Global Information Assurance Certification Paper

The Integration of Information Security to FDA and GAMP 5 Validation Processes

GIAC (GCIH) Gold Certification

Author: Jason Young
Advisor: Barbara Filkins

Accepted: January 26, 2015

Abstract

The validation process for information systems within the pharmaceutical industry has lagged behind others in the incorporation of information security principles into their life-cycle quality management. This is due to ambiguity within guidance on how information security is to be addressed within their governing processes. With the current validation process covering the entire information systems lifecycle using concepts like separating infrastructure from production systems or applications, these structural problems are magnified. The result is systems and processes that do not include basic principles of information security management, technical security controls or incident response to the system design and risk assessment phases of the validation process. Looking at how other regulated environments have incorporated information security into their quality management processes would be the best approach in solving this problem.

1. Introduction

In reviewing the failures of information security (InfoSec) through the lifecycle management of information systems within the pharmaceutical industry, analysis starts with the governing validation process for the qualification of information systems. Problems within this structure are driven by lack of clarity within governmental regulations, which in turn manifest themselves throughout the validation process. First, within the lexicon of the life-sciences industry, the true meaning of qualification vs. validation must be understood. A qualification focuses on whether requirements of a specific process or system can be successfully fulfilled, whereas a validation is the process of verifying all requirements have been tested within the associated qualification (ISPE, 2008). Second is the relationship of GxP (Good x Practices) relevancy to this process, where x could equal anything such as Good Manufacturing Practices (GMP), Good Laboratory Practices (GLP) or Good Clinical Practices (GCP) to ensure that the life-science regulatory requirements are met (ISPE, 2008).

Within the United States, these life-science regulatory requirements for the pharmaceutical industry are governed by the Federal Food, Drug, and Cosmetic Act Chapter V: Drugs and Devices (Department of Health and Human Services, 2012). This act is enforced by Federal Regulations Title 21 Part 11, (also known as 21 CFR Part 11) with a focus on protections to electronic records (ER) and electronic signatures (ES) (Department of Health and Human Services, 2014). These regulations are important because they provide a framework for protecting public health, assure safety and quality to products manufactured for sale within the United States. The Federal Drug Administration's (FDA) approach to creating a validation process was to defer to private industry. The recommended guidance on how to implement processes and procedures to meet these regulations comes from the International Society for Pharmaceutical Engineering (ISPE) (United States Department of Health and Human Services, 2003).

One of the reasons for this approach is the ISPE's focus is much more broad than the FDA's as it seeks to provide frameworks for creating high-quality GMP solutions that are also cost effective. The ISPE ensures that, within these processes, the goals of the

FDA are also met (ISPE, 2014.a). The process that the ISPE created to ensure quality is maintained for GxP related products is called the Good Automated Manufacturing Practice (GAMP). The current version in use right now is 5, commonly referred to as GAMP 5. GAMP 5 was created to promote a risk-based validation approach based on good practices that could meet current life-science regulatory requirements from the FDA for the pharmaceutical industry. Within the GAMP 5 structure, Good Practice Guides (GPG) provide additional frameworks to follow enabling the implementation of the GAMP 5 process for computerized systems validations (ISPE, n.d.). One example is the GPG for IT Infrastructure Control and Compliance (ISPE, 2005a) which covers the implementation and management of infrastructure computer systems.

Within the list of available GPGs, the first notable issues regarding information security are apparent. There is no GPG for information security or any security-related field, nor is its role defined within the validation process. Only 4 pages within Appendix 011 of ISPE's "*GAMP 5 A Risk-Based Approach to Compliant GxP Computerized Systems"* (ISPE, 2008) are dedicated to security management. This section only highlights a few of the areas within information security, and does not address its role structurally within an organization. For example, there is no reference to an Information Security Management System (ISMS) or Chief Security Officer (CSO), nor is their relationship to the Chief Executive Officer (CEO) covered. Instead GAMP 5 distances itself from security by referencing ISO 17799 within the introduction of Appendix 011 for guidance on Information Security Management (ISPE, 2008).

In analyzing impacts of these structural failures within the GAMP 5 process as they relate to information security, limiting the scope is necessary. This is due to the size of the life-science industry which is made up of more than just pharmaceutical companies. Fields such as genetics or zoology may suffer from some of the same issues, but they are far outside the scope of this analysis. GAMP 5 also deals with many aspects of system quality outside areas which are processed within computerized systems. For the purpose of this paper, the discussion will be limited to identifying the gaps in information security and recommending solutions to the pharmaceutical industry

regulated within the United States. Analysis is aimed at proper integration of InfoSec into the lifecycle quality management of information technology (IT) infrastructure systems and their applications that support GxP relevant processes.

To achieve this, a real-world scenario must be created to provide relevancy. This is important because many will read to this point thinking these InfoSec problems do not apply to their situation. They may feel that they have a strong information security strategy within their organization, or that it only impacts other companies. Unfortunately, this is part of the problem, as it would only pertain to their individual organization and not the community as a whole. To clarify this problem, a cloud-based solution will be presented as an example providing a basic Platform-as-a-Service (PaaS) solution. With ambiguity within mandated regulations and lack of governing processes that align InfoSec to the GAMP 5 process, it is hard to specify what level of security a cloud provider must offer. While discussing topics in which regulations provide no clear guidance, analysis will show how they may be interpreted by either the provider or the customer. Exploration will be done on whether there is a possible enforcement mechanism under the current regulations by the FDA, and whether possible recommendations for the ISPE's GAMP 5 can be given.

To recommend solutions to the problems within the GAMP 5 process for InfoSec, an alignment of the differences between the goals of quality from the ISPE and those for information security must be accomplished. This will allow for an integrated solution that contains not just information security management principles, but technical controls for cyber security and incident response as well.

