SYSTEM CONTROLS AND EXAMINATION GUIDE PREPARATION INSTRUCTIONS

CONTENTS PAGE

1. GENERAL

1.01 ***Purpose:*** This practice provides an outline for the preparation of a System Controls and Examination Guide (formerly System Audit Guide). The System Controls and Examination Guide is one of several deliverable documents provided to support the operation of information systems. (See Section 007-230-210, *System Deliverable Documentation*, for a description of each deliverable document and its content.)

1.02 ***Reason for Issue:*** Whenever this section is reissued, the reason(s) for reissue will be given in this paragraph.

1.03 ***Applicability:*** This section is a guideline. The procedures described are recommended for use by developers of both locally and centrally developed systems. Users of the guide may include computer center application administrators, user data administrators, and auditors.

1.04 ***Guide Development:*** Completion of the following "developmental documentation components" as outlined in Section 007-227-310, *Developmental Documentation Specifications—General Information*, will provide most of the information necessary to develop the System Controls and Examination Guide.

- System Controls Description
- System Reliability Measures Description
- System Performance Monitoring Capabilities.

1.05 ***Preparation:*** The System Controls and Examination Guide should be prepared during the Implementation Phase of system development and delivered during the Conversion Phase. The prepared guide consists of five sections. They are:

- General
- System Controls and Examination Capabilities
- Installation Examinations
- Operational System Examinations
- Glossary.

1.06 ***Revisions:*** The guide must be revised each time changes to the system affect the controls, test packages, or examination capabilities.

1.07 ***Security:*** It is important to note that the System Controls and Examination Guide can be used as a means to defeat the controls. Therefore, the guide should carry the "PRIVATE" designation. Distribution should be limited to the application's System Administrator and those designated by the System Administrator.

2. GUIDE STRUCTURE AND CONTENT

2.01 The following paragraphs (2.xx) describe the contents of each of the five sections required for the System Controls and Examination Guide. Examples are provided where appropriate. Cross-references to other documentation may be used to document the controls. However, if cross-referencing is utilized, the reference must provide a complete narrative explanation of the control.

2.02 ***GENERAL:*** The general section of the System Controls and Examination Guide provides an overview of the content to be presented in

NOTICE
Not for use or disclosure outside the
Bell System except under written agreement

the guide. The following logical sections should be addressed:

- Introduction/Overview
- Available Tools
- References.

2.03 ***Introduction / Overview:*** This section should explain the scope and boundaries of the application system. It also should cover the scope, boundaries, and purpose of the System Controls and Examination Guide. The primary users of the guide should be identified.

2.04 If there are examination capabilities or controls outside the scope of this guide, references to the documentation for these examination capabilities or controls should be given here.

2.05 ***Available Tools:*** This section should describe all of the examination capabilities and controls of an application system. This reference lets the reader know what capabilities are available. For example, one method of description would be the use of an annotated list to be followed by a description of the items in a later section of the guide.

2.06 Examination tools can be developed by creating procedures to use existing query languages, report writers, system utilities, or manual checks. For example, the query languages of OTSS and IMS could become tools with the addition of explanations on how they should be used to examine specific areas. Also, MARK IV or SYNCSORT could be employed similarly on files and utilities, such as IDCAMS or IEHLIST for file structures. These tools will require procedures detailing their use for examination of specific fields, files, or transactions for specific applications.

2.07 ***References:*** This section should describe the expected baseline information, skills, and knowledge the reader should have in order to use the guide effectively. For example, the reader may be expected to be familiar with IMS or have an understanding of telephone switching. In addition, references are made to specific documents the reader should review for prerequisite knowledge of the business processes or system processes.

2.08 Any system documentation, such as local procedures or Bell System Practices (BSPs), that defines system boundaries, requirements, usage, and procedures is also described in this section.

2.09 ***SYSTEM CONTROLS AND EXAMINATION CAPABILITIES:*** This section should describe the ***system controls, test packages,*** and ***examination capabilities*** designed into the particular application. Controls, test packages, and examination capabilities are documented mechanized and/or manual procedures to determine that the application is meeting system objectives and constraints for completeness, accuracy, timeliness, security, protection, and privacy.

