white paper Life Sciences

Smart Facility Automation Solutions for Regulatory Compliance

Discover how a Total Environment Management (TEM) solution delivered by an Integrated Facility Automation System can both dramatically improve your business and uniquely enable 21 CFR Part 11 regulatory compliance.

t.a.c®

Table of Contents

I. Executive Summary

This white paper addresses the critical role played by integrated facility automation systems in attaining and maintaining regulatory compliance in life science industry applications. With a recent, near-exponential increase in the number of FDA warning letters, which include citations of non-compliance with 21 CFR Part 11, the scope and importance of this new regulation is quickly becoming understood. Along with the significant technical and procedural challenges of the rule come substantial benefits to those companies who can now seize the opportunity to realize the dream of "going paperless".

The concept of ***Total Environment Management**** will be introduced, offering the ability to capture a holistic picture of the status of a regulated facility through the unification of environmental and security related information and the provision of a framework around which a long-term, comprehensive, and robust facility compliance solution can be built. Appropriate use of electronic records and signatures will be discussed together with the practicalities of assuring compliance through thorough system validation.

***Total Environment Management (TEM):**

Definition: The process of establishing and maintaining a desired environmental state through the integrated monitoring and control of all events and parameters of which it is subject to change.

II. Background on 21 CFR Part 11

In August of 1997, the Food and Drug Administration (FDA) placed into effect regulation 21 CFR Part 11 — a regulation which dictates the manner by which electronic records and signatures are to be captured, secured, retained, and retrieved. The intent of this regulation was to help companies leverage the rapidly expanding role of paperless technologies within their facilities while maintaining and improving compliance with the rigorous quality and safety standards (Predicate Rules) required for pharmaceutical and biotechnology products as well as medical devices.

After an initially slow uptake and the interim focus on Y2K compliance activities, within the past three years, the industry response to this regulation has grown a great deal stronger and many companies are now scrambling to get their 21 CFR Part 11 (hereafter referred to as Part 11) programs in-place. This is due, in part, to the fact that the FDA has recently begun stepping up enforcement of the regulation and is casting an increasingly critical eye upon companies whose facilities are not adequately meeting their record keeping requirements. Punitive action comes in the form of inspectional observations (483s), warning letters or, in the most extreme cases, substantial fines and plant shutdowns. Such actions are made quite public, and in addition to carrying a financial penalty, there's a substantial public relations price a company will have to pay, a situation that pleases neither senior management nor shareholders!

Although the adoption of a paperless system and thereby compliance with Part 11 is not mandatory, realistically, to remain competitive, users have little choice in the matter. That said, compliance should not be viewed as a burden, but rather as an excellent opportunity to improve the quality of not just a manufacturing process but also an entire business.

A. Severe Consequences of Non-Compliance

Among the unpleasantries that can accompany an inadequate response and/or corrective actions to officially documented inspectional findings are:

- CEO gets an official warning letter from the FDA, generally expecting a full compliance plan within 15 days!
- Quality manager could go to jail
- Implementation manager is out of a job
- Company image and share price plummet
- Company's manufacturing license could be revoked
- Huge fines ($100s of millions) could be levied

B. Compelling Benefits of Compliance

The positive reasons for pursuing compliance in an aggressive fashion are the pure business benefits that can be derived by moving to a fully paperless environment. From the ability to accelerate the New Drug Application/Approval (NDA) process to the added security of knowing precisely who was at the controls during any stage of production, employing the audit trail and electronic record and signature capabilities mandated by the regulation delivers a powerful competitive advantage. Those companies who can reduce or eliminate the paper used in their production and approval processes can reduce costs, accelerate time-to-market, and ensure a higher degree of quality and consistency in their end products. Those who adhere to the old paper methods can expect to be left behind.

C. The Compliance Challenge

Achieving compliance, however, is no small task. Although much of Part 11 functionality is software-based, it is certainly not the case that compliance is something that can simply be installed. True compliance embraces more than just environmental and production control systems, methodologies, and operating procedures but extends into virtually every area of the plant and across the regulated industry supply chains. Personnel need to be trained on how to work within the new paperless environment and be made fully aware that any actions or signature manifestations recorded electronically carry the same legal weight as their paper-based predecessors. The systems themselves need to be commissioned, installed, and validated properly to ensure that they're operating in a manner consistent with the letter and law of the regulations. And once the system is up and running, assurances must be put into place to satisfy the requirement that any given record can be called up at any given time in a readily "human" readable format. Compliance with Part 11 is indeed a company and industry-wide undertaking.

