

*Source:* New requirement

# Volume V – Testing Standard

## 1. Examination of Vendor Practices for Quality Assurance and Configuration Management

### 1.1 Quality Assurance

to be defined

### 1.2 Configuration Management

#### 1.2-A Identification of Systems

The test lab shall verify that the voting system has an identification tag attached to the main body as described in Volume III, <1.2-A>.

*Source:* New requirement

#### 1.2-B Configuration Log

The test lab shall verify that the voting system has associated with it a Configuration Log, as described in Volume III, <1.2-B>.

*Source:* New requirement