FDA VALIDATION GUIDELINES AND TITLE 21 CFR PART 11 REQUIREMENTS
PI In Compliance

FDA VALIDATION GUIDELINES AND
TITLE 21 CFR PART 11 REQUIREMENTS
This document has been developed for those interested in the application of the PI System for production monitoring and reporting in the Pharmaceutical and Biotechnology industries. It addresses the requirements of 21 CFR Part 11 compliance, and is intended to assist OSIsoft customers with the validation of their PI Systems.

- Introduction to compliance with FDA regulations
- Review of validation requirements for the PI System
  a. Introduction to validation and verification
  b. Defining computer system validation
  c. Developing the validation plan
  d. Installation qualification
  e. Operational qualification
- Requirements of the Title 21 CFR Part 11 regulation
- PI compliance with these requirements

- Have PI installed or who are considering the PI System
- Want to understand how PI functions meet FDA requirements

- Consultants and technical experts who have worked with the food and drug industry, and the application of 21 CFR Part 11
- Developers and technical experts who know the PI System products
- Knowledgeable customers who are cognizant of FDA requirements and implications
Table of Contents

1 Introduction to Compliance ............................................................................. 4
   Background .................................................................................................. 4
   The Regulation ............................................................................................. 4
   PI Compliance ............................................................................................. 5
   OSIsoft Support .......................................................................................... 5

2 Introduction to Validation ............................................................................. 7
   Validation - General Definition ................................................................... 7
   Computer System Validation ....................................................................... 8
   OSIsoft Software Development Practices ................................................... 10
   Defining a Computer System Validation Plan ............................................ 11
   Responsibility for Validation: Practical Considerations ............................... 11
   Developing the Validation Protocols ........................................................... 12
   Computer System Validation Plan ............................................................... 12
   PI Specific Computer Validation Plan ......................................................... 13
   Areas of Responsibility ................................................................................ 14

3 Installation Qualification Test Protocol ......................................................... 15
   Installation .................................................................................................... 15
   Installation Qualification Verification Scope ................................................. 15
   Manuals Verification .................................................................................. 15
   Software Installation Procedures Verification ............................................ 15
   Security Setup Verifications ....................................................................... 16
   Site Specific PI System Configuration Verification ..................................... 16

4 Operational Qualification Test Protocol ....................................................... 17
   Testing .......................................................................................................... 17
   Operational Qualification Verification Scope .............................................. 18
   PI Point Database Testing ......................................................................... 18
   Interface Testing ........................................................................................ 18
   Buffering Tests .......................................................................................... 19
   Security Issue ............................................................................................. 20
   Audit Trail Testing ...................................................................................... 20
   Activity Tracking Tests ............................................................................. 21

5 Title 21 CFR Part 11 – The Regulation ......................................................... 22
   Summary of the Rule .................................................................................. 22

6 The Regulation and PI Compliance ............................................................. 28
   Requirement ............................................................................................... 28-32
   Response ..................................................................................................... 28-32
The pharmaceutical and biotechnology industries have been investing in paperless systems since the 1980’s, and for compelling economic reasons. These systems are used to automate, monitor and report on production operations, and are an integral component of Good Manufacturing Practice. As such they are subject to FDA regulation. During the 1990’s the technologies available for electronic record processing and authentication reached the point where the industry needed specific guidelines for the FDA's acceptance of paperless systems, and the FDA responded in March 1997 with the regulation known as 21 CFR Part 11.

21 CFR Part 11 is concerned with the authenticity, integrity and confidentiality of electronic records and signatures. Computer systems must be validated to ensure the accuracy, reliability, and consistency of operations, and their ability to identify invalid or altered records. A key requirement for compliance is the ability of the system to create an audit trail, or audit management database. This database must provide a secure log of all attempts to access or log onto the system, together with the operations performed.

The audit management database must enforce these criteria:
- Audit records are secure, computer generated and time-stamped
- The person making any change must be identified
- Both original and changed data must be recorded
- Evidence of previously changed or deleted data must be visible
- FDA must have access for review purposes

21 CFR Part 11 is highly significant because it allows electronic records to be considered equivalent to paper records, and electronic signatures to be considered equivalent to handwritten signatures. The regulation is subject to phased implementation with the initial focus on drug manufacturing. The FDA is expected to stop accepting paper records in the near future, and while there has been a temporary grace period, FDA inspectors are now trained in the regulation, and enforcement has begun. Existing computer systems must be updated or replaced in order to comply.