Electronic Records in Action

Each year the FDA receives many submissions, including more than 100 original new drug applications (NDAs) from pharmaceutical companies wanting to introduce new drugs, market a drug for a different therapeutic purpose, or change dosage recommendations. Since the introduction of Part 11, the FDA can now review NDAs more efficiently and at a lower cost utilizing Electronic Records. Everyone wins: the consumers who benefit from faster introduction of critical medications, the drug companies that can earn as much as $1 million a day from leading drugs, and the taxpayers who fund a more efficient agency.

The FDA employs 700 reviewers to review NDAs, which can contain as many as 1,000 volumes of 300 pages each and must be submitted in triplicate. "When NDAs are submitted electronically instead of on paper, reviewers have fully searchable files that are easier to locate and distribute. Plus, the costs to the agency of storing these documents are reduced substantially," says Greg Brolund, associate director for technology and policy for the FDA's Center for Drug Evaluation and Research (CDER)

D. Part 11 Delivers Peace-of-Mind (but Watch the Bottom Line)

One of the most powerful arguments for Part 11 compliance is that the regulation actually encourages companies to move into the paperless, and thereby more automated, arena. This will introduce new efficiencies, time, and cost savings into the overall drug discovery, testing, and manufacturing process and help companies to ultimately reduce costs and boost ROI. To get there, however, the initial investment in software, services, training, validation, and documentation development must first be subsumed. Due to the complexities and expense of these items, many companies have waited until the FDA's recent onerous enforcement activities to begin moving toward compliance. However, if vendors are chosen wisely and the

manufacturer does his due diligence prior to purchasing by conducting thorough product assessments and vendor audits, there can be a tremendous amount of time and cost-savings realized both immediately and down the road.

III. Part 11 and Total Environment Management (TEM)

A. Consider The Wider Product Life Cycle

In the rush to bring critical systems into compliance while also pursuing ever-pressing business objectives, it's easy for a company to become inwardly focused and forget why they're making these changes in the first place — to deliver superior product to the consumer, in a more efficient manner, with a greater degree of safety and accountability. To this end, there are substantial opportunities for the companies who focus their attentions not only on the product storage, handling, and production systems, but also on the environments in which those systems reside.

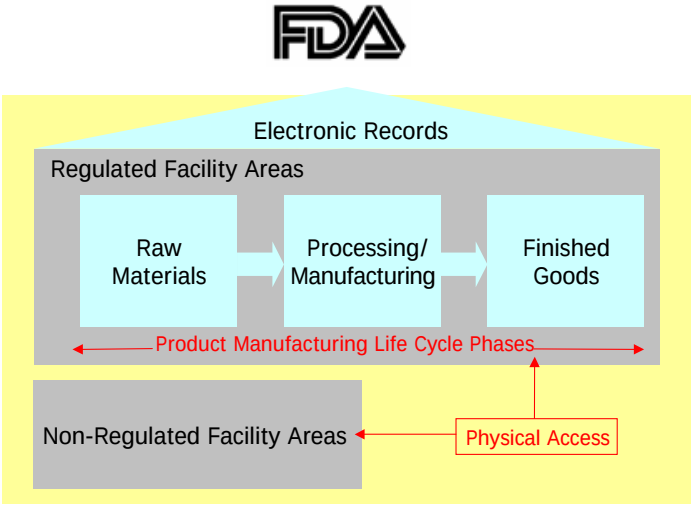

Figure 1. Manufacturing Life Cycle Phases

As depicted in Figure 1, while strict control and record keeping of the manufacturing phase of a product's life cycle is clearly of critical importance, it is also imperative that the upstream and downstream phases are suitably considered for their potential impact on product safety and efficacy. Raw materials storage and handling conditions, as well as finished product warehousing and distribution standards, can potentially affect products just as much as the processing/production phase conditions due to the longer duration of these phases and the higher degree of personnel access typical for these other areas of a facility.

B. Protect Against Direct and Indirect Impact Events

In any production, storage, or laboratory environment, there are two basic classes of unplanned and/or undesirable occurrences able to affect the quality and safety of the end product: direct and indirect impact events. Direct impact events, for example, would be:

- The addition of an improper amount of an active ingredient
- The addition of the wrong ingredient altogether
- An erroneous set point change made to a reaction vessel temperature

These direct impact events are the types of circumstance Part 11 has been expressly designed to capture and reduce the detrimental impacts of to consumers. Electronic audit trails help establish traceability and accountability, aiding the review process objective to "raise flags" should any potentially hazardous actions have been taken or necessary actions omitted during the period under review.

