SYSTEM CONTROL STANDARDS

CONTENTS PAGE

1. GENERAL

1.01 ▶This section states Bell System policies regarding the incorporation of controls in all centrally developed information systems (CDS) and prescribes standard requirements for implementing these policies.◀ System controls are those actions, procedures, processes, or physical barriers that ensure the accuracy, completeness, protection, and security of an information system's data and operations.

1.02 This section has been reissued to clarify its applicability to all CDSs, regardless of the size of the computer. Issue 1 did not receive general distribution. Also, the descriptions of Bell System policy and of the standard requirements have been clarified and separated. Revision arrows are used to denote significant changes.

▶1.03 This section is issued as a standard and applies to:

(a) Project managers and all members of the development teams for CDSs.

(b) All centrally developed computer-based systems, regardless of size, except those internal to Bell Laboratories and Western Electric and those that are integrated into the switching and transmission components of the network or customer products. Although some systems are more specifically referred to as operations systems or operations support systems, they will be referred to as information systems in this section.◀

▶1.04 While this standard applies to CDSs, the content is generally necessary for the adequate control of all information systems. It is recommended that each Operating Telephone Company apply this standard, or an equivalent, to its system development activities.◀

1.05 The terminology used in this section is based on the methodology of Total Systems Development (TSD) as described in Section 007-208-310, Project Management; Section 007-200-201, Glossary of System Development Terms and Acronyms; and Section 007-220-200, System Development Milestones (under development). However, these controls apply to the development of all CDSs regardless of the methodology used.

▶1.06 This section is organized in five parts.

(a) Part 1 describes to whom and when this section applies and contains general information about the section.

(b) Part 2 describes the Bell System policies regarding the control features and facilities in CDSs. Project managers, system developers, and other members of the development team are required to adhere to these standards. Detailed guidelines for implementing these standards are provided in Section 007-209-302, System Control Guidelines. It is the responsibility of the development team to determine how these standards should be implemented in the design of each CDS.

(c) Parts 3, 4, and 5 describe the standard requirements that should be incorporated, in a cost-effective manner, in the design of CDSs. Part 3 outlines the system control areas; Part 4 describes the quality and attributes of the requirements; and Part 5 describes the documentation required by the development team. The standards require the documentation of the controls development process and of the controls themselves.◀

Printed in U.S.A.

2. POLICIES REGARDING CONTROLS

2.01 It is the policy of the Bell System to adequately protect (control) all of its assets (eg, financial, data, etc). The need for adequate controls is particularly important in information system applications. Controls must be included in all aspects of manual and machine processing.

2.02 Controls must be included in the design of any information system that impacts or could potentially impact:

- The level of service provided the customers of the Bell System
- Bell System revenues or expenses
- Bell System compliance with any regulatory or legal requirements
- The protection of Bell System proprietary or private information
- Safeguarding of Bell System assets
- Adherence to the policy stated in the "Bell System Policy Regarding Privacy of Employee Records"
- Service or cost measurement plans
- The protection of proprietary or private information belonging to other companies (non-Bell) when ***data services*** are provided by the Bell System.

2.03 The degree of control necessary for any given information system application must be determined by the project manager (who represents the user) and the developer, based upon such factors as controls development costs, value of the data to the business, the availability of the system, and examination capabilities when operational. This may require a risk and cost-benefit analysis.

(a) In evaluating the degree of control necessary, the designer should also consider the vulnerability of data and programs and the risks associated with their loss or disclosure.

(b) The privacy that personnel data requires is another important consideration in the selection of controls.

(c) The impact of manual/mechanized interactions/interfaces with other systems should be included in the analysis.

2.04 The project manager and the development team are jointly responsible for the identification of the degree of control required based on the system requirements and design objectives. The development team designs and implements the controls.

2.05 The use of the controls features of an information system shall be documented in the appropriate parts of the deliverable documentation for the system.

3. SYSTEM CONTROLS AREAS

3.01 Controls should specifically address the following functional areas:

- Source data preparation
- Input processing
- Update processing
- Output processing (including distribution)
- Error processing
- User products
- Computer operations
- System administration
- Data base administration
- Communications administration
- Installation/conversion
- Change management
- System test and performance review
- System back-up and recovery
- System access.

4. QUALITY ATTRIBUTES

4.01 Each control should be evaluated for the following quality attributes:

- Completeness and accuracy
- Protection
- Security
- Privacy.

4.02 ***Completeness and accuracy*** refer to the degree to which information produced by the system is all-inclusive, up to date, and representative of actual conditions. For every system, the necessary level of completeness and accuracy of data should be established in the system requirements. Management Trials and System Examination capabilities are required in information systems for management to verify completeness and accuracy.

4.03 ***Protection*** involves the controls that safeguard data and physical facilities. Protection controls should provide the capability for:

- Reconstruction of data bases
- Recovery in a timely manner
- Back-up processing capabilities.

Retention requirements should be established for all information to comply with legal and corporate policy needs.

4.04 ***Data security*** involves the controls that restrict or deny information and resources from unauthorized use. It is the user's responsibility to authorize access to the system. Systems should employ security control measures consistent with the proprietary or private nature of the information they handle and to the extent to which the information is exposed to potential unauthorized access. United States Government classified information should be protected in accordance with the requirements of the Department of Defense *Industrial Security Manual for Safeguarding Classified Information.* State and local government information should be protected in accordance with relevant laws.

4.05 ***Privacy*** involves the controls that restrict or deny access to information about individuals based on rights determined by law and by corporate policy. Controls should be established that ensure the requirements of applicable privacy laws are met. Controls should be established that ensure access to and use of personnel information in accordance with the policy stated in the "Bell System Policy Regarding Privacy of Employee Records" and the guidelines for its implementation and administration.

5. CONTROLS IMPLEMENTATION STANDARDS

5.01 The cost-effective selection and design of information system controls shall be in relationship to controls development cost vs. the value of the resource to the business and shall be formally documented. These documents shall contain the following items:

(a) The vulnerabilities considered in determining the system's control requirements.

(b) The rationale used to select and design the controls actually employed.

5.02 The control needs of an information system shall be considered in all phases of the system's development. This includes new systems, existing systems with identified control weaknesses, and planned enhancements to existing systems. The following describes the control considerations when a system is developed using TSD methodology. Information systems developed using other developmental methodologies shall employ similar control considerations.

(a) During the feasibility phase, the area of control shall be considered in the investigation of alternative system designs. The recommended alternatives shall include a general outline of the control requirements of the system.

(b) Feasibility phase reports shall include supporting control documentation that identifies:

- Critical data
- Potential vulnerabilities
- General levels of controls
- Major costs of controls.

(c) The control requirements of the system shall be determined in detail in the definition phase. The control requirements shall be included in appropriate outputs of the definition phase (eg, sys-

tem definition, system requirements, or system specifications).

(d) In the preliminary design phase, the general control techniques to be used in the system are designed. Documentation at the completion of this phase shall include a description of the control techniques.

(e) When a review and approval step is conducted at the end of the preliminary design phase, the reviewing organization shall ***review the planned controls*** to ensure that system control concerns have been adequately considered and the selected controls appear valid.

(f) In the detail design phase, the designer incorporates the controls into the system design.

(g) A description of the controls employed in the completed system shall be included in the developmental and deliverable system documentation. When developing system documentation, the following sections should be referenced:

SECTION	TITLE
007-227-305	Developmental Documentation
007-227-310	Developmental Documentation Specifications
007-230-210	System Deliverable Documentation