Conducting an Internal Audit for Electronic Records Compliance: *A Primer*

The internal audit for electronic records compliance is a management tool designed to measure compliance with the standards, policies, and procedures designed to promote compliance with 21 CFR Part 11.

by
Leonard A. Grunbaum
President
META Solutions, Inc.

This article is written to provide guidance for the internal auditor who is, or is thinking about, performing an audit for electronic records compliance. It is written as a primer – a place to start – that the internal auditor can build upon based upon the level of his or her experience. The internal audit for electronic records compliance is a management tool designed to measure compliance with the standards, policies, and procedures designed to promote compliance with 21 CFR Part 11.[1] This regulation provides the requirement to control the creation, modification, maintenance, archiving, and distribution of electronic records and is fast becoming a priority for Industry and the FDA. Company management is consequently devoting an increasing amount of resources – time and money – to achieve compliance. The audit will allow management to (1) determine if the organization is adhering to the standards, policies, and procedures established to promote compliance with the 21 CFR Part 11 and (2) identify the deficiencies that exist vis-à-vis compliance with 21 CFR Part 11.

The Audit Strategy

So where do you start? The answer is: develop an audit strategy; that is, define what you will audit and why. Logically, the basis for your audit strategy should be the document titled *Guidance for Industry: Computerized Systems Used in Clinical Trials*,[2] located on page 17 of this Journal. This document addresses the requirements of 21 CFR Part 11 and its principles are applicable to clinical sites, contract research organizations, data management centers, and sponsors where computerized systems are employed. If the internal audit is designed to map to the provisions of the guidance document at a minimum, the risk that significant issues will be overlooked is small and you can always make the audit more robust.

Audit Conduct

Figure 1 provides the relationship of the provisions of the guidance document to specific audit steps to perform and the impact of any deficiencies noted. The information provided is as follows:

- Guidance document provision: These are the specific

regulatory requirements and/or expectations taken directly from the guidance document.

- Suggested audit steps: There are specific activities to perform (e.g., documents to review, items to look for in the documentation, types of reviews to conduct) to determine if the given requirement/expectation per the guidance document is being met.
- Impact of deficiency (to be included in audit comment): This column provides suggested language to include in the audit comment section of the internal audit report regarding the significance of audit deficiencies (i.e., the regulatory requirements/expectations not met).

Figure 1

Relationship of Guidance Document Provisions to Internal Audit Strategy

Guidance Document Provisions	Suggested Audit Steps	Impact of Deficiency (To Be Included in Audit Comment)
I. INTRODUCTION		
II. DEFINITIONS		
III. GENERAL PRINCIPLES		
IV. STANDARD OPERATING PROCEDURES		
Standard Operating Procedures (SOPs) pertinent to the use of the computerized system should be available on site. SOPs should be established for, but not limited to: ■ *System Setup/Installation* ■ *Data Collection and Handling* ■ *System Maintenance* ■ *Data Backup, Recovery, and Contingency Plans* ■ *Security* ■ *Change Control*	1. Request copy of all formal, approved SOPs. Note that the specific SOP titles may differ from the categories included in the guidance. 2. Determine that the approved SOPs address the issues identified in the guidance document and that they provide a means to confirm compliance. 3. Review applicable compliance procedures to confirm that the approved SOPs are being complied with and that documented evidence exists to confirm compliance. 4. Perform a documentation review to confirm that the documents are available on-site (i.e., wherever the respective processes are being performed).	SOPs provide the methods that management relies upon to help ensure the integrity of the electronic data and the processes that produce and maintain the data. Lack of SOPs, or the lack of SOPs on-site, means that the applicable staff will not have approved procedures to follow to maintain control of the applicable computer systems and electronic data. Lack of documented evidence of compliance increases the risk that controls are weak or non-existent.
V. DATA ENTRY		
A. Electronic Signatures		
1. To ensure that individuals have the authority to proceed with data entry, the data entry system should be designed so that individuals need to enter electronic signatures, such as combined identification codes/passwords or biometric-based electronic signatures, at the start of a data entry session.	1. Review the approved functional specifications to determine if the following requirement is included: electronic signatures must be entered at the start of a data entry session. 2. Review the approved technical specifications to determine if the following requirement is designed and programmed properly: electronic signatures must be entered at the start of a data entry session. 3. Review the test cases and scripts and documented test results to confirm that the following requirement functions properly: electronic signatures must be entered at the start of a data entry session.	An electronic signature is a means to help ensure that only authorized data entry takes place. Unauthorized data entry is a limitation on the integrity of study data.
2. The data entry system should ... be designed to ensure attributability... [E]ach entry to an electronic record, including any change, should be made under the electronic signature of the individual making that entry. *a. The printed name of the individual who enters data should be displayed by the data entry screen throughout the data entry session.*	1. Review the approved functional specifications to determine if the following requirements are included: (a) each entry to an electronic record is made under the electronic signature of the individual making that entry; (b) the printed name of the individual who enters data is displayed by the data entry screen throughout the data entry session. 2. Review the approved technical specifications to determine if the following requirements are designed and programmed properly: (a) each entry to an electronic record is made under the electronic signature of the individual making that entry; (b) the printed name of the individual who enters data is displayed by the data entry screen throughout the data entry session. 3. Review the test cases and scripts and documented test results to confirm that the following requirements function properly: (a) each entry to an electronic record is made under the electronic signature of the individual making that entry; (b) the printed name of the individual who enters data is displayed by the data entry screen throughout the data entry session.	Entry of data by one individual under someone else's name is unauthorized data entry, which is a limitation on the integrity of study data.