Good Manufacturing Practice (GMP) ensures that production processes repeatedly conform to batch recipes, and products meet stringent quality specifications. The PI System supports GMP by monitoring the entire production process from recipe download, through process template profiling, to automated batch reporting, and also enforces logon security
and audit trails for any manual data changes. The PI System is validation-ready with supporting documentation to meet all FDA requirements.

The PI System has been installed for electronic record management in the pharmaceutical and biotechnology industries for many years. Capabilities that have contributed to PI’s successful deployment include long-term archiving, automated back-up, integration of all process data across the plant, batch tracking and reporting, and statistical quality control.

In 2002, OSIsoft released an audit management database with tools to support specific customer electronic requirements for 21 CFR Part 11. The PI System addresses 21 CFR Part 11 compliance by:

- Auditing all value, system configuration and user security changes
- Supplying tools to generate selected reports and facilitate FDA audit requests
- Enforcing authorized access and password management
- Detecting any attempt to modify records in the audit management database

The provisions of the regulation make computer system validation a prerequisite for compliance with 21 CFR Part 11. Therefore, the availability of software functions to meet access security and electronic record and signature management, although necessary, do not on their own constitute compliance. Compliance is contingent on successful validation of the specific computer systems used in drug manufacturing, and their ongoing support.

The application of computers in regulated industries requires a thorough and common sense approach to meeting requirements for validation and verification. Many industries are subject to regulation in regard to environment, health and safety, especially pharmaceuticals and biotechnology, where plant information and control systems are used to make decisions, which affect product quality, safety, and fitness for use. Both the underlying process control system and associated Plant Information (PI) System must be subjected to rigorous and documented validation and verification. The focus of this document is, therefore, on how to validate the PI System, where process and system validation have the objective of ensuring that manufacturing processes and documented computer systems perform exactly as intended.

Compliance with 21 CFR Part 11 starts with validation of the computer system. PI has specific characteristics and capabilities that support
compliance, and OSIsoft offers customer assistance and support to simplify the process of validating PI software and verifying system specifications and functionality. This document offers guidelines for validation of the PI System. It should be considered a starting point in developing a plan for the requisite documentation and test protocols that will be used to develop a site-specific validation plan.

Every manufacturing process is unique, and each company follows its own practices and policies. Only the user can determine the exact requirements for validating a process. Obtaining the vast amount of information needed to withstand the scrutiny of an FDA inspection or internal QA audit can seem overwhelming. OSIsoft is committed to providing the help and support its customers may require for successful validations. This document is a guide to successful validation.
The FDA regulations require that each system be validated on its own merits, and these guidelines provide an objective framework, which ensures that the organization is in control of their PI System and its application. Validation involves three fundamental steps:

- Establishment of a detailed plan, which documents the process of reviewing and testing the computer system throughout its life cycle, from procurement through system and application implementation, and throughout ongoing enhancements. This provides the objective framework needed to ensure that you are in control.
- Documentation to ensure that specific system and application requirements and design specifications are in place, using the appropriate procedures and protocol.
- Verification that the computer system and applications perform reliably and consistently as documented.

It is important to understand that the responsibility for validation lies entirely with the regulated manufacturer. The FDA does not itself validate systems, and you cannot just buy a validated system from the vendor. The regulated manufacturer will always have to take action to ensure that the system can be validated. If the FDA does conduct an audit, they will inspect the documentation associated with each step to ascertain whether or not the manufacturer is legitimately in control of both system and process.

Every pharmaceutical and biotechnology manufacturer must develop internal operating standards for processes that govern product quality, production efficiency, and product safety. These organizations operate under Federal regulations established by the Food, Drug, and Cosmetic Act, and the Public Health Service Act, which are intended to ensure that products are produced according to accepted practices, and that each product's fitness for use, including such characteristics as safety, identity, strength, quality, purity, and efficacy, is assured. These regulations, which also ensure that products have not been adulterated during the processing, packaging or handling, are known as current Good Manufacturing Practice, or cGMP.