Indirect impact events, however, can be equally harmful to the quality and integrity of the end product but are not as easily recognized — certainly not from within the electronic records generated by a typical production-centric control system. Examples of indirect impact events could include:

- Unexpected changes in ambient temperature or relative humidity that could affect the performance of active pharmaceutical ingredients waiting in raw materials storage locations, perhaps due to a faulty control valve or a door mistakenly left ajar

- Variances in ultraviolet light levels in a finished goods warehouse possibly due to insufficient or degraded screening

A very serious indirect impact event, but one of which we must all be acutely aware, is the theft of an individual's username and password to gain access to a closed system.

So how does one protect their product, their company, and their customers from the potentially devastating effects of both direct and indirect impact events? The answer lies within a robust, simple, and easy to configure TEM solution.

TEM solutions, such as the Continuum™ and Vista systems from TAC, deliver unparalleled environmental integrity across multiple manufacturing life cycle phases. Specific areas of importance include:

Security - Physical and Logical

Despite the standard two-token username and password combination typically employed within a Part 11 compliant production environment, your manufacturing processes and up/downstream storage resources are only as secure as your overall facility. Proximity cards, smartcards, biometrics and video surveillance technologies can easily be combined to ensure the identity of an entrant into a secure area. The need to fulfill physical security requirements is of critical importance in high-stakes applications and is actually spelled-out by the FDA in 21 CFR Part 11.10. Combined with a sophisticated software security model, these measures can guarantee the authenticity and authority level of personnel with access to restricted areas and workstations. Additionally, you can easily trigger alarms if an individual swipes his/her card in an attempt to enter an area for which they are not authorized or if an authorized employee is being forced to attempt entry under duress. The comings and goings of all personnel can be recorded and reproduced via electronic records, delivering yet another layer of accountability. Furthermore, you can instantly restrict specific users from individual areas or entire zones (all but the exit doors, for example) with a mouse-click. This is an important function, as 21CFR Part 11.10 not only covers the protection of facility areas directly related to physical products, but also extends to the protection of the environment of the electronic records (i.e. secure server rooms and archive vaults.)

Environmental Controls

Again, the nature and quality of the air in a regulated facility can dramatically affect the quality of the end product. While simple HVAC-only control systems can monitor and adjust temperature and humidity, a TEM solution can also monitor, control and alarm upon a wide variety of other potentially critical variables such as particulate counts, differential pressure, toxic gas levels, lighting conditions and laboratory fume hood positions. The level of any one (or all) of these factors, in addition to any corrective actions taken to regulate these levels, can all be recorded electronically, providing yet further evidence when reviewing the overall quality and safety history of an end product.

C. Data in Context Reveals the Bigger Picture

Raw data, in and of itself, is often of little use without some complementary data (metadata) to imbue it with relevance. The fact that a particular room's temperature was 73 degrees Fahrenheit, for example, could be of limited value. Knowing that same room's temperature is 73 degrees when it typically should be 64 degrees adds a fairly significant piece of context to the original data and could provide valuable clues as to why the quality of a particular product batch may have been compromised. Add to that data from a card reader that indicates that a particular individual gained access to that room and physically changed the temperature and you have now added accountability to the equation and have a more complete picture of what happened at that precise moment in time.

Alongside the technical requirements of Part 11, an equally important set of documented (and enforced!) company policies and procedures are required for compliance. A company policy requiring the vigilant protection of the confidentiality of electronic signatures ranks high among them. However, as with any username/password-based security system, these two tokens can be compromised. Despite company polices to the contrary, operators may write them down so they don't forget or; they might share them with someone else in the department, or any number of other such activities could occur. As a result, by using a production process-only Part 11-based solution, you can easily glean who was purportedly logged in under a particular username/password combination on any given workstation, but there is no concrete way to know if that individual was actually the one who made the changes that were logged to the audit trail.

With a TEM solution, however, you can track who enters a room by their physical security authentication device and/or biometric readings, then see if the subsequent login information corresponds with any of the individuals who have entered the room. If, for example, Joe Smith is the only operator who has gained access to a secure area, yet Bob Stephens appears as a login for that system during the same time period, you can be relatively certain that access was gained — to either the room or the system — under false pretences and take immediate action. (The corrective security action can also be indicated in a log report and made available to FDA inspectors or other authorities, should the need arise.) Add a security camera to the mix and you have a total, accurate, near foolproof system for delivering the ultimate in security and system integrity for your employees and your customers.

In the above examples, you can clearly see how the aggregation of data and metadata from different sources allows substantial added value to be derived by the creation of true environmental intelligence. This underscores the significant role TEM solutions can play in the overall Part 11 compliance mix — helping you (and possibly the FDA) form a more complete, holistic picture of what really occurred.