Figure 1
Continued

Guidance Document Provisions	Suggested Audit Steps	Impact of Deficiency (To Be Included in Audit Comment)
3. Individuals should only work under their own passwords or other access keys and should not share these with others. Individuals should not log on to the system in order to provide another person access to the system.	1. Determine that an approved SOP or other formal policy/procedure exists to preclude the sharing of passwords and logging on to the system to allow someone else to access the system. 2. Confirm compliance with the control by reviewing documented evidence of compliance.	The risk of unauthorized access to the electronic data and to the computerized system is increased when there is a lack of an effective control (including documented evidence of compliance) to preclude sharing of passwords and logging on to the system to allow someone else to access the system.
4. Passwords or other access keys should be changed at established intervals.	1. Determine that an approved SOP or other formal policy/procedure exists that facilitates changing of passwords or other keys at established intervals. 2. Confirm compliance with the control by reviewing documented evidence of compliance.	The risk of unauthorized access to the electronic data and to the computerized system is increased when there is a lack of an effective control (including documented evidence of compliance) to facilitate changing of passwords or other keys at established intervals.
5. When someone leaves a workstation, the person should log off the system. Failing this, an automatic log off may be appropriate for long idle periods. For short periods of inactivity, there should be some kind of automatic protection against unauthorized data entry.	1. Determine that an approved SOP or other formal policy/procedure exists that facilitates automatic log off after a pre-determined period of time. 2. Confirm compliance with the control by reviewing documented evidence of compliance.	The risk of unauthorized access to the electronic data and to the computerized system is increased when there is a lack of an effective control (including documented evidence of compliance) to facilitate automatic log off after a pre-determined period of time.
B. Audit Trails		
1a. Persons must use secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. A record is created when it is saved to durable media, as described under "commit" in Section II, Definitions.	1. Review the approved functional specifications to determine if the following requirement is included: a secure, computer-generated, time-stamped audit trail is independently generated to record the date and time of operator entries and actions that create, modify, or delete electronic records. 2. Review the approved technical specifications to determine if the following requirement is designed and programmed properly: a secure, computer-generated, time-stamped audit trail is independently generated to record the date and time of operator entries and actions that create, modify, or delete electronic records. 3. Review the test cases and scripts and document test results to confirm that a secure, computer-generated, time-stamped audit trail is independently generated to record the date and time of operator entries and actions that create, modify, or delete electronic records.	The lack of an effective audit trail limits the study sponsor's ability to (1) protect the authenticity, integrity, and, when appropriate, the confidentiality of electronic records and (2) reconstruct and evaluate study records.
1b. Audit trails must be retained for a period at least as long as that required for the subject electronic records ... and must be available for Agency review and copying.	1. Determine that an approved SOP or other formal record retention policy exists that mandates the retention of audit trails for a period at least as long as that required for the subject electronic records. 2. Confirm compliance with the SOP or other record retention policy by reviewing documented evidence of compliance. 3. Observe the audit trails (either hard copy or electronic) and confirm the existence and effectiveness of procedures designed to copy the audit trails.	As above.
2. Personnel who create, modify, or delete electronic records should not be able to modify the audit trails.	1. Review the security/authorization profiles to confirm that personnel who create, modify, or delete electronic records do not have written access to the audit trails. 2. Review the test cases and scripts and documented test results to confirm that testing verifies that personnel who create, modify, or delete electronic records cannot modify the audit trails.	Unauthorized access to audit trail records increases the risk that the audit trail data will be corrupted and therefore not usable to (1) protect the authenticity, integrity, and, when appropriate, the confidentiality of electronic records and (2) reconstruct and evaluate study records.