2. Defining the Information Security Problem and Providing Solutions within the Pharmaceutical Industry

Obviously the ISPE did not purposefully leave out information security when creating GAMP 5, but they did not correctly define it as a critical process within their risk-based approach. The reason was their focus was on quality for GxP relevant

processes. Security was only a concern as it intersected with the requirements for data integrity within 21 CFR Part 11. This may seem foreign from a security practitioner's perspective as the community looks at things holistically with defense-in-depth in mind, but the ISPE was only looking to address risk as related to the GxP portion of a system. Looking at the differences between quality and information security within GAMP 5 as they relate to the guidance given from the FDA will help us identify the specific areas in which information security solutions can be provided.

2.1. The FDA's Role in Enforcing Information Security

Before reviewing the relationship of quality versus security within GAMP 5, the role the FDA plays in the process must be evaluated. An understanding of how data integrity is interpreted by the FDA from an InfoSec perspective is imperative in knowing how the ISPE will create a framework to protect it. Though 21 CFR Part 11 enforces the protections for ES and ER, the most important role the FDA plays is leadership. They set the tone for the industry through their audits, fines and documentation.

2.1.1. FDA Guidance on Electronic Records and Electronic Signatures

The FDA defines an ER as "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" (Department of Health and Human Services, 2014 p. 2), and an ES as "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" (Department of Health and Human Services, 2014 p. 2). When describing both ER and ES together, they are commonly referred to at ERES.

The FDA mandates that ERES have procedures and controls in place to protect its confidentiality, integrity and authenticity. This is not to be confused with the traditional confidentiality, integrity and availability (CIA) triad that is commonly referred to in the security community. Within the InfoSec community, the idea of authenticity, as with digital signatures for example, is part of integrity. The FDA splits this off due to its regulated environment for paper based processes as well as computerized systems. For

the most part, the FDA is not concerned with availability unless it impacts the quality of a product. Finally, ERES must be protected in relation to whether a system is considered open or closed. The main difference between the two is that, within an open system, the environment is not controlled by personnel responsible for the contained ERES, while in a closed environment it is. For example an outsourced system where a system administrator controls access to the GxP relevant data on a system would be considered an open system. ERES in both cases must be protected, but within an open system environment the ERES must be secured from its "creation to the point of their receipt" (Department of Health and Human Services, 2014 p. 2).

2.1.2. FDA Guidance on Information Security Management

Within the life-sciences industry, there is no guidance given by the FDA on how information security management is to be accomplished. The FDA only refers to the same ISO 17799 that the ISPE does within the GAMP 5 guide (United States Department of Health and Human Services, 2003). With this in mind, it is unknown whether the FDA considers it a conflict of interest when InfoSec reports to the IT Manager of an organization. There are no yearly requirements for InfoSec, such as those for reporting within the federal government under the Federal Information Security Management Act (FISMA), or penetration testing within the payment card industry (PCI) (United States Office of Management and Budget, 2014; PCI Security Standards Council, 2008). Again, with no mandated reporting or structural guidance for information security management, there will be nothing for auditors to request in assessing the health of an organization or system during an audit. Finally, there will be no reason for the ISPE to define, or pharmaceutical companies to employ, InfoSec measures deemed important within the security community. It would then rely on the skills of individual security practitioners that can define to management what needs to be employed to protect intellectual property, or systems within other regulated areas such as personal identifiable information (PII) within human resources.

2.1.3. FDA Requirements for Technical Security Controls

Without mandating or providing the basis for an information security management framework by the FDA, defining technical security controls is not a possibility. Without a standard to go by, how can systems be properly audited from a security perspective? For example, when trying to define protections required by the FDA to provide data integrity to ERES, there is not a lot of substance within the policy to justify large expenditures within the private sector for information security. In other words, if the FDA is not going to audit technical security controls, pharmaceutical companies will not design frameworks to employ them. Though the FDA covers cyber security for the production of medical devices, they do not provide guidance within 21 CFR Part 11 for the pharmaceutical industry. Expanding on the areas within information security that these failures have direct influence over, mainly information security management, technical security controls and incident response, will aid in understanding why the ISPE has not addressed them adequately.

When taking a closer look at the requirement to provide "authenticity, integrity and, when appropriate, the confidentiality of electronic records" (Department of Health and Human Services, 2014 p. 3) to section 11.10 (d) of 21 CFR Part 11 for "Limiting system access to authorized individuals" (Department of Health and Human Services, 2014 p. 3) the following is noted. The requirement to limit system access varies too greatly in terms of what constitutes appropriate protections without specific guidance. These protections are subject to a range of factors such as individual experience, education level or even the culture of the firm implementing the controls. As an example, one word will be used that possibly could describe several different means of limiting system access -- "encryption".

Encryption was chosen because it is only covered one time within the policy. It is mentioned as "document encryption" within the controls to be employed for a computerized system. The questions beg to be asked: Is encryption required for communications from system to system? Is data at rest (DAR) encryption required for mobile systems? Should the application data be encrypted because it is part of a platform

as a service implementation within a datacenter hosted by a third party? What about public key infrastructure (PKI) for managing Windows authentication? All these questions relate to forms of limiting access to a system as required by 11.10 (d) of 21 CFR Part 11 by using encryption. The problem is the methods are left to the judgment of the individual deciding what would constitute proper access control to the system.

An information security professional may ask themselves, how could this be left so ambiguously open for interpretation? The reason is the focus is on quality and not InfoSec. It is easy to say that there is a failure here, but this is not truly the case. In defense of the FDA, they must plan for a range of things outside of the small world of information security that would necessarily impact the quality of a product. Information security, especially as it relates to the computerized systems processing data is a very small piece to this industry's puzzle, even as critical as it may be.

2.1.4. FDA Requirements for Incident Response

Last before the discussion on the ISPE's role begins, let us address incident response. The main piece to take away from the FDA's approach to incident response is that no documentation or guidance exists on what constitute a reportable incident, or whether an incident needs to be reported. Back to the example from section 11.10 (d) that described limiting access to authorized individuals, even if there was a reporting requirement, it is difficult to determine with this guidance what constitutes a breach of access. When a company is publicly traded, they must report the incident if it involves financial data under Sarbanes-Oxley Act (United States of America 107th Congress, 2002). It is hard to imagine why, given the nature of pharmaceutical industry, there are no reporting requirements within 21 CFR Part 11 mandating disclosures to the public. This a gross failure from the FDA on reporting within the pharmaceutical industry for data breaches.