D. Evaluating TEM Compliance Solutions

From both the production and the building automation side, two words that should be front-of-mind when evaluating TEM solutions are *interoperability* and *comprehensiveness*.

Interoperability

Technology is advancing and is being adopted at a remarkable rate. At no time in history has change come so quickly and it's finding its way onto our desktops and into our buildings at an ever-increasing rate. Because of the rapid advancements from across the entire landscape, you want to be sure that you'll always have the flexibility to work with best-of-breed, complementary products, regardless of the vendor. So when you're ready to implement a solution, make sure that it has an extensive, diverse communications driver library and can converse freely using many of the well-established and emerging open protocol, networking, and software standards currently available — such as Ethernet, TCP/IP, SNMP, BACnet, Modbus, OPC, XML, SQL, and SVG. By doing so, you can both facilitate interoperation with legacy systems and maximize your forward migration opportunities, extending the working life of your systems and hence you're ROI. In fact, legacy systems require special attention as Part 11 does not contain a "grand fathering" clause — i.e., Part 11 still applies. This generally means that legacy systems must be replaced or upgraded. Therefore, if you have systems already installed, the ability of their original suppliers to provide cost-effective forward migration paths to compliance should be a highly significant differentiator.

Comprehensiveness

Many of the concepts and functionalities encompassed in this white paper are provided by devices from diverse fields of the facility automation landscape — from HVAC to access control, digital video surveillance to fire detection. As such, they typically require different interfaces to get the job done… after all; collecting data on a temperature point once per minute is a very different activity from checking an employee I.D. against a database in sub-second time. However, a TEM solution will deliver this complementary functionality within a single architecture — eliminating the time, expense, and aggravation typically associated with the integration of disparate "point solution" products.

A clean room, as shown in Figure 2, typically requires the tight control of its internal conditions, such as temperature, humidity, and pressure, which, in isolation, can be provided by a relatively simple HVAC control system. However, the purging of the air within the gowning area and access controls/door interlocking are usually managed by separate systems, often from different vendors, that must be integrated. Considering the ability to completely solve this problem and the ease of adding glass-break detection, fume hood position monitoring, and even video surveillance, the abundant advantages of TEM become obvious.

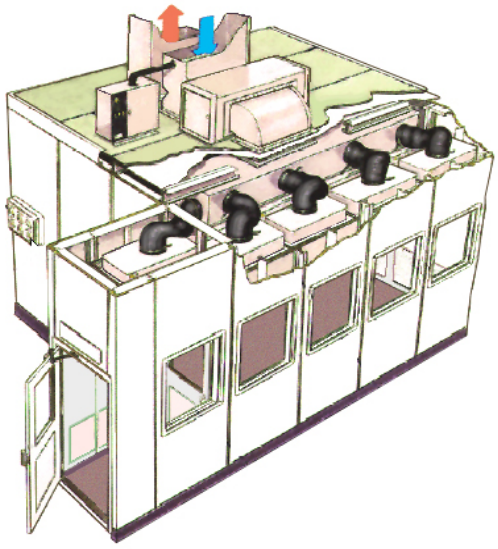

Figure 2. Typical Clean Room (Diagram by Clean Air Technology, Inc.)

E. A Compliance Umbrella for All

An often-overlooked benefit of a TEM system is its ability to provide a compliance "umbrella" for the many subsystems and devices that connect as part of the overall solution architecture. The traditional types of facility automation equipment such as air handling units, chillers, card readers, and door controllers are covered, but other devices that do not have the requisite computational processing, durable media storage, or alarming and database management capacities can easily be integrated into a compliant solution.

Examples include: Variable Speed Drives, Programmable Logic Controllers, Packaged Boiler and Chiller Controls, Power Monitoring Equipment, Video Surveillance Systems, Lighting Controllers, and Fire Monitoring Systems.

Clearly, a facility-wide TEM system, with its innate ability to manage metadata and utilize high capacity and performance databases, resides at the natural and most efficient level of an automated system hierarchy to achieve Part 11 compliance for all such subsystems and devices.

F. Don't Forget to Protect the IT Infrastructure

Keeping in mind that facility automation solutions use many of the same IT infrastructure components as the business as a whole, special focus should be directed towards the particular requirements and responsibilities of these systems when used in regulated applications.