Figure 1
Continued

Guidance Document Provisions	Suggested Audit Steps	Impact of Deficiency (To Be Included in Audit Comment)
3. Clinical investigators should retain either the original or a certified copy of audit trails.	Perform a documentation review of the clinical investigators to confirm that they are in possession of either the original or a certified copy of audit trails. In the case of changes to the system, this also includes copies of source code and change control documentation, so the scope would also include developer and support personnel.	The original audit trails (or a certified copy) provide the documented evidence of study conduct. The lack of such documentation, and the ability to review the documentation, increases the risk that improper, incomplete, and/or inaccurate processing will go undetected.
4. FDA personnel should be able to read audit trails both at the study site and at any other location where associated electronic study records are maintained.	Observe the audit trails and all associated electronic study records (e.g., Case Record Forms (CRFs)), source code, change control documentation), in all locations where they are maintained, and confirm the existence and effectiveness of procedures designed to copy the audit trails.	The original audit trails (or a certified copy) provide the documented evidence of study conduct. The lack of such documentation, and the ability to review the documentation, increases the risk that improper, incomplete, and/or inaccurate processing will go undetected.
5. Audit trails should be created incrementally, in chronological order, and in a manner that does not allow new audit trail information to overwrite existing data in violation of §11.10(e).	1. Review the approved functional specifications to determine if the following requirement is included: audit trails should be created incrementally, in chronological order, and in a manner that does not allow new audit trail information to overwrite existing data. 2. Review the approved technical specifications to determine if the following requirement is designed and programmed properly: audit trails are created incrementally, in chronological order, and in a manner that does not allow new audit trail information to overwrite existing data. 3. Review the test cases and scripts and documented test results to confirm that audit trails are created incrementally, in chronological order, and in a manner that does not allow new audit trail information to overwrite existing data.	The lack of a complete audit trail increases the risk that improper, incomplete, and/or inaccurate processing will go undetected.
C. Date/Time Stamps		
The ability to change the date or time should be limited to authorized personnel and such personnel should be notified if a system date or time discrepancy is detected. Changes to date or time should be documented.	1. Review the security/authorization profiles to confirm that authorization to change the date or time is limited to system administration or other appropriate personnel. 2. Review the test cases and scripts and documented test results to confirm that testing confirms that only the authorized personnel can change the date or time. 3. Determine that an approved SOP or other formal policy/procedure(s) exists that facilitates (1) notification to the appropriate staff if a system date or time discrepancy is found and (2) that changes in date or time are documented. 4. Confirm compliance with the SOP or other record retention policies by reviewing documented evidence of compliance.	The lack of an effective control to ensure that the system's date and time are correct increases the risk that improper, incomplete and/or inaccurate processing will take place.
Dates and times are to be local to the activity being documented and should include the year, month, day, hour, and minute.	1. Review the approved functional specifications to determine if the following requirement is included: dates and times are to be local to the activity being documented and should include the year, month, day, hour, and minute. 2. Review the approved technical specifications to determine if the following requirement is designed and programmed properly: dates and times are local to the activity being documented and should include the year, month, day, hour, and minute. 3. Review the test cases and scripts and documented test results to confirm that dates and times are local to the activity being documented and should include the year, month, day, hour, and minute.	As above.