2.1.5. FDA Requirement for GAMP 5

Within the FDA's "*General Principles of Software Validation*" the GAMP 4 (now GAMP 5) is referenced for guidance in validating computer systems (United States Department of Health and Human Services, 2014). Since the FDA did not adequately

address information security within their guidance, the task fell to the ISPE. In the next section, the discussion changes focus from the FDA to the ISPE and their GAMP 5 process to see if any improvements with relation to the information security integration is present.

2.2. Information Security Gaps within the GAMP 5 Process

With the tone set by the FDA, the ISPE did not pursue stronger integration of InfoSec practices into their GAMP 5 process. Though the ISPE added a Security Management and Incident Response appendices to the GAMP 5 Guide, they are woefully inadequate in defining how to integrate InfoSec to the validation process. Even today there is still a lack of emphasis on InfoSec. At the 2014 ISPE annual conference in Las Vegas, there were no education topics for InfoSec over the five day period. Only within the data integrity discussions was InfoSec talked about, and only as it related to that specific topic. No information security vendors or consultants were present in the exhibit halls, and no key note speakers covered any InfoSec management related topics (ISPE, 2014.b). This is important because it shows that the industry still is not aware of the problem, or does not know how to address the issues of information security.

Three areas of InfoSec within the GAMP 5 process that should be integrated to the GAMP 5 risk based approach are information security management, technical security controls and incident response. These areas are critically deficient in addressing risks as they are perceived in terms of information security and, as seen when the discussion turns to the risk assessment, are compounded in their impact. This is due to the manner in which the validation process feeds the risk assessment during the validation efforts.

2.2.1. Information Security Management

Though there are two appendices within the GAMP 5 guide dedicated to incident response and security management, the ISPE fails to provide their relationship to the GAMP 5 process. Only ISO 17799 is referenced for guidance on information security management. This is a failure because the ISPE must address structurally where information security falls within an organization and how it is to be deployed within the

GAMP 5 validation process. Further, the GAMP 5 guide leads the reader to believe InfoSec is a part of IT because of the manner in which it is referred to. Within the GAMP 5 guide, InfoSec is not listed as one of the core disciplines, has no assigned responsibilities, and there are no key roles defined within the process (ISPE, 2008). This leaves individual firms with the decision on how to deploy InfoSec within their validation process. This is important because when the InfoSec team reports to the IT manager, a conflict of interest is created within the validation process.

InfoSec, within the context of providing support to a computerized system validation, should be reviewing the configuration and design of systems built by the IT department from an information security perspective. As this could affect budgetary, time lines, or functional requirements for the system, decisions may be made by the IT department that are not in the best interest of the process owner creating this conflict of interest.

Information security management is expanded on within the GPG for Infrastructure where the ISPE recommends the use of the ISO 17799 once again for the planning of InfoSec. What is good with the ISO standard is it does cover the organizational structure of information security and talks about the conflict of interest involved with IT. Unfortunately it is only a recommendation, and provides no relevancy to this standard or how it applies within their validation strategy (ISPE, 2005).

2.2.2. Guidance for Technical Security Controls

Expanding beyond the problems within managing InfoSec within a GxP environment, the relationship between data integrity, security controls, and GxP must also be analyzed. With regulations left open to interpretation by the FDA, the ISPE should have provided guidance on how to align technical security controls to the process addressing how GxP relevant items and data integrity intersect. Unfortunately there is no guidance for technical security controls integration within the ISPE GPGs or governing documentation. So, what is the impact? If there are no roles or structured process for how to manage InfoSec within the GAMP 5 process and no means to correlate security controls to policy, then typically information security is not involved. In other words,

how can quality assurance (QA), IT or the process owner be expected to make complex decisions on data integrity from an InfoSec point of view when they do not have the expertise? In short, they cannot as long as information security is excluded from the GAMP 5 validation process.

2.2.3. Incident Response Guidance

Since the FDA does not require any mandatory reporting in relation to InfoSec breaches, there is not a big focus on incident response within the GAMP 5 process. It is mentioned in a holistic manner with not much depth. The main point noticed within this methodology, is the GAMP 5 process tries to ensure that there is a corrective action and preventative action (CAPA) process for tracking critical and non-critical issues. Unfortunately no guidance on how to coordinated efforts between information security and the CAPA process is given for tracking security-related incidents. The ISPE makes the mistake of identifying the 'help desk' as the normal first point of contact for an incident. This helps to reinforce the mentality that InfoSec is an IT function (ISPE, 2008). There is however one section within the GPG for infrastructure that does support proper integration. Though small and not specific, security incident management is directly referred in the context of "problem escalation processes with increased levels of priority to ensure appropriate responses" (ISPE, Appendix 6, 2005, P4) for incident response. This is a very important section as it is the prime example of how to tackle the overall problem of the integration of security into the quality-based approach for the validation process.

2.2.4. Initiating Validation Efforts for the Qualification of a System

Leading into the discussion on InfoSec problems within a quality-based risk assessment for GAMP 5, the formal validation process must be briefly analyzed in relation to the problems found for information security management and technical controls. Within the GAMP 5 validation process, the risk assessment is dependent on the items contained within the user requirements, functional specification, system design specification, and module or unit specification with priority given to those which are GxP relevant. (ISPE, 2008). Each of these documents will be supported by a separate

qualification plan and test which is performed after the risk assessment. These primary documents vary in complexity depending on whether the system is a GAMP category 3, 4 or 5 System. For example a category 3 is a non-configured product which only requires the completion of user requirement prior to proceeding to the risk assessment, while a category 5 system is one which employs the use of custom code, requiring the system to necessarily go through code reviews and a much more extensive validation process.