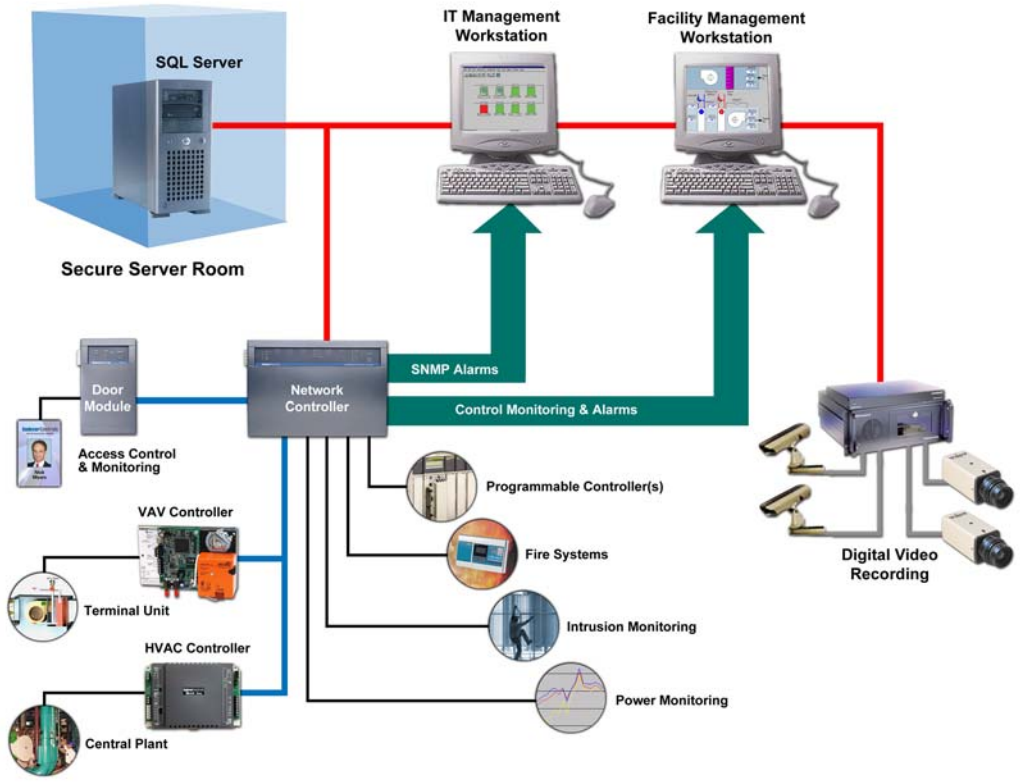

Figure 3. A TEM Architecture for a Regulated Industry Application

The FDA recently issued a Guidance to Industry document concerning the Maintenance of Electronic Records. In this document, the need to go beyond the basic Part 11 requirement to be able to discern invalid or altered records is clearly stated. The security, well-being, and availability of the Electronic Records repository (server room, records vault, data center etc.) must be assured.

A TEM system that includes SNMP alarming provides the answer.

The Network Controller shown in Figure 3 natively supports SNMP alarming capability. This allows a wide variety of environmental and security-related parameters to be monitored, controlled, and alarmed upon, not just by the facilities automation system and personnel, but also by IT asset management software packages (such as HP Openview) and the IT staff. Temperature, humidity, and pressure levels along with door forced or propped open alarms can all be easily detected, recorded, and used as documented evidence to prove the FDA guidelines are being followed.

Furthermore, if you are concerned about the possibility of your facility automation Ethernet backbone being breached and your database being hacked into, a TEM system can be configured to transparently support the use of MS Windows network encryption to make the communication packets unintelligible and therefore useless to the perpetrator.

As the record retention period required for many drugs and medical devices can span many years, automated archiving of electronic records should be considered. Solutions in this area exist to allow encrypted copies of all electronic records for critical environmental parameters, security related events and alarm conditions to be automatically backed up to tape, CD-ROM, or other durable storage media. With appropriate authority, archived data can be easily accessed for review, report generation, and export to other systems.

IV. Conclusion — It's Not Only About Compliance

In addition to regulatory compliance (although eliminating the threat of punitive action from the FDA is a big plus!), the true business benefits that can be achieved are as a result of the applications, policies, and procedures established in the process. As a result, make sure that all relevant parties know precisely what you're expecting to get out of your investment *beyond* mere compliance. Some of the business benefits you can reasonably expect and explore are:

- **Enhanced productivity**
  Paperless records mean accelerated approval processes, significantly reduced storage costs, and the ability to search and analyze record data far more efficiently and comprehensively than ever before.

- **Enhanced quality**
  Because you'll have tighter control, greater insight and more complete records of what's happening, you can more readily replicate the total environmental conditions favorable for "perfect" storage, handling, and manufacturing operations.