Figure 1
Continued

Guidance Document Provisions	Suggested Audit Steps	Impact of Deficiency (To Be Included in Audit Comment)
VI. SYSTEM FEATURES		
A. Facilitating the Collection of Quality Data		
Prompts, flags, or other help features within the computerized system should be used to encourage consistent use of clinical terminology and to alert the user to data that are out of acceptable range. Features that automatically enter data into a field when that field is bypassed should not be used.	1. Review the approved functional specifications to determine if the following requirements are included: (1) consistent use of clinical terminology; (2) alerts to the user regarding data that are out of acceptable range; (3) features that automatically enter data into a field when that field is bypassed and cannot be used. 2. Review the approved technical specifications to determine if the following requirement is designed and programmed properly: (1) consistent use of clinical terminology; (2) alerts to the user regarding data that are out of acceptable range; (3) features that automatically enter data into a field when that field is bypassed are not used. 3. Review the test cases and scripts and documented test results to confirm that (1) consistent use of clinical terminology is employed; (2) users are alerted when data are out of acceptable range; (3) features that automatically enter data into a field when that field is bypassed are not used.	The lack of an effective control to facilitate the collection of quality data increases the risk that improper, incomplete, inconsistent and/or inaccurate data will be collected. This, in turn, can increase the risk to the integrity of the data and decrease the efficiency of the study processing.
Electronic patient diaries and e-CRFs should be designed to allow users to make annotations... The record should clearly indicate who recorded the annotations and when (date and time).	1. If electronic diaries or e-CRFs are used, review the approved functional specifications to determine if the following requirements are included: (1) annotations are permitted; (2) the study record should clearly indicate who recorded the annotations and when (date and time). 2. Review the approved technical specifications to determine if the following requirement is designed and programmed properly: (1) annotations are permitted; (2) the study record clearly indicates who recorded the annotations and when (date and time). 3. Review the test cases and scripts and documented test results to confirm that (1) annotations are permitted; (2) the study record clearly indicates who recorded the annotations and when (date and time).	Annotations represent study data. The lack of an effective means to facilitate the collection of quality data increases the risk that improper, incomplete, and/or inaccurate data will be collected. This, in turn, can increase the risk to the integrity of the data.
B. Facilitating the Inspection and Review of Data		
Systems used for direct entry of data should be designed to include features that will facilitate the inspection and review of data. Data tags (e.g., different color, different font, flags) should be used to indicate which data have been changed or deleted, as documented in the audit trail.	1. If direct data entry is applicable, review the approved functional specifications to determine if the following requirement is included: features (e.g., data tags) to facilitate inspection and review. 2. Review the approved technical specifications to determine if the following requirement is designed and programmed properly: features (e.g., data tags) to facilitate inspection and review. 3. Review the test cases and scripts and documented test results to confirm that features (e.g., data tags) to facilitate inspection and review are operational.	The lack of an effective means to facilitate the collection of quality data increases the risk that improper, incomplete, inconsistent and/or inaccurate data will be collected. This, in turn, can increase the risk to the integrity of the data and decrease the efficiency of the study processing.
C. Retrieval of Data		
Recognizing that computer products may be discontinued or supplanted by newer (possibly incompatible) systems, it is nonetheless vital that sponsors retain the ability to retrieve and review the data recorded by the older systems. This may be achieved by maintaining support for the older systems or transcribing data to the newer systems.	1. Determine that an approved SOP or other formal policy/procedure exists that addresses maintenance/support of older systems and/or the transcribing of data to the newer systems. 2. Confirm compliance with the SOP or other policy by reviewing the older system documentation or the evidence of transcription. 3. Observe the audit trails (either hard copy or electronic) and confirm the existence and effectiveness of procedures designed to copy the audit trails. 4. For systems that are being, or will be, migrated,	FDA expects to be able to reconstruct a study, and expects that study sponsors be able to do so as well. This applies not only to the data, but also how the data were obtained or managed. The lack of complete information regarding versions of application software, operating systems, and software development tools, as well as applicable hardware, involved in the process-