In verifying a system according to this validation process, traceability is applied. This means that all items identified during the requirements and specifications portion of the validation are traced through the life-cycle of the system. This is a core principal within GAMP 5 and is used for identifying items through every stage of the process. GxP-related items are identified as well within this traceability for classification during the risk assessment process. From this point on in the validation process, there are no large holes related to information security. Instead, the process suffers from the GIGO, or "garbage in, garbage out" principle.

2.2.5. Risk Assessment Failures

In continuing the GIGO topic in relation to traceability from the previous section, it is understood that the GAMP 5 process is completely dependent on the information contained within the requirements and specifications documentation that have been created. If the risk assessment based on these inputs is not incorporating information security correctly, with no strategy for correlating InfoSec technical controls to GxP relevant quality controls, the risk will not be assessed appropriately. What is being said here is that, through traceability, only items that were identified in associated requirements or specifications documentation will be included in the risk assessment. This highlights the failures within the GAMP 5 validation process as it relates to information security. The FDA may not have addressed InfoSec appropriately within 21 CFR Part 11, but they did reference ISO 17799, which left the ISPE to address it. Therefore, this is a failure within the ISPE to adequately address the role that InfoSec plays in the validation process. It gives process owners a false sense of security when they receive a qualified system according to the current GAMP 5 validation model. This

is important because critical GxP and non-GxP related items are identified within the risk assessment to be tested during the qualification phases. If InfoSec items are not contained within this portion of the validation, there will be no requirement for them to be tested or results recorded.

2.2.6. Types of Qualifications and their relation to InfoSec failures

In performing the qualification testing according to the GAMP 5 validation process, GIGO continues to structurally undermine the perceived risk of the system. The types of qualifications are generically broken down into installation qualification (IQ), operational qualification (OQ), and performance qualification (PQ) (ISPE, 2008). The process ensures that qualifications are done in the reverse order of documentation they will be validating. For example, the IQ will be qualifying that the system meets all requirements or "performs" according to the system design specification first since it covers the system installation and infrastructure controls. Traceability continues to be important as all issues identified to be tested within the risk assessment are performed here. Using the encryption example from earlier, the process tests this control as follows.

First, the IQ will be performed. The IQ will test the functionality of the system according to the requirements from within the systems design specification. These requirements may include the installation guide for the operating system and/or application installation documentation. This would test that the software providing the encryption was installed correctly. The next qualification to be performed would be the OQ. The OQ ensures the software operates according to the functional specification. This would now test that the encryption software operates according to the functional specification using test accounts. Last, the PQ would not necessarily test the encryption method itself, but test that the user can log on via the encryption method without interfering with the intended use of the system according to the user requirements documentation.

The GAMP 5 process for testing items from the risk assessment within the appropriate qualification is a very thorough and well defined process. Its ability to provide traceability for requirements and specifications from the risk assessment by

identifying items to be tested within the qualification efforts is outstanding. It could be a perfect platform for the integration of InfoSec controls if the underlying foundational alignment is created.

2.2.7. Hazards in Splitting Application from Infrastructure or 'Platform' Qualifications

In setting up the real world scenario for analysis, one particularly common method of performing validations is at odds with the principles of information security and must be discussed. When infrastructure platforms or underlying operating systems are separated from their applications for validation efforts, it creates a complex environment with barriers for InfoSec. What this means is, if a firm wants to install a software application that performs a specific GxP related function, they will not perform a validation on the entire system, they will only perform it on the application. This is done when the application is installed on a "qualified platform". This means that the underlying system or infrastructure was already qualified according to the GAMP 5 validation process. More specifically, the GPG for infrastructure states that the "validation applies to those GxP applications that run on the IT Infrastructure rather than the IT Infrastructure platforms themselves, where the focus should be on qualification of components" (ISPE, 2005, p.13).

Defense in Depth principles and information security management create an environment where InfoSec practitioners look at systems in a more holistic view. This is due to the manner in which risk is applied from an information security perspective where all things are related and can impact one another. So in the case where an application is installed on a qualified system under GAMP 5, priority will be given to the application due to the manner in which the GxP relevancy is calculated. This means that the underlying qualified platform is referenced within the system design documentation, and any changes may be noted within the change control process.

This might be compared this to a baseline for a server, but that would be incorrect. A baseline is a starting point in which basic security and configurations are incorporated into a system, while a qualified platform is a finished solution that includes

all security controls and configurations for a system that would be implemented by an organization. From a security perspective, how can any security requirements or technical controls to an application be created without placing a priority on the underlying system for providing these protections? There is no standards or examples for this scenario within the GPSs in relation to InfoSec to assist. Within the InfoSec community however, best business practices support defense in depth methodologies where overlapping defenses are created and monitored to provide security. This is all done in concert with the application to provide security to the entire organization and not just a single system or application.

2.2.8. Impacts of Cloud Based Solutions

Within the context of the PaaS example cited earlier, what are the impacts of the previously discussed gaps? In this scenario, our task becomes more complicated as the process owner may have control of the application, but the service provider controls the underlying hardware, operating system and supporting infrastructure.

First, a decision must be made as to the type of system to be validated. Is this an open or closed system? To answer this question, the definition of what the FDA considers a system must be evaluated.

> "a functional unit, consisting of one or more computers and associated peripheral input and output devices, and associated software, that uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program; executes user-written or user-designated programs; performs user-designated data manipulation, including arithmetic operations and logic operations; and that can execute programs that modify themselves during their execution. A computer system may be a stand-alone unit or may consist of several interconnected units" (United States Department of Health and Human Services, n.d.)

The main point within this definition in the context of cloud computing is storage. If storage is considered a common asset that covers several interconnected computers, then how is that impacted within the cloud environment? For example, the argument

could be made that within this environment storage includes the hypervisor, storage area network (SAN), random access memory (RAM), the virtual host operating system, host applications, associated mirror site, and virtualized network equipment. This is further complicated when it is realized that shared memory is used with other tenants on the same hypervisor. These tenants may work in other industries that may be less than favorable to the environment in which a pharmaceutical industry computerized system should be deployed.