- **Improved security**
  At the heart of Part 11 is the ability to limit access to systems, record "who did what" in a very precise way, and eliminate the possibility of record tampering. With the heightened security, the likelihood that your product can be damaged or hampered by malicious intent is dramatically reduced.

- **Improved traceability**
  With regards to discovering what might have gone wrong (or right) with a particular production lot, Part 11 functionality can help you to not only identify what happened at any point during the production life cycle, but can also help you to identify the individuals who had access to that particular area at any given time.

All of the above improvements add up to a dramatic bottom-line impact for your business. The streamlining of your processes means you can get product to market faster. The security and repeatability aspects mean that you can improve consistency and deliver a high-quality, safe product to consumers. And the traceability aspects of the regulation help you to install systems and procedures that will minimize the impact of recalls and, in all likelihood, help you to catch any potential product issues before a single item leaves your facility.

Remember — Your Process Is Only As Secure As Your Facility

V. Appendices

A. Validation & Adhering to GAMP

Claims of regulatory compliance are valueless without "establishing documented evidence which provides a high degree of assurance that a specified process will consistently produce a product meeting its predetermined specifications and quality attributes" – literally, the definition of validation.

Creating and following a comprehensive Validation Master Plan (VMP) ensures that your systems are working in a manner that is consistent not only with the letter of the law and the spirit of the regulation, but also with the expectations and internal policies of your plant. In developing an environment that is Part 11 compliant, you're truly seeking to satisfy two critical conditions: one set forth by the FDA, the other set forth by your own operating policies, procedures, and guidelines of your business. If these two conditions conflict in any way, it should be obvious that the manner that satisfies Part 11 takes precedence. What isn't so obvious, however, is that such a conflict points to a larger problem… that your plant and/or business has not been operating in a manner consistent with GAMP.

The GAMP (*Good Automated Manufacturing Practice*) Forum is a highly influential pharmaceutical industry body whose *Guide for Validation of Automated Systems* is considered the authoritative reference work for validation. It provides an internationally accepted set of guidelines for the validation of computerized systems used within regulated environments. Currently on its fourth revision, GAMP is of particular interest with regards to Part 11 because it helps both solution providers and end-users to define maintenance practices and supporting documentation to help in compliance efforts. And the best way to assure a smooth validation process — and the best way to ensure a pain-free visit from an FDA inspector — is to adhere to and fully integrate the practices and principles espoused by GAMP throughout your entire business.

As you begin to define and develop the system architecture that you will put in place for your Part 11 compliance efforts, GAMP serves as a blueprint for the entire process. From helping you to scope the systems to helping you define what types of functionality you'll ultimately need in each area, GAMP eliminates a great deal of the guesswork and ambiguity which accompanies such regulations.

One of the early, crucial steps of a VMP is vendor selection based upon a determination of the suitability of their products, but equally upon the results of vendor audits. The quality of a supplier's product is directly attributable to the engineering processes and methodologies employed during its development. Software development is particularly susceptible to quality problems given the availability of a huge scope of implementation choices and the relatively recent evolution of software engineering best practices compared with hardware development disciplines. Unfortunately, this situation can often lead to the creation of what has been euphemistically termed SOUP or Software of Uncertain Pedigree. The best way for prospective customers to assure themselves of a vendor's ability to provide reliable products and support them throughout their lifecycles is to conduct a thorough supplier audit.

GAMP also serves as a wonderful tool for leveling the playing field among different vendors. Because Part 11 spans multiple systems and disciplines within your facility, you'll likely rely upon the resources and expertise of different third parties to ultimately achieve and maintain compliance. Each vendor might have their own interpretation of the regulation and how each of their components satisfies the various requirements of Part 11 and, when forced to work together as a single team, this could cause unnecessary delays or inconsistencies in your system… even if you leverage the services of a systems integrator.

An easy way to avoid such problems is through the establishment of a clear, well-documented delineation of what *your* expectations are and what your own internal procedures dictate. Developing this at the onset, with the aid of GAMP procedures, will serve to mitigate the risk commonly associated with bringing together multiple providers to work on a single, all-encompassing solution. Clearly, choosing vendors with a thorough understanding of GAMP and their

responsibilities related to performing the activities and delivering the documentation required by the GAMP lifecycle model (see Figure 4) is key.