Figure 1
Continued

Guidance Document Provisions	Suggested Audit Steps	Impact of Deficiency (To Be Included in Audit Comment)
When migrating to newer systems, it is important to generate accurate and complete copies of study data and collateral information relevant to data integrity. This information would include, for example, audit trails and computational methods used to derive the data. Any data retrieval software, script, or query logic used for the purpose of manipulating, querying, or extracting data for report generating purposes should be documented and maintained for the life of the report. The transcription process needs to be validated.	determine that a migration plan exists and that it addresses the following: generating accurate and complete copies of study data and collateral information relevant to data integrity; documenting and maintaining data retrieval software, script, or query logic used for the purpose of manipulating, querying, or extracting data for report generating purposes; validating the transcription process. 5. For systems that have been migrated, determine that the following objectives have been achieved: documented evidence exists to confirm that accurate and complete copies of study data and collateral information relevant to data integrity have been generated; data retrieval software, script, or query logic used for the purpose of manipulating, querying, or extracting data for report generating purposes is documented and is being maintained according to an approved SOP or other formal policy/procedure; the transcription process has been validated.	ing of data or records limits the Agency's ability to reconstruct and evaluate study records.
D. Reconstruction of Study		
...[A]ll versions of application software, operating systems, and software development tools involved in processing of data or records should be available as long as data or records associated with these versions are required to be retained.	1. Determine that an approved SOP or other formal policy/procedure exists that mandates the retention of all versions of application software, operating systems, and software development tools involved in processing of data or records for as long as data or records associated with these versions are required to be retained. 2. Confirm compliance with the SOP or other record retention policy by reviewing documented evidence of compliance.	FDA expects to be able to reconstruct a study. This applies not only to the data, but also how the data were obtained or managed. The lack of complete information regarding versions of application software, operating systems, and software development tools involved in processing data or records limits the Agency's ability to reconstruct and evaluate study records.
VII. SECURITY		
A. Physical Security		
Staff should be thoroughly aware of system security measures and the importance of limiting access to authorized personnel. *SOPs should be in place for handling and storing the system to prevent unauthorized access.*	1. Determine that approved SOPs or other formal policies/procedures exist that mandate (1) training for personnel who use the system and maintain/support the system on the applicable security policies and procedures and (2) for handling and storing the system to prevent unauthorized access. 2. Confirm compliance with the approved SOPs or other formal policies/procedures by reviewing documented evidence of compliance. With respect to training, this would include an inspection of the training records and evidence of staff understanding of the information learned (e.g., test results).	In addition to internal safeguards built into the system, external safeguards should be in place to ensure that access to the computerized system and to the data is restricted to authorized personnel. The lack of such safeguards increases the risk of unauthorized/improper processing. This is a limitation on data integrity.
B. Logical Security		
Access to the data at the clinical site should be restricted and monitored through the system's software with its required log-on, security procedures, and audit trail. The data should not be altered, browsed, queried, or reported via external software applications that do not enter through the protective system software.	1. Review the approved functional specifications to determine if the following requirements are included: (1) access to the data at the clinical site (e.g., investigator site, sponsor database) should be restricted and monitored through the system's software with its required log-on, security procedures, and audit trail; (2) the data should not be altered, browsed, queried, or reported via external software applications that do not enter through the protective system software. 2. Review the approved technical specifications to determine if the following requirements are designed and programmed properly: (1) access to the data at the clinical site (e.g., investigator site, sponsor database) is restricted and monitored through the system's software with its required	The risk of unauthorized access to the electronic data and to the computerized system is increased when there is a lack of effective logical security control (including documented evidence of compliance).

Figure 1

Continued

Guidance Document Provisions	Suggested Audit Steps	Impact of Deficiency (To Be Included in Audit Comment)
	log-on, security procedures, and audit trail; (2) the data is not to be altered, browsed, queried, or reported via external software applications that do not enter through the protective system software. 3. Review the test cases and scripts and documented test results to confirm: (1) access to the data at the clinical site (e.g., investigator site, sponsor database) is restricted and monitored through the system's software with its required log-on, security procedures, and audit trail; (2) the data cannot be altered, browsed, queried, or reported via external software applications that do not enter through the protective system software.	
There should be a cumulative record that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. The record should be in the study documentation accessible at the site.	1. Review the approved functional specifications to determine if the following requirements are included: a cumulative record should exist that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. 2. Review the approved technical specifications to determine if the following requirement is designed and programmed properly: a cumulative record is generated that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. 3. Review the test cases and scripts and documented test results to confirm: a cumulative record exists that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. 4. Perform a documentation review to confirm that the authorization records is available in the study documentation.	A cumulative record that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges is an audit trail of authorization privileges. The lack of a complete audit trail increases the risk that improper, incomplete, and/or inaccurate processing will go undetected.
If a sponsor supplies computerized systems exclusively for clinical trials, the systems should remain dedicated to the purpose for which they were intended and validated.	1. Determine that approved SOPs or other formal policies/procedures exist that mandate a periodic review to ensure that the systems remain dedicated to the purpose for which they were intended and validated. 2. Confirm compliance with the approved SOPs or other formal policies/procedures by reviewing documented evidence of compliance. If undocumented/unvalidated changes to the system are identified, determine if documented justification exists for not documenting/validating the changes.	If the system is not completely dedicated to the purpose for which it was intended and validated, the ability to collect quality data is jeopardized. The lack of an effective means to facilitate the collection of quality data increases the risk that improper, incomplete, inconsistent, and/or inaccurate data will be collected. This, in turn, can increase the risk to the integrity of the data and decrease the efficiency of the study processing.
If a computerized system being used for the clinical study is part of a system normally used for other purposes, efforts should be made to ensure that the study software is logically and physically isolated as necessary to preclude unintended interaction with non-study software. If any of the software programs are changed the system should be evaluated to determine the effect of the changes on logical security.	1. Review the approved technical specifications to determine if the system is part of a system normally used for other purposes and, if so, the specification includes details of how the study software is logically and physically isolated as necessary to preclude unintended interaction with non-study software. 2. Review the test cases and scripts and documented test results to confirm that study software is logically and physically isolated from non-study software. 3. Determine that approved SOPs or other formal policies/procedures exist that mandate that changes to software programs are evaluated to determine the effect of the changes on logical security. 4. Confirm compliance with the approved SOPs or other formal policies/procedures by reviewing documented evidence of compliance.	As above.
Controls should be in place to prevent, detect, and mitigate effects of computer viruses on study data and software.	1. Determine that approved SOPs or other formal policies/procedures exist that mandate precautions against computer viruses and training for	A computer virus represents an attempt to access records in an unauthorized manner. Unauthorized access to study records increases