2.10 ***System Controls:*** System controls provide users with information concerning what the application is doing, why the application is doing it, when it is being done, and how much is being done. Controls can be mechanized or manual, depending on the specific needs of the application. They are of the following three types:

(a) ***Preventive Controls:*** These controls block events from occurring. Examples are passwords in transaction applications and employee passes in manual security systems, both of which block access from unauthorized personnel.

(b) ***Detective Controls:*** Users are informed of events by these controls. Run activity messages that are returned to users, as well as employee time reporting with supervisory review, are examples of detective controls. They inform users of job activity or provide management with information on time charged.

(c) ***Corrective Controls:*** These controls help management recover from errors. Backup/recovery procedures typify this type of control. Other examples are checkpoint processing during computer runs or retention of paid checks or vouchers.

System controls may be described through the use of diagrams, flowcharts, and/or narratives.

2.11 A flowchart for the application should show system flows and the location of each control. The flowchart, together with a narrative explaining what the control is designed to do, how it works, what control information is provided, and what corrective action management can take for each control message (where possible), will provide the most complete documentation.

2.12 Two examples of system controls are (1) header/trailer count checking and (2) building access reporting. In the first example, this narrative

will explain where the check is done, why the counts are checked, what control messages are provided, and, if possible, what corrective action management should take. The flowchart and narrative for the second example will establish where, when, and how access is controlled (ie, visitor escort procedures, balancing sign-in to sign-out sheets, etc), as well as corrective action to be taken for exceptions, if known. It is important to remember that the documentation of the corrective action is an integral part of the control.

2.13 ***Test Packages:*** Test packages employ known inputs that are processed and then compared to predetermined results. They are used before the system is in production, after problems are encountered, after changes are made, or when a result or process is questionable.

2.14 The verification and/or the regression test packages are perhaps the best known test-package examples. The verification test package will verify that the system was installed correctly through the use of sample inputs that, when processed, will compare correctly with the supplied outputs. In the case of performance tests, sample inputs should produce the sample outputs within specified performance boundaries. Another example, regression test packages allow the testing of changes to determine that changes have not affected other parts of the application.

2.15 Many other types of test packages exist. For each test package a narrative should be prepared explaining what system areas or processes are tested by the package, how to run the test package, and what the specific results should be.

2.16 For larger, more complex applications, references to existing test procedures and documentation may be appropriate. In these instances, sufficient detail should be included to identify where the referenced information resides, how to access it, and the person(s) responsible for it (Test Coordinator Data Base Administrator, Project Manager, etc). Critical areas of the system requiring special test treatment should be identified.

2.17 ***Examination Capabilities:*** Examination capabilities permit the user to identify and scrutinize elements and processes within the system boundaries, allowing verification of the completeness and accuracy of the information system and associated data. In addition, security and privacy are confirmed.

2.18 This section should describe any manual or mechanized examinations which have been built into the system to permit review and inspection of specific system functions. A program designed to report on all deposit refund transactions for a given day or office is an example of a mechanized examination capability. Instructions on how to conduct a manual inventory on a specific stock item and verify the results against a system report is an example of a manual examination.

2.19 Even though certain software or manual procedures were not designed specifically as examination capabilities, they may still serve this purpose. Functions of the system which disclose information on system processing, content of system files, or data bases should be reviewed for potential as examination capabilities. Those with high examination potential should be considered for documentation. Data base management software, query languages, report generators, standard system reports, utilities, manual verifications, manual procedures or instructions on system operations are all examples of facilities of a system which were not developed as examination capabilities but could be used as such. It is important to remember that the instructions and the processor (report generator, query language, manual procedure, etc) could provide the examination capability.

2.20 Since every process or element may not warrant inspection, discretion should be used in the selection of examination subjects. If an element or process should be examined, a narrative should be prepared. This narrative will explain why the examination is being done. how to perform the examination, and the results expected (where predictable) of the examination.

2.21 The management trail capabilities of the system should also be described here. These are control procedures that provide the ability to trace original transactions forward to related records and reports, as well as the ability to trace records and reports back to their component source transactions. A typical management trail may consist of a copy of the original transactions, lists of records which were accepted or rejected, reports on changes or modifications to the data, run-to-run control totals, and a copy of the output using this data. With these items a transaction could be traced or reconstructed.