**Validation** is the process of documenting and verifying that such standards are being reliably met.

**Process Validation** establishes documentary evidence which provides a high degree of assurance that a specific process will consistently result in a product that meets its pre-determined specifications and quality attributes. Computer System Validation is, in turn, a component of the larger task of process validation.
Computer System Validation provides a high degree of assurance that any computer system associated with the manufacturing process will consistently operate in accordance with pre-determined specifications.

Validation Test Protocol is the specific plan or documentation intended to produce evidence that the system or process has been validated. A summary of the definitions and issues that apply to computer system validation is provided in this section. The training documents used by the FDA for its inspectors are an excellent source of reference material. A good way to gain an understanding of computer system validation is to describe what happens during an FDA Inspection.

The inspector will first identify the employees responsible for managing and maintaining the computer systems, review their resumes and look for relevant experience and training.

The inspector will then want an orientation covering the systems to be audited and their functions. A graphical overview of the computer systems architecture with some functional description should be sufficient for this purpose. Only systems that have an impact on “Good Manufacturing Practice” (GMP) are of interest. This typically means control systems used for production automation, QA/QC systems, laboratory automation systems, and any systems used to monitor production processes and document batch records. This document assumes that validation testing of field devices and controllers has been addressed, and that the inspector will want to identify the computer equipment involved in each area, and the associated production processes.

FDA Inspectors are well trained on the software development process, and, when auditing custom developed software, expect to see a professional and methodical approach to purchasing, engineering and ongoing system maintenance.

The expected system life cycle steps include:
- User requirements definition
- Vendor evaluation and audit
- Computer system design — hardware and software
- Software development, coding and testing
- Acceptance testing (FAT/SAT)
- Maintenance plans for the installed system

Verification that these steps have been properly undertaken will be sought in documents such as proposals, functional requirement specifications,
design specifications, source code documentation, software test results and maintenance procedures.

For a vendor supplied package such as the PI System, evidence of professional software development practices are sought in vendor audit reports, system manuals and technical support logs. Inspectors are also trained to look for areas of concern such as data integrity, time consistency (actual versus recorded time), system security (accountability, authorization for changes and the ability to discern unauthorized changes), and system performance (repeatability and performance measurement).

An overall Validation Master Plan references the specific Computer System Validation Plan, and in a typical inspection this is one of the first documents to be evaluated. The Computer System Validation Plan should contain overview architecture diagrams, a description of each computer system’s purpose and a description of how the systems have been tested to prove they perform as designed. References should be made to all of the Software Life Cycle documents mentioned earlier. The Computer System Validation Plan should also define responsibilities and reference any change control and maintenance procedures.

The Plan references two other validation documents, an Installation Qualification (IQ) Test Protocol and an Operational Qualification (OQ) Test Protocol.

The IQ documents all aspects of system installation. All hardware and software are listed with software version numbers recorded. Any vendor standards of operation are referenced, all physical connections recorded, the results of any diagnostic testing included, and any listed safety parameters tested. OSIsoft Field Services will document the specific PI installation as part of their installation activities. The location of manuals and system documentation can also be listed here with controls to ensure that the versions of the documents match the release of software installed. The OQ documents testing of the operational aspects of the system prior to going into full production. The FDA defines the testing of software as “the process of executing programs with the intent of finding errors”.

These are some of the installed system validation issues that inspectors encounter:

- Companies often have no validation plan.
- Design requirements are poorly defined.
- No life cycle approach can be identified.
- System compliance cannot be measured.
• Functional specifications cannot be identified.
• Change control and software configuration management are inadequate.
• Maintenance procedures for backups and system administration functions are poorly written, or completely lacking.

In reality, most of these issues can be addressed by taking a common sense approach to planning and documenting the implementation of any system introduced into a drug-manufacturing environment. The appearance, conduct and credentials of the system owners should address most of an inspector's concerns. The rest of an installed system's defense comes down to documentation, documentation and more documentation. But bear in mind that all statements and claims must be supported by evidence in the form of test results, and specific evidence of the Quality Unit will be part of documentation review and approval.

Clearly, most of an FDA inspector's training is focused on the phases required to build custom applications. And this involves software development, with all the risks and pitfalls associated with programming. This is not the world of the off-the-shelf packaged product that characterizes the PI System. It is important to understand what exactly the FDA does expect, as it can be difficult to appreciate this. The Software Development Life Cycle for a custom application must take into account the development cycle for the underlying vendor software package.