Figure 1
Continued

Guidance Document Provisions	Suggested Audit Steps	Impact of Deficiency (To Be Included in Audit Comment)
	staff in these precautions. 2. Confirm compliance with the approved SOPs or other formal policies/procedures by reviewing documented evidence of compliance. With respect to training, this would include an inspection of the training records and evidence of staff understanding of the information learned (e.g., test results). 3. Determine that an appropriate anti-virus software package is employed to detect viruses and confirm that procedures are in place to confirm its effectiveness.	the risk that such records will be corrupted and therefore not usable to (1) protect the authenticity, integrity, and, when appropriate, the confidentiality of electronic records and (2) reconstruct and evaluate study records.
VIII. SYSTEM DEPENDABILITY		
The sponsor should ensure and document that computerized systems conform to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance.	Perform a documentation review at each applicable site at which the system is developed, operated and/or supported to determine the existence of current approved functional specifications, approved technical specifications, operations manuals, pertinent approved SOPs and other procedures, and applicable reference documentation.	Systems documentation provides information that describes what the software is intended to do and how it is intended to do it. The lack of such documentation limits management's ability to effectively manage the study and the Agency's ability to reconstruct and evaluate study records.
A. Systems Documentation		
Systems documentation should be readily available at the site where clinical trials are conducted. Such documentation should provide an overall description of computerized systems and the relationship of hardware, software, and physical environment.		
B. Software Validation		
FDA may inspect documentation, possessed by a regulated company, that demonstrates validation of software.	1. Determine that approved SOPs or other formal policies/procedures exist that provide the requirements for system validation, as defined in the guidance document, and the requirement to ensure that the documentation can be inspected by FDA. 2. Confirm compliance with the approved SOPs or other formal policies/procedures by reviewing documented evidence of compliance. This would involve reviewing the validation documentation for each applicable system to ensure that all validation deliverables are provided in the validation file.	Validation documentation represents documented evidence that the system operates as intended and will continue to do so. The lack of such documentation, or the lack of FDA's ability to review such documentation, limits the Agency's ability to reconstruct and evaluate study records.
1. For software purchased off-the-shelf, most of the validation should have been done by the company that wrote the software. The sponsor or contract research organization should have documentation (either original validation documents or on-site vendor audit documents) of this design-level validation by the vendor, and should have itself performed functional testing (e.g., by use of test data sets) and researched known software limitations, problems, and defect corrections.	1. Determine that approved SOPs or other formal policies/procedures exist that mandates: (1) the performance of a vendor audit when necessary to assess the effectiveness of the design level validation by the vendor; (2) the performance of an adequate level of functional testing based upon the effectiveness of the vendor's validation status; (3) researching known software limitations, problems, and defect corrections. 2. Confirm compliance with the approved SOPs or other formal policies/procedures by reviewing documented evidence of compliance. This would include a formal audit report documenting the results of the vendor audit.	The sponsor's ability to ensure and document that computerized systems conform to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance will be limited without a vendor audit, adequate functional testing, knowledge of software limitations, problems, and defect corrections.
In the special case of database and spreadsheet software that is (1) purchased off-the-shelf, (2) designed for and widely used for general purposes, (3) unmodified, and (4) not being used for direct entry of data, the sponsor or contract research organization may not have documentation of design level validation. However, the sponsor or contract research organization should have itself performed functional testing (e.g., by use of test data sets) and researched known software limitations, problems, and defect corrections.	1. Determine that approved SOPs or other formal policies/procedures exist that mandates, in the case where design level validation is unavailable, performing an adequate level of functional testing based upon the effectiveness of the vendor's validation status and researching known software limitations, problems, and defect corrections. 2. Confirm compliance with the approved SOPs or other formal policies/procedures by reviewing documented evidence of compliance.	The sponsor's ability to ensure and document that computerized systems conform to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance will be limited without adequate functional testing and knowledge of software limitations, problems, and defect corrections.