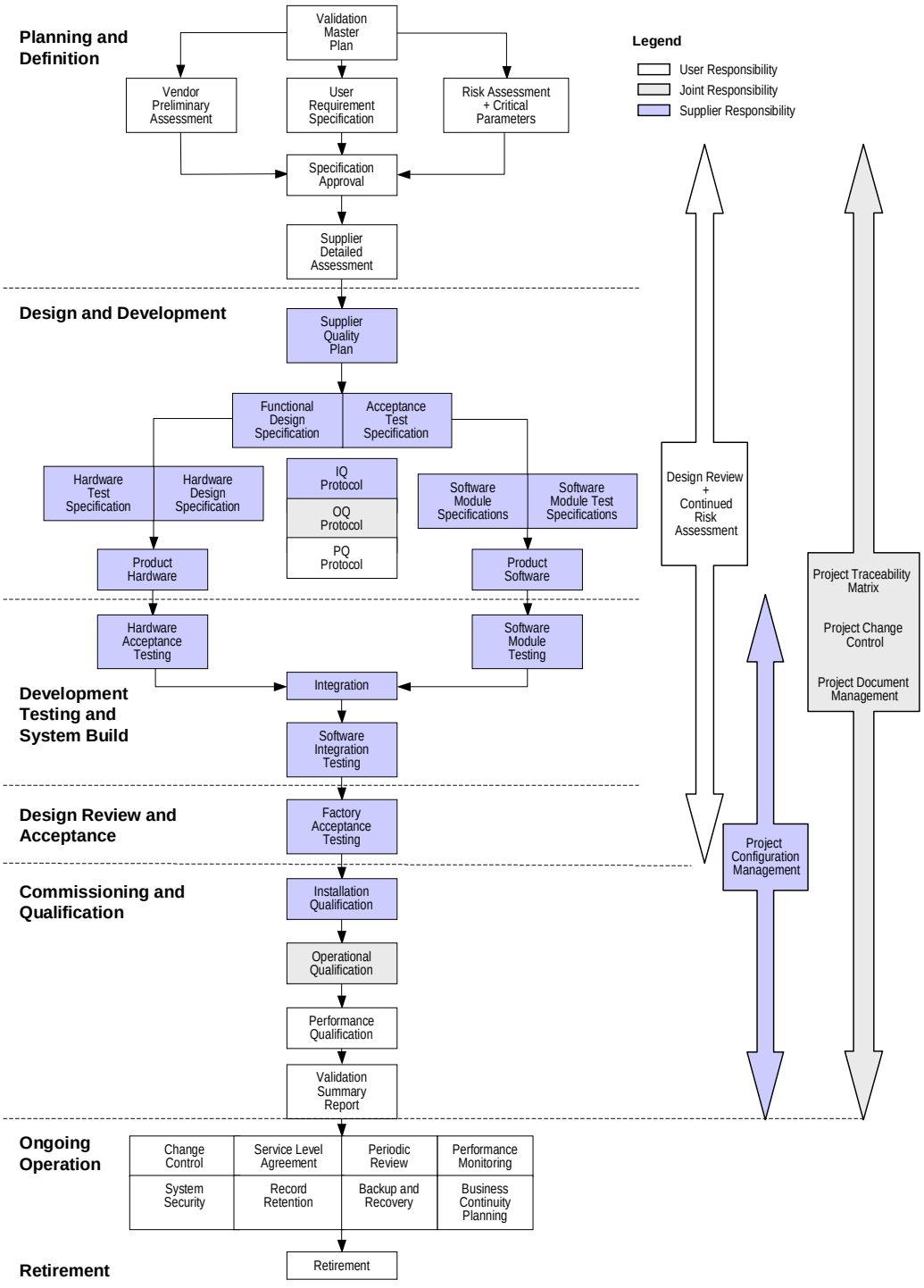

Figure 4. GAMP System Life Cycle Activities and Documentation Deliverables

B. Part 11 in a Nutshell

For all systems to which Part 11 applies:

- Systems must be validated to provide evidence of compliance
- Systems must have a read-only audit trail providing computer-generated date/time stamped records of record changes and operator activities
- Systems must have sufficient security to limit access to authorized, qualified individuals held accountable by written policies
- Systems must be able to accurately generate, retain, protect and readily retrieve all records stored electronically throughout the retention period. Records must be able to be reproduced in human-readable form
- Systems must use operational checks to enforce step and event sequencing where appropriate
- Systems must use authority checks to ensure that only authorized personnel access or use the system in any way
- Systems must use device checks to verify that data or instructions are from a proper source
- Controls must be provided over the distribution, revision, access to, and use of system documentation
- For systems where access is not under the control of those responsible for the content of the electronic records (open systems), special security measures must be provided, such as encryption