In fact, the potential buyer is encouraged by the FDA to perform audits on software package suppliers, and look for evidence of professionalism throughout the development cycle. Proof of good design is sought. Test results, code walk-throughs and review reports are asked for, and source code is examined to see that it includes comments and follows standards.

The consensus amongst industry experts is that since the inspection of vendor software source code is not a total solution, companies using vendor software packages should be sure to obtain assurances that the vendor has complied with acceptable software design, development, testing, and change control practices, including:

• Development standards that address the assignment of responsibilities and authorities for code design, implementation, testing, and quality assurance
• Programming standards that establish documentation practices and coding standards
Testing standards that define responsibilities for software testing, how test scripts are to be developed, and how test results are to be documented and acted on

Revision control standards that govern how revision management is to be accomplished, how software defects (reported both from the field and internally) are to be documented and corrected, and how the installation of software upgrades in the field is to be managed

OSIsoft’s PI System has successfully passed audits by many large pharmaceutical customers. This fact may be sufficient for many customers, but some make an Audit Report a mandatory part of their procedures. Requests for an audit of OSIsoft are welcomed.

OSIsoft is often asked, “Has PI ever been validated?”

Now that we have provided insight into the validation issues, this question is best answered in three parts:

1) OSIsoft has been successfully audited by a number of large pharmaceutical manufacturers who are PI users, and have FDA approved products on the market.

2) The installation and operation of the PI System by these companies has been documented as part of their overall computer system validation plans.

3) OSIsoft can guide you on the IQ and OQ testing recommended for PI, but this is only one aspect of the validation process. We also recommend that personnel be trained and standard operating procedures (SOP’s) developed for the ongoing change control and maintenance of your computer systems.

Conforming to cGMP (current Good Manufacturing Practice) does not, in itself, ensure a valid process. Nor does the FDA validate a specific process or plant information system, because it would be impossible for the FDA to impose specific production rules on manufacturers. Every process is different, because every pharmaceutical product is unique. Similarly, there are countless models, combinations, and configurations of computer system hardware and software that are applied to controlling these processes. It is, therefore, the obligation of the pharmaceutical manufacturer to provide documented evidence that the system is operating as intended and within the operating limits for which it is specified. The FDA functions as an inspector for the system, arriving on-site to determine if the manufacturer has given proper consideration to product quality and safety, and is able to provide documented evidence to this effect.
This evidence should include information about:

- System hardware and software functionality
- Data definitions including process variables
- How products are tracked through manufacturing
- Manufacturing processes — batch or continuous
- Production periods, batch numbers and lot numbers
- Actual data validity — this is particularly important given FDA regulations for Electronic Records and Electronic Signatures (21 CFR Part 11).

Any discrepancies found during an inspection may result in warning letters, “483s”, fines and even suspension of the license to manufacture.

The validation protocol comprises one or more documents that generate evidence that the system has been validated. It must be developed in accordance with:

- The current Good Manufacturing Practice (cGMP) regulations which the manufacturer must adhere to during the design and implementation of the processing system
- Existing SOP’s
- QA requirements
- Company standards

The activities of this phase include the development of the overall Computer System Validation Plan, the definition of what area protocols are needed to support the Validation Lifecycle of the system, and the assignment of responsibilities to personnel. The Computer System Validation Plan defines a master strategy governing consistent standards, approaches, and requirements for area-specific protocols. It defines the manufacturing facility and each of the facility’s specific areas, and describes the extent of validation required for each.

The Computer System Validation Plan will:

- Specify the scope and use of the computer system.
- Specify which validation tests must be performed against each system specification, and how.
- Specify which protocols and standard operating procedures need to be written.
- Define how and where results are to be recorded.
- Identify which system life cycle activities need to be addressed in the area-specific protocols, such as ongoing system maintenance.
- Define standards for change control, and when process changes and enhancements are required.
- Provide draft guidelines for assessing the impact of such changes, obtaining authorization for the changes, and determining the extent of revalidation required.
- Establish audit procedures and responsibilities.

The most important aspect of the protocol is to stipulate what constitutes acceptable test results.

The intended use of the PI System should be precisely defined, and specifically, the real-time monitoring of equipment and processes identified. Some areas of the facility may require more extensive validation than others. The PI System plan should provide justification for these decisions.