Figure 1
Continued

Guidance Document Provisions	Suggested Audit Steps	Impact of Deficiency (To Be Included in Audit Comment)
2. Documentation important to demonstrate software validation includes: *Written design specification that describes what the software is intended to do and how it is intended to do it;* *A written test plan based on the design specification, including both structural and functional analysis; and* *Test results and an evaluation of how these results demonstrate that the predetermined design specification has been met.*	1. Determine that approved SOPs or other formal policies/procedures exist that provide the requirements for system validation, as defined in this section of the guidance document, and the requirement to ensure that the documentation can be inspected by FDA. 2. Confirm compliance with the approved SOPs or other formal policies/procedures by reviewing documented evidence of compliance. This would involve reviewing the validation documentation for each applicable system to ensure that all validation deliverables are provided in the validation file.	Validation documentation represents documented evidence that the system operates as intended and will continue to do so. The lack of such documentation, or the lack of FDA's ability to review such documentation, limits the Agency's ability to reconstruct and evaluate study records.
C. Change Control		
Written procedures should be in place to ensure that changes to the computerized system such as software upgrades, equipment or component replacement, or new instrumentation will maintain the integrity of the data or the integrity of protocols. *The impact of any change to the system should be evaluated and a decision made regarding the need to revalidate. Revalidation should be performed for changes that exceed operational limits or design specifications.* *All changes to the system should be documented.*	1. Determine that approved SOPs or other formal policies/procedures exist that provide a formal change control procedure designed to ensure that changes to the computerized system such as software upgrades, equipment, component replacement, or new instrumentation will maintain the integrity of the data or the integrity of protocols. The SOPs or other procedures should include an evaluation of the impact of changes to determine if revalidation is required. 2. Confirm compliance with the approved SOPs or other formal policies/procedures by reviewing documented evidence of compliance. If undocumented/unvalidated changes to the system are identified, determine if documented justification exists for not documenting/validating the changes.	Change control procedures represent an audit trail of changes to the automated processes. The lack of a complete audit trail, including changes to associated documentation, increases the risk that improper, incomplete, and/or inaccurate processing will go undetected.
IX. SYSTEM CONTROLS		
A. Software Version Control		
Measures should be in place to ensure that versions of software used to generate, collect, maintain, and transmit data are the versions that are stated in the systems documentation.	1. Determine that approved SOPs or other formal policies/procedures exist that provide configuration control requirements; that is, controls to ensure that all elements of the system configuration (e.g., hardware, software, documentation) remain consistent throughout the life of the system. 2. Confirm compliance with the approved SOPs or other formal policies/procedures by reviewing documented evidence of compliance.	Change control procedures represent an audit trail of changes to the automated processes. Version control represents an identification of the different components resulting from the change. The lack of a complete audit trail, including controls over identifying the various versions, increases the risk that improper, incomplete, and/or inaccurate processing will go undetected.
B. Contingency Plans		
Written procedures should describe contingency plans for continuing the study by alternate means in the event of failure of the computerized system.	1. Determine that an approved contingency plan (a.k.a., disaster recovery plan) exists that describes plans for continuing the study by alternate means in the event of failure of the computerized system or inability to access the system or facility. 2. Confirm that the disaster recovery plan was completely tested and that the test results are documented.	The lack of a contingency plan increases the risk of not being able to collect data in the event of failure of the computerized system or inability to access the system or facility. The lack of an effective means to facilitate the collection of quality data increases the risk that improper, incomplete, inconsistent and/or inaccurate data will be collected. This, in turn, can increase the risk to the integrity of the data and decrease the efficiency of the study processing.
C. Backup and Recovery of Electronic Records		
Backup and recovery procedures should be clearly outlined in the SOPs and be sufficient to protect against data loss.	1. Determine that approved SOPs or other formal policies/procedures exist that mandate periodic backup of programs and files, storage of backup programs and files in a secure location, and applicable recovery procedures (including the mainte-	Records should be backed up regularly in a way that would prevent a catastrophic loss and ensure the quality and integrity of the data.