As to the question of open or closed system, the FDA does not define what controlled system access is in regards to a cloud environment. For example the service provider's administrators have access to the underlying infrastructure which includes the hypervisor and associated virtual host system, but not necessarily the application in a PaaS architecture. Does simply creating a service level agreement (SLA) defining when an administrator can access the application cover this? How is this impacted when the application is covered in a separate qualification because the PaaS solution was provided as a qualified infrastructure? Again there is no guidance from the FDA or the ISPE for this type of scenario.

This cloud-based scenario highlights risks associated within the GAMP 5 validation process. These risks and gaps will now be expanded upon within the discussion of a fictitious PaaS implementation by a typical cloud provider.

2.3. Real World Cloud-Based Scenario

To better understand how these issues impact a real world system installation, an example is defined to further cover main information security failures discussed within the GAMP 5 process for a computerized system validation. A pharmaceutical company called Pharma-X whose main customers are in the United States is outsourcing their critical GxP enterprise resource planning (ERP) system called ERP-Y to company Cloud-Z's datacenter. The ERP system will be installed within Cloud Z's PaaS offering as a means to reduce costs and improve efficiency within the organization. Both management and the quality assurance department is excited about this new implementation because

the application is to be installed on the service provider's "qualified" infrastructure, reducing work, time and costs to validating the system.

Cloud-Z's approach to their PaaS is to include the basics of what is covered within the GAMP 5 process. This provides a standardized method for supporting pharmaceutical clients and creates a great platform for marketing. Their main and hot backup facilities are located in Dublin, Ireland. Customers from Pharma-X access their facilities mainly from the United States and Germany.

Technically the datacenter uses a standard configuration employed today by most facilities with the exception of its qualified datacenter and infrastructure systems for the use of pharmaceutical customers. (To ensure that the analysis stays focused on the GAMP 5 process and not specific products or vendors, no specific names will be mentioned on the types of technology.) This equipment boasts the latest in virtual firewalls and switches within their environment that manages the hosts via the hypervisors. The main and hot sites are approximately 10km apart with a dedicated fiber line between them and a backup line provided by an external provider. This enables the SANs to operate seamlessly in maintaining full redundancy.

2.3.1. Defining the InfoSec Problems Within the ERP Solution

Simply defining the system type will be a difference of perspectives from the quality assurance department and InfoSec. In defining whether this PaaS implementation is an open or closed system, QA will likely support the case that it is a closed system since only the application is being qualified. This separation also allows QA to maintain the illusion that only those responsible for the ER have control access to the environment. Another reason for performing the validation in this manner is it enables Pharma-X to maintain the "closed system" status to reduce the amount of effort involved in building the system. Implementing protections for ER from its creation to the point of receipt may prove to be cost prohibitive and, in some cases, not technically possible for some PaaS solutions.

From an information security perspective, a cloud-based solution must be an open system as the customer has no means available to control access to the system or data

contained within. To clarify this statement further, if the cloud provider has administrative access to the hypervisor and host operating systems, then Pharma-X cannot control their access to the application from the underlying system.

2.3.2. Separation of the Qualified Infrastructure From the Application

Beyond the debate on whether the system is open or closed, the separation of the infrastructure and application within this PaaS environment will cause drastic differences between the results of a risk assessment based on either the traditional GAMP 5 quality-based model, or a traditional InfoSec-based approach to risk assessment. To justify this stance, imagine how the underlying system may be been qualified along with the datacenter qualification. Even if Pharma-X has a mature InfoSec process that has been integrated, as was stated earlier, they are now dependent on the cloud provider's interpretation of information security in the GAMP 5 process.

Think of this in the terms of the FDA's requirement for access control. Since access control is defined so ambiguously by the FDA and ISPE, what exactly does it mean in this case? Further, what are the impacts when the GAMP 5 process only tracks GxP-related items to the application within its validation process? Will the impacts of access control even be checked for the underlying operating system or hypervisor? Will there be a review of the documentation from the Cloud provider's qualification to ensure that it is acceptable? This example shows where the rubber meets the road so to speak. It gives a specific example of the many ways in which one control can be interpreted. How could access control be appropriately implemented or audited according to the 21 CFR Part 11 to assure quality? The bottom line is, there is no way to assure the quality of a risk assessment provided by the cloud provider using the GAMP 5 process.

Within the discussion of this scenario, a few other areas that will be impacted more than others will be highlighted. Though changes to regulations are needed from the FDA, clarification rather than new policies should be emphasized. This is because most of the failures are process- or procedure-based and should be addressed by the ISPE within GAMP 5 coordinated with support from the FDA.

2.3.3. Virtual Host Management

Within the system design of the underlying operating system, there is no control or oversight to Cloud-Z's configurations. Imagine the scenario where Cloud-Z builds virtual hosts by copying other hosts from within their datacenter. This could be an excellent way of providing a stable base-lined system with cost savings every time, provided that the copied host is a documented and managed system designed for this purpose. Now imagine this copied server came from another customer from within the datacenter with partial configurations and production data. The problem to be noted here within these two scenarios is that the method for deploying the PaaS underlying operating system is based on trust. There is no way to check this and further, within the current GAMP 5 process, this requirement would not be addressed unless a proactive security professional was looking out for the company.

This line of thought can also be applied to the patching and systems maintenance as well. Service level agreements can be put in place, but they do not provide a means to verify that the checks have been done.

2.3.4. Issues Within the Hypervisor

Moving from the host operating system to the hypervisor, there is even less control and guidance. How are the technical challenges or administrative management of the hypervisor to be incorporated to the GAMP 5 validation process for this situation? This is important because the host systems saved within the hypervisor are not just vulnerable to technical exploits from outside, but from administrative abuses inside as well. When these exploits have been realized against certain types of hypervisors, the host systems can be extracted in their entirety. If snapshots were taken for example, the contents of RAM are also available for extraction. Shared memory and networking resources of the hypervisors needs to be addressed as there are multiple exploits to guard against. There is an entire discipline around the implementation of virtualized infrastructure. Given the challenges on how it is to be treated and the size of the problem within the GxP environment, the ISPE needs to address this within its processes.

