Volume I, Section 8
Table of Contents

8 Configuration Management

8.1 Scope

This section contains specific requirements for configuration management of voting systems. For the purpose of the Standards, configuration management is defined as a set of activities and associated practices that ensures full knowledge and control of the components of a system, starting with its initial development and progressing through its ongoing maintenance and enhancement. This section describes activities in terms of their purposes and outcomes. It does not describe specific procedures or steps to be employed to accomplish them. Specific steps and procedures are left to the vendor to select.

Vendors are required to submit these procedures to the Independent Test Authority (ITA) as part of the Technical Data Package (TDP) for system qualifications described in *Volume II, Voting Systems Qualification Testing Standards*, for review against the requirements of this section. Additionally, state or local election legislation, regulations, or contractual agreements may require the vendor to conform to additional standards for configuration management or to adopt specific required procedures. Further, authorized election officials or their representatives reserve the right to inspect vendor facilities and operations to determine conformance with the vendor's reported procedures and with any additional requirements.

8.1.1 Configuration Management Requirements

Configuration management addresses a broad set of record keeping, audit, and reporting activities that contribute to full knowledge and control of a system and its components. These activities include:

- Identifying discrete system components;
- Creating records of a formal baseline and later versions of components;
- Controlling changes made to the system and its components;
- Releasing new versions of the system to ITAs;

- Releasing new versions of the system to customers;
- Auditing the system, including its documentation, against configuration management records;
- Controlling interfaces to other systems; and
- Identifying tools used to build and maintain the system.

8.1.2 Organization of Configuration Management Standards

The standards for configuration management presented in this section include:

- Application of configuration management requirements;
- Configuration management policy;
- Configuration identification;
- Baseline, promotion, and demotion procedures;
- Configuration control procedures;
- Release process;
- Configuration audits; and
- Configuration management resources.

8.1.3 Application of Configuration Management Requirements

Requirements for configuration management apply regardless of the specific technologies employed to all voting systems subject to the Standards. These system components include:

a. Software components;

b. Hardware components;

c. Communications components;

d. Documentation;

e. Identification and naming and conventions (including changes to these conventions) for software programs and data files;

f. Development and testing artifacts such as test data and scripts; and

g. File archiving and data repositories.

8.2 Configuration Management Policy

The vendor shall describe its policies for configuration management in the TDP. This description shall address the following elements:

a. Scope and nature of configuration management program activities; and

b. Breadth of application of the vendor's policies and practices to the voting system (i.e., extent to which policies and practices apply to the total system, and extent to which policies and practices of suppliers apply to particular components, subsystems, or other defined system elements.

8.3 Configuration Identification

Configuration identification is the process of identifying, naming, and acquiring configuration items. Configuration identification encompasses all system components.

8.3.1 Structuring and Naming Configuration Items

The vendor shall describe the procedures and conventions used to:

a. Classify configuration items into categories and subcategories;

b. Uniquely number or otherwise identify configuration items; and

c. Name configuration items;

8.3.2 Versioning Conventions

When a system component is used to identify higher-level system elements, a vendor shall describe the conventions used to:

a. Identify the specific versions of individual configuration items and sets of items that are used by the vendor to identify higher level system elements such as subsystems;

b. Uniquely number or otherwise identify versions; and

c. Name versions.

8.4 Baseline, Promotion, and Demotion Procedures

The vendor shall establish formal procedures and conventions for establishing and providing a complete description of the procedures and related conventions used to:

a. Establish a particular instance of a component as the starting baseline;

b. Promote subsequent instances of a component to baseline status as development progresses through to completion of the initial completed version released to the ITAs for qualification testing; and

c. Promote subsequent instances of a component to baseline status as the component is maintained throughout its life cycle until system retirement (i.e., the system is no longer sold or maintained by the vendor).

8.5 Configuration Control Procedures

Configuration control is the process of approving and implementing changes to a configuration item to prevent unauthorized additions, changes, or deletions. The vendor shall establish such procedures and related conventions, providing a complete description of those procedures used to:

a. Develop and maintain internally developed items;

b. Acquire and maintain third-party items;

c. Resolve internally identified defects for items regardless of their origin; and

d. Resolve externally identified and reported defects (i.e., by customers and ITAs).

8.6 Release Process

The release process is the means by which the vendor installs, transfers, or migrates the system to the ITAs and, eventually, to its customers. The vendor shall establish such procedures and related conventions, providing a complete description of those used to:

a. Perform a first release of the system to an ITA;

b. Perform a subsequent maintenance or upgrade release of the system, or a particular components, to an ITA;

c. Perform the initial delivery and installation of the system to a customer, including confirmation that the installed version of the system matches exactly the qualified system version; and

d. Perform a subsequent maintenance or upgrade release of the system, or a particular component, to a customer, including confirmation that the installed version of the system matches exactly the qualified system version.

8.7 Configuration Audits

The Standards require two types of configuration audits: Physical Configuration Audits (PCA) and Functional Configuration Audits (FCA).

8.7.1 Physical Configuration Audit

The PCA is conducted by the ITA to compare the voting system components submitted for qualification to the vendor's technical documentation. For the PCA, a vendor shall provide:

a. Identification of all items that are to be a part of the software release;

b. Specification of compiler (or choice of compilers) to be used to generate executable programs;

c. Identification of all hardware that interfaces with the software;

d. Configuration baseline data for all hardware that is unique to the system;

e. Copies of all software documentation intended for distribution to users, including program listings, specifications, operations manual, voter manual, and maintenance manual;

f. User acceptance test procedures and acceptance criteria; and

g. Identification of any changes between the physical configuration of the system submitted for the PCA and that submitted for the FCA, with a certification that any differences do not degrade the functional characteristics; and

h. Complete descriptions of its procedures and related conventions used to support this audit by:

   1) Establishing a configuration baseline of the software and hardware to be tested; and

   2) Confirming whether the system documentation matches the corresponding system components.

8.7.2 Functional Configuration Audit

The FCA is conducted by the ITA to verify that the system performs all the functions described in the system documentation. The vendor shall:

a. Completely describe its procedures and related conventions used to support this audit for all system components;

b. Provide the following information to support this audit:

   1) Copies of all procedures used for module or unit testing, integration testing, and system testing;

   2) Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests; and

   3) Records of all tests performed by the procedures listed above, including error corrections and retests.

In addition to such audits performed by ITAs during the system qualification process, elements of this audit may also be performed by state election organizations during the system certification process, and individual jurisdictions during system acceptance testing.

8.8 Configuration Management Resources

Often, configuration management activities are performed with the aid of automated tools. Assuring that such tools are available throughout the system life cycle, including if the vendor is acquired by or merged with another organization, is critical to effective configuration management. Vendors may choose the specific tools they

use to perform the record keeping, audit, and reporting activities of the configuration management standards. The resources documentation standard provided below focus on assuring that procedures are in place to record information about the tools to help ensure that they, and the data they contain, can be transferred effectively and promptly to a third party should the need arise. Within this context, a vendor is required to develop and provide a complete description of the procedures and related practices for maintaining information about:

a. Specific tools used, current version, and operating environment;

b. Physical location of the tools, including designation of computer directories and files; and

c. Procedures and training materials for using the tools.