Figure 1
Continued

Guidance Document Provisions	Suggested Audit Steps	Impact of Deficiency (To Be Included in Audit Comment)
Backup records should be stored at a secure location specified in the SOPs. *Backup and recovery logs should be maintained to facilitate an assessment of the nature and scope of data loss resulting from a system failure.*	nance of recovery logs). 2. Confirm compliance with the approved SOPs or other formal policies/procedures by reviewing documented evidence of compliance. This would include an audit of the backup site to confirm the completeness and accuracy of the inventory therein.	
X. TRAINING OF PERSONNEL		
A. Qualifications		
Each person who enters or processes data should have the education, training, and experience or any combination thereof necessary to perform the assigned functions. *Individuals responsible for monitoring the trial should have education, training, and experience in the use of the computerized system necessary to adequately monitor the trial.*	1. Determine that approved SOPs or other formal policies/procedures exist that mandate that each person who enters or processes data, persons who monitors the trial, and persons who conduct the training, should have the education, training, and experience or any combination thereof necessary to perform the assigned functions. 2. Confirm compliance with the approved SOPs or other formal policies/procedures by reviewing documented evidence of compliance. With respect to training, this would include an inspection of the training records and evidence of staff understanding of the information learned (e.g., test results).	Lack of education, training, and experience to perform study-related activities, and documented evidence thereof, increases the risk that improper, incomplete, inconsistent and/or inaccurate data will be collected. This, in turn, can increase the risk of the integrity of the data and decrease the efficiency of the study processing.
B. Training		
Training should be provided to individuals in the specific operations that they are to perform. *Training should be conducted by qualified individuals on a continuing basis, as needed, to ensure familiarity with the computerized system and with any changes to the system during the course of the study.*	As above.	As above.
C. Documentation		
Employee education, training, and experience should be documented.	1. Determine that records of education, training, and experience exist. 2. Perform a review of these records and confirm that they are current.	As above.
XI. RECORDS INSPECTION		
A. ...[S]ystems should be able to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the Agency.	1. Determine that approved SOPs or other formal policies/procedures exist that mandate that systems should be able to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying. 2. Confirm compliance with the approved SOPs or other formal policies/procedures by reviewing documented evidence of compliance. For a given system, this would include testing and documented test results to confirm this functionality.	FDA may inspect all records that are intended to support submissions to the Agency, regardless of how they were created or maintained. The lack of appropriate documentation, lack of FDA's ability to review such documentation, and/or lack of applicable hardware and software to perform required processes limits the Agency's ability to reconstruct and evaluate study records.
B. The sponsor should be able to provide hardware and software as necessary for FDA personnel to inspect the electronic documents and audit trail at the site where an FDA inspection is taking place.	Perform a documentation review at the applicable site(s) to determine the existence of the hardware and software specified in the approved technical specification.	FDA may inspect all records that are intended to support submissions to the Agency, regardless of how they were created or maintained. The lack of appropriate documentation, lack of FDA's ability to review such documentation, and/or lack of applicable hardware and software to perform required processes limits the Agency's ability to reconstruct and evaluate study records.

Figure 1
Continued

Guidance Document Provisions	Suggested Audit Steps	Impact of Deficiency (To Be Included in Audit Comment)
XII. CERTIFICATION OF ELECTRONIC SIGNATURES		
As required by 21 CFR 11.100(c), persons using electronic signatures to meet an FDA signature requirement shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	If electronic signatures are being used to meet an FDA signature requirement, determine that the certification was filed as specified in 21 CFR Part 11.	This certification is a legal document created by persons to acknowledge that their electronic signatures have the same legal significance as their traditional handwritten signatures. The lack of such certification means that the electronic signatures will not be the legally binding equivalent of traditional handwritten signatures.

Audit Checklist

The internal auditor should develop an audit checklist using the contents of *Figure 1* to facilitate collecting and evaluating information. While the author suggests organizing the checklist to correspond to the guidance document provisions, the internal auditor can use whatever organization makes the most sense. The key issue is to ensure that all guidance document provisions are addressed.

Summary

This is the place to start if you are, or are thinking about, performing an audit for electronic records compliance. Remember, the internal audit is a tool to advise management as to compliance with the 21 CFR Part 11 regulation. You need to be both thorough and efficient. This article provides the means to achieve both objectives. ❑

About the Author

Leonard A. Grunbaum is the President and Chief Operating Officer of META Solutions, Inc. He is responsible for all operational aspects of the company, and the management of all aspects of the validation consulting services to the pharmaceutical industry. Len has a B.A. and a M.B.A. from Long Island University. He was a Director of the Electronic Data Processing (EDP) Auditors Association and is a member of the Drug Information Association (DIA). Len is the author of Do It Right The First Time: A Handbook for Controlling Technology Through Good Validation Practices, *published in the February 2000 issue of the* Journal of Validation Technology. *He has also presented validation and audit-related training sessions to clients and professional groups. Len can be reached by phone at 732-845-4904, by fax at 732-845-4834, or by e-mail at len_g@metasol.com.*

References

1. FDA. Code of Federal Regulations, Title 21, Food and Drugs, Part 11. "Electronic Records; Electronic Signatures: Final Rule." *FDA Federal Register* 62 (54), 13429-66. 20 March 1997.
2. FDA. "Guidance for Industry: Computerized Systems Used in Clinical Trials." April 1999.