Where electronic signatures are used:

- Measures must be provide to ensure use of electronic signatures is only by genuine owners and that attempted use by others is detected, promptly reported, and requires collaboration by two or more persons
- Controls must be provided to ensure security, integrity, and uniqueness of identification e.g. username and password combinations used as electronic signatures
- Users must provide for initial and periodic testing, periodic recalls and revision, and comprehensive loss management procedures for codes and passwords
- Users must provide measures to ensure that each individual's unique electronic signature is not reused or reassigned to another and that electronic signatures are assigned only to individuals whose identities are properly verified
- If electronic signatures without biometric/behavioral links are used, two or more distinct identification mechanisms must be employed and both must be executed together at initial signing – i.e. username and password
- If electronic signatures with biometric/behavioral links are used, it must be ensured that the system design precludes use by anyone but genuine owners
- Systems must clearly display the name of the signer who signs a record electronically
- Systems must clearly indicate the purpose of each electronic signature
- Systems must clearly indicate the time and date the signature was made
- Systems must provide measures to prohibit excising (cut/copy/paste) of electronic signatures by ordinary means
- Users of electronic signatures must provide written certification to the FDA that all electronic signatures in use are the legally binding equivalent of traditional hand-written signatures

VI. Glossary of Terms and Acronyms

Audit Trail: An independent, time-stamped record of the date and time of operator entries and actions that create, modify, or delete electronic records.

Authority Checks: Determination of the authority of a system user to undertake particular actions.

BACnet: A Data Communication Protocol for Building Automation and Control Networks.

cGMP: Current Good Manufacturing Practice

Closed System: An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

Configuration Management: The process of identifying and defining the configuration items in a system, controlling the release and change of these items throughout the system life cycle, recording and reporting the status of configuration items and change requests, and verifying the completeness and correctness of configuration items.

COTS: Commercial Off-The-Shelf Software. A generally available software component for which the user cannot claim complete software life cycle control.

CPG: Compliance Policy Guide

CSV: Computer Systems Validation

Device Checks: Determination of the authenticity of a signal or command from a particular device e.g. checking a command is being sent from an authorized workstation.

Electronic Record: Any combination of text, graphics, data, audio, pictorial, or other information represented in digital format that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

Electronic Signature: 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 individuals handwritten signature.

FDA: The US Food and Drug Administration

GAMP: Good Automated Manufacturing Practice

GMP: Good Manufacturing Practice

GxP: Compliance requirements for all good practice disciplines in the regulated pharmaceutical sector supply chain from discovery to post marketing.

Hybrid System: A system utilizing a combination of both electronic records and signatures and paper-based records and hand-written signatures.

IQ: Documented verification that a system is installed according to written and pre-approved specifications.

Metadata: Definitional data that provides information or documentation of other data managed within an application or environment.

Modbus: The defacto serial communications protocol standard of the industrial automation industry.

OQ: Documented verification that a system operates according to written and pre-approved specifications throughout all specified operating ranges.

Open System: 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.

Operating Environment: Those conditions and activities interfacing directly or indirectly with the system of concern, control of which can affect the systems validated state.

PQ: Documented Verification that a system is capable of performing or controlling the activities of the processes it is required to perform or control, according to written and pre-approved specifications, while operating in its specified operating environment.

Predicate Rules: Requirements set forth in the Act, PHS Act, or any FDA regulation, with the exception of Part11. Responsible for establishing the retention period, content and signing requirements of electronic records.

QSR: Quality System Regulation

Remediation: The process by which a non-compliant system is brought into compliance**.**

Retention Period: The time for which electronic records must be kept. Often 6 years but sometimes much longer.

SNMP: Simple Network Management Protocol. A protocol used to manage network devices such as switches and routers.

SOP: Standard Operating Procedures

SOUP: Software of Uncertain Pedigree

Stand Alone System: A self-contained computer system, which provides data processing, monitoring or control functions but which is not embedded within automated equipment. A Facility Automation System falls with this GAMP definition.

System Life Cycle (SLC): The period of time that begins with the decision to develop a system and ends when the system is removed from service.

Total Environment Management (TEM): The process of establishing and maintaining a desired environmental state through the integrated monitoring and control of all events and parameters of which it is subject to change.

URS: User Requirement Specification

Validation: Establishing documented evidence which provides a high degree of assurance that a specified process will consistently produce a product meeting its pre-determined specifications and quality attributes.

Validation Summary Report: Document that describes the system, summarizes the test protocols, and discusses the results of the validation process. Approval of this document results in the system being considered to be in a validated state.

WP-TEM-US
11/05