2.22 ***INSTALLATION EXAMINATIONS:*** This section should describe those procedures (test packages and examination capabilities) that should be performed as a part of the system installation process. These procedures include the installation of the application and the conversion (if any) of data required. Additionally, cross-references to the Operational System Examinations section should be made for those operational examinations that would be performed during installation. These operational examinations ensure, at a minimum, that the system controls have been correctly installed.

2.23 Each examination should be explained in a narrative. This narrative will explain why the examination is done (purpose), at what point during the installation process the examination is performed, the process or element being examined, instructions on how to perform the examination, and any expected results (where predictable). It is entirely possible that an examination can be performed during installation and also on an ongoing basis. For example, the system performance may be examined and compared to the requirements during acceptance testing at installation, as well as on a recurring basis, to ensure that the application performance remains acceptable.

2.24 There are many possible areas that could be the subject of an installation examination; for example, completeness, accuracy, security, integrity, etc. The documented examinations should be those that are most important to the proper processing of the application, providing the greatest potential benefit. Usually examinations are performed on those areas which are the most volatile or critical to the application and those areas from which error recovery would be difficult or expensive.

2.25 ***OPERATIONAL SYSTEM EXAMINATIONS:*** This section should describe those procedures (test packages and examination capabilities) that should be performed on the operating application to determine:

- That the system controls are operating correctly
- That the system is meeting its objectives
- That the information in the system is complete, accurate, up-to-date, protected, private, and secure.

2.26 The term "operating application" encompasses the computer system, manual procedures, and interfaces to all other computer systems, as well as manual procedures required to result in satisfaction of the operational objectives for the business function.

2.27 Each examination should be explained in a narrative. It should describe the purpose or objective of the examination, when it should be performed, what the target (element or process) is, how to perform the examination, and what results are to be expected. If the expected results are not realized, instructions for the notification of appropriate person (System Administrator, Maintenance Control Center, Project Manager, etc) should be detailed in the narrative and cross-referenced to other documents, if possible. If the procedure for reexamination after problem resolution differs from the original examination procedure, the reexamination procedure should also be documented in the narrative. It is expected that these examinations will be performed on a recurring basis.

2.28 Any area of an application can be a target for an operational examination. The documented operational examinations should address those areas of the system that are most critical to the proper processing of the application. The management trail capabilities of the application should be examined. At a minimum, examinations should be performed for applications with any of the following characteristics:

- They offer opportunities for personal gain.
- They have a direct effect on the company accounts.
- They produce work measurements from actions which can be examined for accuracy.
- They are personnel records.

2.29 Some examples of applications with these characteristics are any which access employee information, report or create service indicators which could be a component of performance results, or deal with expense authorization, revenue collection, or funds distribution. In addition, other factors have a bearing when selecting areas for examination. These include:

(a) The value of the examination compared to the cost of performing it. If the possible benefit is

not greater than the cost, the examination should not be considered unless there were other considerations such as regulatory requirements.

(b) The complexity of the examination. If the examination is complex, it should be broken into smaller, simpler parts. This is similar to functional decomposition during system analysis. If this approach is taken, care must be exercised to ensure that the examination of the components results in an examination of the whole; this is similar to the way that integration testing ensures that the component parts of an application act together to reach the desired objective.

(c) The effect on company operations of a system failure. If the failure of an application component would have a great impact on the company operations or customers, this component should be considered for examination.

(d) Known potential problem areas. If an area of the system is particularly volatile, it should be considered for examination. Examples of problem areas might include duplicate payments, inventory tracking, or overtime tracking.

2.30 ***GLOSSARY:*** This section should consist of an alphabetical annotated list of project terms and acronyms. Every acronym and unfamiliar term should be listed with an explanation so that the reader can understand the application. This section can be thought of as the application dictionary.

3. REFERENCES

3.01 The following documents were used as references in the preparation of this guide. These documents contain supplemental information that is of additional benefit in detailing specific areas and components for the System Controls and Examination Guide.

SECTION	TITLE
007-227-310	Developmental Documentation Specifications—General Information
007-209-302	System Control Guidelines*
007-209-201	System Control Standards
007-230-210	System Deliverable Documentation

* Check Divisional Index 007 for availability.