2.3.5. Networking Challenges

Still part of the hypervisor, but outside of the system, the next area to discuss would be the local area network (LAN). The LAN will be a mix of virtual and physical equipment at the datacenter location consisting of the connected physical switches and the virtual network provided by the hypervisor. The main issue within the LAN is access control. The initial question is, what is on the LAN? Is it shared with other host systems from other customers? If it is shared, what protections are in place for these other systems? In other words, can a user access another system within the same LAN? Is the management to the hypervisor on this same LAN as production or is it separated? If it is separated, is it accessible to all systems management interfaces? Who manages the internal firewall for the system, and ensures there are no conflicts with the new application installed by Pharma-X? These questions focus on access control, which is mandated by the FDA, but there currently is no guidance on how to address it in this environment. This why the ISPE should become more proactive in defining these relationships between installations on qualified platforms within a cloud environment.

External access and perimeter defenses are also important when discussing these solutions. The most important reason why is due to the added risk of accessing an application that is available from the Internet. The GAMP 5 process does not address this, and it must. There is no guidance on how to implement appropriate access control rule sets to perimeter devices such as firewalls. The process does not tackle the complexities involved with comingling of data that may come from implementation of virtual firewalls and network systems. For example, when the customer Pharma-X implements their new application on the hypervisor, how are the ports and protocols for this systems application to be addressed by Cloud-Z? This should be an important part of any service level agreement, but it should also be addressed within the GAMP 5 validation process as well. Beyond the perimeter, guidance is also needed to ensure end-to-end encryption from the customer to the virtual host located on the hypervisor to protect data in transit. The fear is, all of these items contained within the context of network security will not be addressed sufficiently due to the nature of installation on a qualified platform.

2.3.6. Security Administration

With regards to security administration and monitoring, a different set of problems emerge from this scenario due to a coordinated effort that must exist between the cloud provider and the customer. For example what exactly needs to be monitored? This is something that would necessarily need to be coordinated from Pharma-X to Cloud-Z within a PaaS implementation. Guidance is needed, and specific examples should be given by the ISPE on how to handle these situations. More importantly is how it impacts incident handling, what needs to be reported as an incident, and how it is to be reported. How is the security administration impacted when infrastructure services such as Active Directory are extended to the host system to provide authentication to the application? What technical and procedural measures should be put in place for these situations?

In short, implementing a solution within the cloud environment as is currently done by the pharmaceutical industry has a significant amount of risk if not done correctly. Even with the implementation of new information security standards and procedures, correcting mistakes from years of faulty implementation of computerized systems within this environment will be difficult.

2.3.7. Gap Analysis Summary

Prior to discussing overall solutions, a summarization of gaps found during the analysis is appropriate. This is important because it is not a single failure attributed to a single organization, but a systematic failure of integration throughout the entire validation process across many companies. Beginning with 21 CFR Part 11 regulations at the FDA and ending with the GAMP 5 process qualification testing, there are several specific areas where gaps to information security have occurred.

1. There is no recognition of the problem of InfoSec integration from both the FDA and ISPE. Currently this is not seen as an industry issue, nor are any attempts at correcting the problem apparent.
2. Though critical items such as access control have been identified, there is a lack of clarity within regulations from the FDA with regards to InfoSec. There

is also no enforcement mechanisms currently in place for technical information security controls.

3. No annual reporting requirements from the FDA for the industry in the area of InfoSec like those in other industries to ensure basic compliance.
4. No mandated reporting from the FDA on security breaches or guidance to what constitutes a breach.
5. FDA auditors are not trained to understand and see risks as they pertain to information security.
6. The field of information security is not identified as a critical process within GAMP 5 with no defined critical roles.
7. No method of integrating technical and procedural security controls are available for the current risk assessment in the GAMP 5 validation process.
8. No methodologies to apply technical security controls and information security principles to qualified platforms and cloud environments for applications to be validated is available.

2.4. Providing Solutions

Providing solutions to the gaps identified within the GAMP 5 process in relation to security is the most important step in this analysis. Rather than approaching this as a broken process that needs to be re-built from an InfoSec perspective, areas must be found where InfoSec can insert its processes into existing ones. This is important because regardless of whether security becomes a core component of the GAMP 5 process, the goals of GAMP 5 must remain the same. A more proactive approach is to try and align the goals of InfoSec with quality at the beginning.

2.4.1. FDA Guidance

The FDA needs to do more to address InfoSec guidance on how to employ protections to ERES and they should provide qualified auditors that understand information security. The FDA itself must conduct a security test and evaluation (ST&E) for all systems according to the HHS Certification and Accreditation Guide (Department of Health and Human Services, 2005). The FDA also uses the National Institute of

Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems a Security Life Cycle Approach* (National Institute of Standards and Technology, 2010). These standards and guidelines answer the questions to the issues described throughout this analysis when directed at the FDA internally. This is why the FDA must provide similar guidance to the life-sciences industry either directly or through working with the ISPE to ensure information security is maintained throughout the life-cycle management of information systems.

For example SP 800-37 Task 2-2 requires the selection of security controls for the information system. It also requires that they must be documented in the security plan (National Institute of Standards and Technology, 2010). How is this important? Well the FDA could mandate a similar version of this within 21 CFR Part 11 regulation. Another example would be a directive such as the one used by the United States (US) military for the use of approved cryptography within directive 8500.2 (United States Department of Defense, 2003) would cause the industry to create a process for implementing it. The ISPE in the end would be forced to address the problem of both how information security management is to be accomplished, and how the technical security control alignment is to be done.

The FDA should also establish yearly reporting requirements for InfoSec. These yearly requirements should follow the examples given within PCI. Yearly penetration testing or vulnerability assessments should be mandated with reporting to the FDA. Security related incidents should also be defined with how to report them to the FDA. The FDA should follow this up with a mechanism to report this to the public for general awareness.