Examples of typical project statements and objectives are given below.

The introduction of the PI System will automate the collection, storage and presentation of plant data. The PI System will serve as a central data repository for all plant/facilities data. PI Systems are designed to accommodate very large real-time and historical databases, and are typically configured so that every process point is stored on-line for as many years as required, and at its original resolution. Given these high-resolution databases and associated client software programs, users can view current manufacturing status, together with a very clear and accurate picture of past operations.

Process automation and control systems are typically used to collect and store data into separate files on separate individual systems. These files are difficult to access, inefficient and do not provide an integrated view.

Establish the PI System as a manufacturing/facilities information infrastructure and data archive that unifies data into a single repository, and allows authorized individuals to access, view and analyze common information and, as necessary, to enter manual data values.
The scope of the PI System Validation Plan pertains only to the collection, storage and display of process control and facilities related data. The plan will define the scope of work based upon company policy and critical functions performed by the system. The plan will also define documentation deliverables, responsibilities, and any special procedures unique to the validation of the PI System.

The PI System Validation Plan will also:

- Define specific test plans that are consistent with the standards of the company’s master protocol for system components, installation, hardware validation and software configuration.
- Identify and document specific maintenance procedures, including any preventative maintenance.
- Define specific procedures for change control.
- Establish an audit trail for the area and a logical and consistent organization for all validation information.

It may well be desirable to have a statement from management underscoring the importance of the validation process and their intention to adhere to good manufacturing practice in the overall Computer System Validation Plan. A validation team should be assigned with overall responsibility for validation of the facility. The validation team will, in turn, generally delegate responsibility to other individuals for portions of the PI System Validation Plan.
This section is concerned with the definition of the PI System Installation Qualification Test Protocol. At a minimum the following PI System software components will typically be installed and documented for validation:

- PI Server
- PI Interface Nodes
- PI Client Tools

As defined in the PI System Validation Plan, the validation strategy has been developed to systematically test the system at numerous levels. These levels start with the basic installation and setup documentation, and finish with system level operational testing.

The PI System must be installed as detailed in each of the specific OSIsoft PI System manuals. This will ensure that during the installation of each PI System software component, OSIsoft product documentation and development guidelines are followed.

An Installation Qualification (IQ) Test Protocol should be written to cover all aspects of the software installation including the pre-qualification and post-installation qualification activities. In order to simplify and facilitate the logistical breakout of the different computers, this protocol should refer to independent testing procedures for each appropriate computer.

The Installation Verification Forms should be developed and included in an Installation Qualification (IQ) Test Protocol. These forms can be used to record installation information such as installed software programs, date of installation and version numbers.

The IQ should cover the minimum set of verifications needed to assure proper installation of the software components for the PI System. Consult OSIsoft if you experience any difficulty getting installation information for your PI System.

Installation Verification Forms should be developed to:

- Verify and document the availability, location, and, as appropriate, the version, status and accuracy of the manuals supplied by OSIsoft.
- Verify and confirm that all pertinent installation instructions contained in OSIsoft manuals were followed. Document specific software configuration choices or settings made for the FDA regulated PI System during software installation.
Document the security configuration for PI System users. This includes the identification of:

- All computers with access to the PI Server
- User groups and permissions
- User names and PI data access permissions

Special consideration should be given to ensuring that PI Server access is set up to inherit any operating system security settings that satisfy 21 CFR Part 11 compliance. Note that operational checks used to ensure that the security configuration prevents unauthorized personnel from changing or modifying the PI System are part of the OQ testing.

Each system requires configuration validation, which means documenting the way the PI System has been configured to collect real-time data from process measurement and control systems. This includes PI Point Database configuration and installed automation system device interfaces. There are several areas to be considered, and examples include:

- Documenting the PI Digital State Set definitions used to interpret the meaning of digital point numeric values
- Documenting the PI Module Database data structures used to model and keep track of entities and relationships monitored by the PI System, such as equipment definitions and batch activities tracked by PI
This section is concerned with defining the PI System Operational Qualification Test Protocol. Once the PI System has been installed and properly configured, software operation can be verified.

There are several unique areas of the PI System that need to be validated, each having its own distinct impact on overall system operation. The following list highlights some important areas, but each site must compile a comprehensive list that meets its own specific validation requirements.