2.4.2. Integrating Information Security Management

Guidance for solving the issue of how information security management is done within the life-sciences industry must come from the ISPE. In solving the problem, looking at how other industries have approached this problem is an essential first step. Referencing standards as they did within GAMP 5 does not solve the problem, they must

address how the structure within these separate standards interface with the GAMP 5 validation process.

In looking at other best business practices, points of intersection can be found to address the dilemma of quality vs security. Within the pharmaceutical industry, an unofficial role has taken hold within some organizations that is not described within the GAMP 5 process. This role is the Validation Manager (VM). The VM is sometimes filled by a subject matter expert (SME), someone from quality of the organization or the governance branch within IT. The important thing about this role is that it closely resembles the Information Assurance Manager (IAM) from the US Army. What is important about the IAM role that could be learned? The first is that the IAM does not report to IT or Quality Assurance. They perform InfoSec duties according to the best business practices for InfoSec within the DoD. The second reason is the IAM has an information systems security officer (ISSO) to help with the more technical areas that they may need assistance with.

Take these two important attributes and apply them to the pharmaceutical industry. Keep in mind that a common problem existing outside the world of InfoSec is that IT and QA do not communicate effectively. This could be a point of insertion for InfoSec. What is meant here, is that the process of validating systems design is currently done by either someone from QA or IT. In this situation you either have someone not qualified to review technical configurations, or a conflict of interest because it is being reviewed by the person who designed it. The bridge between the two is information security. InfoSec analysts understand policy and technology by the nature of the trade. Taking this into account, Validation Managers should be made full time InfoSec positions within information security management. This of course will not work unless information security is broken off and structured the under the CSO as defined within ISO 17779. This would have to be backed up with official roles and processes created and supported by the GAMP 5 validation process. This small but important change to the roles in the process will cause sufficient change to lead in to correcting the next issue.

2.4.3. Creating a Technical Security Control Framework

If the main criteria for applying security within the life-sciences industry is contained within data integrity, then that is where the technical framework should focus its efforts. Data integrity is currently made up of quality controls for accurate, attributable, available, complete, consistent, contemporaneous, enduring, legible, and original data (Schmitt, 2014). Creating a methodology to apply security controls to different subsets of data integrity would be an initial way into correcting the problem. This allows changes to occur without effecting the way the current process is being completed.

First and foremost, the creation of a GPG for InfoSec needs to be created to address these methodologies. These do not have to be as detailed as Security Technical Implementation Guides or STIGS as they are commonly referred to in the DoD, but they should provide an adequate roadmap to address the problem of applying information security controls to policy items directed from the FDA. They should focus more on the process of applying information security within the GAMP 5 model. Secondly, there needs to be a GPG created for cloud security. This GPG should not focus purely on security, but attempt to address the challenges that many companies struggle with implementing cloud-based systems. Security should be addressed as an appendix with specific guidance on how to tie it in to the GAMP 5 process.

Last, issues surrounding the installation of applications on qualified systems must also be addressed. A methodology should be created within the GPG for information security as to how cross-platform InfoSec should be applied and tracked in conjunction with other qualified systems. This process must leverage the existing CAPA and traceability process within GAMP 5.

2.4.4. Cross Referencing the Information Security Risks with GxP Risks Through a Formal Risk Assessment Process

Due to the nature of InfoSec risks and their ability to span multiple platforms, like GxP risks, they should be given a higher priority than non-GxP items within the risk assessment process. The methodology should closely resemble that used to identify GxP

relevant risks to align the process and limit confusion. It should also provide an overall picture of risk that involves InfoSec and the traditional GxP related quality risks side by side. This will make the risk assessment more complex, which reinforces the idea using an information security analyst as the Validation Manager.

This methodology should modify the approach used for GxP items where risk classes are decided by (probability x severity) and risk priorities are defined by (detectability x risk class). This approach generates a numeric value to be used for quickly identifying risks as seen in figure 1.

		Probability		
		Low	Medium	High
Severity	High			9
	Medium			
	Low			

		Detectability		
		High	Medium	Low
Risk Classes	1			9
	2			
	3			

Figure 1. Risk Matrix

Using the example in Figure 1, if an encryption control used has a high probability with a high severity rating plus a high risk class with a low detection rate, the matrix would calculate the highest number on the risk scale. This would be overall risk of 18, calculated by high probability (3) x high severity (3) added to the risk class 1 (3) x low detection rate (3) or (3x3) + (3x3) =18.

Using this approach for assigning risk to specific InfoSec items would be the function of the VM and should be documented as such within the GAMP 5 process. If clear guidance was given on the importance of the distinct role that InfoSec plays in the process, many of the technical issues would resolve themselves through the inclusion of a methodology that supports this InfoSec integration. To be more clear, and using the original encryption example for access control, a numeric value within the risk assessment would be assigned to that individual control to provide a realistic picture of its risk to the system. The end product would have three areas of risk evaluated: non-GxP, GxP relevant and InfoSec relevant. The purpose of identifying the GxP relevant and

InfoSec relevant controls in this fashion facilitates two important aspects of risk. First, it allows items which are both GxP and InfoSec relevant to be given a higher priority than those that are only in one category. Second, it would give the ability to identify those risks that span multiple platforms enabling the inclusion of defense in depth principles to be applied to the methodology.

2.4.5. Creating the Atmosphere for Information Security Inclusion

As was apparent during the 2014 ISPE conference in Las Vegas, InfoSec was not a priority within the GAMP 5 community. This is something that must change to generate interest in addressing the problems and solutions that have been presented throughout this analysis. Workshops, marketing, sales events and InfoSec demonstrations are desperately needed to educate the target audience. When talking about these workshops or InfoSec events, the target audience is the most important piece. Security practitioners must learn the GAMP 5 processes, jargon within the industry, and how they can make information security a relevant to support important processes for the products the pharmaceutical industry is producing. Understanding ways to integrate these important principles to the pharmaceutical industries solutions is not something that can be learned or supported quickly.