- PI Interface Nodes support real-time data collection from automation and control systems, and perform exception reporting or filtering based on attributes defined in the PI Point Database. Tests must prove that the data values originating in the control system are read, interpreted and reported properly to the PI Server.

- Data buffering is a function of the PI Interface Node, and must be checked to prove that incoming data are stored in the buffer queue when the PI Server goes off-line, and that buffered data are forwarded correctly when the PI Server comes back online.

- The PI Point Database defines the attributes of points associated with values collected via device interfaces, calculations or external data systems. This database is maintained in the PI Server Node and must be scrutinized to ensure that each point is correctly defined, and corresponds with its data source.

- The PI Server stores incoming and calculated real-time values in the memory resident snapshot. Values are then processed for archiving on permanent storage, using point-selectable compression algorithms. Values in the archive must be evaluated to determine that compression is set to meet the desired data fidelity.

- PI Client applications get data from the PI Server snapshot and archive databases. Values must be checked to ensure that accuracy is in line with expectations, and data is displayed correctly. Data values should be checked against source at the interface, snapshot, archive and client to ensure the required fidelity is maintained.

- The system’s security options must be shown to restrict PI Server login and point access to authenticated users, and to log details of all manual changes made to electronic records.

- The PI Audit Management database must be shown to correctly capture any changes made to original data or database attributes.

- If the PI Module Database is used, it should be checked to ensure that it accurately tracks the structured data elements monitored by the PI System.
An Operational Qualification Test Protocol should be written to ensure that the installed software operates according to the appropriate design specifications.

Operational testing forms should be developed to document the results of executing the Operational Qualification (OQ).

The OQ should cover at least the minimum set of verifications needed to assure correct operation of the PI System software components. Consult OSIsoft if you experience any difficulty acquiring operational information for your PI System.

Operational testing forms should be developed for the areas like:

The PI Point Database definitions need to be verified to ensure that the points being monitored are properly represented in PI. There are many different attributes for each point in the database, and those that are critical to proper data access and labeling are shown below:

- **Tag**: This is the identifier used to make references to a specific data point. Tag names must be uniform and consistent throughout the control system and PI System. They should conform to some convention that makes it easy to access specific sets of tags.
- **PointSource**: This attribute is used to associate PI tags with a specific interface or control system type. For example “A” could be used for points from Allen Bradley PLC’s, or G from GE Fanuc PLC’s.
- **Location Codes**: These are associated with the PointSource and Instrument Tag, and can be used to define control system addresses for specific point values.
- **PointType**: This attribute identifies the data type for values stored in PI. The choices are numeric (Float and Integer), status (Digital State) and text (String).

Other PI Point attributes define point description, engineering units, zero and span, calculations, exception and compression limits and other information as needed. These should be added to the test list as required.

Interfacing with automation systems involves several software and hardware components. For example, a specific PI Interface reads point values from the associated automation system across some communication link. Incoming values may be in engineering units...
or the raw contents of registers, which have to be scaled. If exception reporting is enabled, only values that cross the deviation threshold will be sent to the PI Server.

PI validation assumes that testing of the field device to controller has already been performed. All PI software modules (interface, server and client applications) use standard function calls to access and process exception information, or events. Based on this, the following operational testing guidelines can be written to validate data flow and integrity:

- Test selected points for each defined control system.
- Test all the points that are to be used in any batch reports.
- Verify that data point values fall within the required precision.
- Verify that PI node and control system computer times are automatically synchronized, and set as close to each other as possible.
- Verify that the timestamps of values in the PI snapshot are the same for the equivalent control system values.
- Verify that the PI Clients display the correct timestamp and current value.

Data buffering is a function of the PI Interface Node, and ensures the continuous collection of data on the local interface computer regardless of the status of the PI Server Node or the network link to the server.

Bufserv is the process that queues data locally when the PI Server is unavailable, and then sends the queued data to the PI Server when it becomes available. Bufutil is the process that monitors and controls the buffering process.