Efforts should not only target the ISPE and their events, but should also include educational efforts with the FDA. The FDA has the best platform for disseminating this type of information, whether it is a regulatory requirement or only a recommendation. From this perspective it is imperative that the FDA starts to prepare its pharmaceutical base for any new regulations that may come in the future. With an industry as large as the pharmaceutical industry, changes are slow to come, and even slower to be implemented. This is due to the trickle-down effect of changes coming from the FDA to the ISPE and finally at the corporate level for many of the larger pharmaceutical companies.

3. Conclusion

In summary, it is apparent that the failures relevant to information security within the validation process for the pharmaceutical industry are going to take a collaborative effort between the FDA and ISPE. With the core of this problem being more process based than regulatory, the ISPE will have to take the lead on creating the methodologies, while the FDA sets up the environment for enforcement. Other industries like PCI are incorporating drastic changes to their information security policies due to the environmental changes that have occurred within the last few years. It is understandable that these changes will be coming to the pharmaceutical industry as well, but it is irresponsible to wait until the last minute and try to make too many changes at once.

When looking at the problems that exist, it seems strange that such small changes in the structure of how GAMP 5 is currently implemented would be so successful. This is because the structure of GAMP 5 is a good one, it is only missing some of the principles of InfoSec at the core of its processes. If the problems are addressed and supported by clarity to regulations from the FDA, the problem will solve itself over time.

4. References

ISPE (2014.a) *About Us*. Retrieved December 18, 2014 from http://www.ispe.org/about-ispe

ISPE (2014.b) *ISPE Annual Meeting Schedule-at-a-Glance*. Retrieved December 18, 2014 from http://www.ispe.org/2014-annual-meeting/schedule-at-a-glance

ISPE (2008) GAMP 5 A Risk-Based Approach to Compliant GxP Computerized Systems. Tampa: ISPE

ISPE (2005). GAMP Good Practice Guide: IT Infrastructure Control and Compliance. Tampa: ISPE

National Institute of Standards and Technology. (2010) *NIST Special Publication 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems a Security Life Cycle Approach*. Retrieved November 21, 2014, from http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

PCI Security Standards Council. (2008). *Data Security Standard (DSS), 11.3.* Retrieved December 18, 2014, from https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf

Schmitt, S. (2014) Data Integrity –FDA and Global Regulatory Guidance IVT Network Institute of Validation Technology. Retrieved December 18, 2014 from http://www.ivtnetwork.com/article/data-integrity-fda-and-global-regulatory-guidance

United States Department of Health and Human Services. (2012) *FD&C Act Chapter V: Drugs and Devices.* Retrieved November 30, 2014 from http://www.fda.gov/regulatoryinformation/legislation/federalfooddrugandcosmeticactfdcact/fdcactchaptervdrugsanddevices/default.htm

United States of America, 107th Congress, (2002). *Public Law 107–204 - JULY 30, Sarbanes-Oxley Act of 2002.* Retrieved December 18, 2014, from https://www.sec.gov/about/laws/soa2002.pdf

United States Department of Defense. (2003). *Department of Defense Instruction, number 8500.2, Information assurance (IA) implementation*. Retrieved November 21, 2014, from http://www.cac.mil/docs/DoDD-8500.2.pdf

Jason N. Young, jason.n.young@silverbulletsecurity.com

United States Department of Health and Human Services. (2002) *General Principles of Software Validation; Final Guidance for Industry and FDA Staff*. Retrieved November 21, 2014, from http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085281.htm

United States Department of Health and Human Services. (n.d.) *Glossary of Computer System Software Development Terminology (8/95).* Retrieved December 17, 2014, from http://www.fda.gov/iceci/inspections/inspectionguides/ucm074875.htm

United States Department of Health and Human Services. (2003) *Guidance for Industry Part 11, Electronic Records; Electronic Signatures — Scope and application.* Retrieved November 21, 2014, from http://www.fda.gov/downloads/RegulatoryInformation/Guidances/ucm125125.pdf

United States Department of Health and Human Services. (2005) *Information Security Program Information Technology Security Test and Evaluation Guide.* Retrieved November 21, 2014, from http://csrc.nist.gov/groups/SMA/fasp/documents/c&a/HHS_Security_Test_and_Evaluation_Guide_08242005.pdf

United States Department of Health and Human Services. (2014) *Title21--Food and Drug Chapter I—Food and Drug Administration Department of Health and Human Services Subchapter A – General Part 11 Electronic Records; Electronic Signatures.* Retrieved November 21, 2014, from http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1

United States Office of Management and Budget. (2014) *Annual Report to Congress: Federal Information Security Management Act.* Retrieved December 18, 2014, from http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy_2013_fisma_report_05.01.2014.pdf

Appendix A: Acronyms

Acronym	Description
CAPA	Corrective Action and Preventative Action
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
CIA	Confidentiality, Integrity and Availability
CSO	Chief Security Officer
DAR	Data at Rest
DoD	Department of Defense
ER	Electronic Record
ERES	Electronic Signature Electronic Record
ERP	Enterprise Resource Planning
ES	Electronic Signature
FDA	Federal Drug Administration
FISMA	Federal Information Security Management Act
GAMP	Good Automated Manufacturing Practice
GCP	Good Clinical Practices
GIGO	Garbage in Garbage out
GLP	Good Laboratory Practices
GMP	Good Manufacturing Practices
GPG	Good Practice Guide
GxP	Good (x) Practices
HHS	Health and Human Services
IAM	Information Assurance Manager
InfoSec	Information Security
IQ	Installation Qualification
ISMS	Information Security Management System
ISSO	Information Systems Security Officer

Acronym	Description
ISO	International Organization for Standardization
ISPE	International Society for Pharmaceutical Engineering
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OQ	Operational Qualification
PaaS	Platform as a Service
PCI	Payment Card Industry
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
PQ	Performance Qualification
QA	Quality Assurance
RAM	Random Access Memory
SAN	Storage Area Network
SLA	Service Level Agreement
SME	Subject Matter Expert
SP	Special Publication
VM	Validation Manager