There are several possible causes for data buffering to occur, so to validate the system as operational, test cases should be constructed to exercise the buffering functionality. For example, the following tests could be performed:

- Controlled shutdown and re-start of the PI Server Node
- Disconnection and reconnection of the link between PI Interface Node and PI Server

The ability to recover from failures should be checked from end to end. This involves verifying that buffered data are sent to the snapshot and that the archive is fully recovered.
A number of security mechanisms will be employed at a manufacturing site to protect the PI System from willful attacks or accidental tampering. These will typically include physical security, network security, operating system security and PI System security.

First, the PI System files can be protected by physical security measures. The PI Server may be located in a secure computer room where electronic locks are employed to restrict personnel access. Second, the computer that runs the PI Server can be used solely for specific PI applications, with the system files protected by operating system logon and password protection.

Even though unauthorized physical access to the PI System can be prevented, access is available over the network. Network security can be provided by several mechanisms. Typically GMP facilities may employ firewalls, VPNs or proxy servers, or some combination of these to restrict access to the PI Server computer.

The PI System also has specific security databases. The PI Trust Login mechanism can be used to automatically check that the logged-in operating system user is a valid PI user in the PI User and PI Group databases, and it then grants the appropriate access rights. A description as to how the PI Trust Database is configured can be found in the PI UDS Manual, Chapter 10, “Defining Trust Records in the Trust Database”.

Security extends down to the PI point level. Each point is assigned an owner and a group. The site’s PI administrator assigns read and write access for the owner, group and world. The attributes of a point (such as zero, span, engineering units etc.) may be assigned to a different owner and a different group, with independently assigned access permissions.

There may be instances where PI points are used to record manually entered data such as lab test results. The PI OQ testing should have additional focus where user access permissions allow manual entry of point data values and PI point attributes, since physical access and network security should fall under separate IT department testing.

For FDA compliance, process information systems require stringent measures to insure data integrity. Data integrity involves accountability for all data added, edited, and removed from the systems.

The PI Audit Management Database provides the databases and tools needed to accurately monitor changes to the key databases in the PI System. It is described in detail in the OSIsoft manual, “Auditing the PI UDS”.

Audit Trail Testing

Security Issues
The PI Audit Database contains records for changes to the following databases:

**Configuration Databases**
- PI Point Database
- Digital State Database

**Security Databases**
- PI User Database
- PI Group Database
- PI Trust Database

**Time Series Databases**
- PI Archive
- PI Snapshot

Each audit record is assigned a unique ID and contains all pertinent change information including the original value and timestamp, new value and timestamp, type of audit record and who made the change.

OQ tests should be developed to verify that the audit trail is functioning as required.

When the PI Module Database is used to record activities such as batch execution, operational checks should be made to ensure that the PI System tracks such activity correctly. This should be developed as part of the OQ testing.

It is strongly recommended that the Operational Qualification (OQ) Test Protocol also include descriptions of both the basic functionality of the PI System, and how PI Interface Nodes and specific interfaces are used to collect process data. These descriptions will aid the OQ reviewer in understanding how process data are collected and stored by the PI System.
Section 11.1 Scope

(a) The regulations in this part set forth the criteria under which the agency (FDA) considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with Sec. 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

Section 11.2 Implementation

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of additional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving
unit(s) not specified in the public docket will not be considered as official if they are submitted in form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

2. Agency means the Food and Drug Administration.
3. Biometrics means a method of verifying an individual’s identity based on measurement of the individual’s physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.
4. Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
5. Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
6. Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.
7. Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual’s handwritten signature.
8. Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.
9. Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, performance, and the ability to discern invalid or altered records.

(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

(d) Limiting system access to authorized individuals.

(e) Use of 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. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign records, access computer system input or output devices, alter records, or perform the operation at hand.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

(i) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

(j) Use of appropriate controls over systems documentation including:
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
(2) Revision and change control procedures to maintain an audit trail that documents time sequenced development and modification of systems documentation.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in Sec. 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;
(2) The date and time when the signature was executed; and
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or assigned to anyone else.
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual’s electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.
(c) Persons using electronic signatures 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.

1. The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

2. Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer’s handwritten signature.

(a) Electronic signatures that are not based upon biometrics shall:

1. Employ at least two distinct identification components such as an identification code and password.
   i. When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.
   ii. When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

2. Be used only by their genuine owners; and

3. Be administered and executed to ensure that attempted use of an individual’s electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.
The Regulation and PI Compliance

The relevant sections of the FDA 21 CFR Part 11 regulation are listed together with how PI can be used to comply with the regulation. Any PI technology and products used to implement a compliant system are outlined. The reader should note that PI is not an electronic signature (Esig) data entry application. Therefore, we have detailed how the PI Server complies with Section B – Electronic Records, and no response is made to Section C – Electronic Signatures. However, once generated, electronic signatures can be considered as Electronic Records, and this is addressed in Sections B/11.50 and B/11.70.

<table>
<thead>
<tr>
<th>21 CFR Part 11 Regulation</th>
<th>PI Statement of Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section</td>
<td>Requirement</td>
</tr>
<tr>
<td>B/11.10</td>
<td>Controls for closed systems</td>
</tr>
<tr>
<td>(a)</td>
<td>Validation of systems to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records.</td>
</tr>
<tr>
<td>(b)</td>
<td>The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.</td>
</tr>
<tr>
<td>(c)</td>
<td>Protection of records to enable their accurate and ready retrieval throughout the records retention period.</td>
</tr>
<tr>
<td>Section</td>
<td>Requirement</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>(d)</td>
<td>Limiting system access to authorized individuals.</td>
</tr>
<tr>
<td>(e)</td>
<td>Use of 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. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.</td>
</tr>
<tr>
<td>(f)</td>
<td>Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.</td>
</tr>
<tr>
<td>(g)</td>
<td>Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.</td>
</tr>
<tr>
<td>Section</td>
<td>Requirement</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>(h)</td>
<td>Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.</td>
</tr>
<tr>
<td>(i)</td>
<td>Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.</td>
</tr>
<tr>
<td>(j)</td>
<td>The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.</td>
</tr>
<tr>
<td>(k)</td>
<td>Use of appropriate controls over systems documentation including:</td>
</tr>
<tr>
<td>(1)</td>
<td>Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.</td>
</tr>
<tr>
<td>(2)</td>
<td>Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</td>
</tr>
<tr>
<td>21 CFR Part 11 Regulation</td>
<td>PI Statement of Compliance</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td><strong>Section</strong></td>
<td><strong>Requirement</strong></td>
</tr>
<tr>
<td><strong>B/11.30</strong></td>
<td><strong>Controls for open systems</strong></td>
</tr>
<tr>
<td></td>
<td>Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.</td>
</tr>
<tr>
<td><strong>B/11.50</strong></td>
<td><strong>Signature manifestations</strong></td>
</tr>
<tr>
<td></td>
<td>(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:</td>
</tr>
<tr>
<td></td>
<td>(1) The printed name of the signer</td>
</tr>
<tr>
<td></td>
<td>The PI UDS can store the printed name of the signer as a text data electronic record.</td>
</tr>
<tr>
<td></td>
<td>(2) The date and time when the signature was executed;</td>
</tr>
<tr>
<td></td>
<td>The PI UDS can store the printed name of the signer as a text data electronic record, along with the date/time stamp for the time when the signature was executed, if this execution time is provided by the signature application.</td>
</tr>
<tr>
<td></td>
<td>(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.</td>
</tr>
<tr>
<td></td>
<td>The PI UDS can also store associated text data to give meaning to a specific entry, if this is provided by the signature application.</td>
</tr>
<tr>
<td></td>
<td>(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).</td>
</tr>
<tr>
<td></td>
<td>The PI Audit Management Database provides secure binary storage for manual changes to electronic records, and also detects any attempts to alter audit trail records. Note that some systems keep records in a non-PI database such as a relational database, and it’s then up to the customer to ensure records cannot be altered.</td>
</tr>
</tbody>
</table>
Electronic signatures and hand-written signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Electronic signature applications may use the PI UDS to store signatures as electronic records. Signatures stored in PI inherit the robust security and audit capabilities of PI.
For further discussion or questions about the PI System in compliance with 21 CFR Part 11, please write pharma@osisoft.com.

Headquarters, USA
OSIssoft
777 Davis St., Suite 250
San Leandro, CA 94577
USA
(01) 510-297-5800
(01) 510-357-8136 (fax)
(01) 510-297-5828 (support)

www.osisoft.com

OSIssoft™

Copyright © 2002 OSI Software, Inc. OSIssoft and the OSIssoft logo (and the PI System, PI ProcessBook and PI ActiveView) are trademarks of OSI Software, Inc. All other trademarks are the property of their respective owners.