A Comprehensive Information System Validation Model

Kyungsub Steve Choi

Computer Information System Department, School of Business
Manhattan College, Riverdale, NY 10471 U.S.A
Tel: +1-718-862-7309, Fax: +1-718-862-8032, E-mail:kyungsub.choi@manhattan.edu

Abstract

Along with the significance of information systems in today's global business operation, the significance of information systems control and audit is ever increasing in the effort to secure accuracy and integrity of vital business data. A study is undertaken to integrate Food and Drug Administration computerized systems validation regulations, Securities & Exchange Commission Sarbanes-Oxley Act of 200 and other significant regulations, and lastly, People Capability Maturity Model into one comprehensive information system validation model. The initial benefits to this comprehensive model are convenience, time-saving, and synchronization of the regulations. An organization that is striving for a high level of quality system in its essential operating areas of organization may opt for this model. After the complete development of the model, a field test would be scheduled to test its efficacy and validity.

Keywords:

Validation, Quality System, P-CMM, Computerized System, Quality Model.

1. Introduction

Regardless of what type of field, information systems have become the key business enabler for many prominent organizations. Among the many factors underpinning this information systems success, the category of quality probably receives the least attention. Compare to the bells and whistles of new technology in information systems, the quality aspect has us looking back to the practices of controls and measurements.

In this paper two U.S. federal agencies, the Food and Drug Administration (FDA) and the Securities and Exchange Commission (SEC) are presented with their validation and quality control practices on information systems. We will explore the attributes of their regulations on information system quality control which is the manifestation of their information system validation philosophy. Added to this is the People Capability Maturity Model (P-CMM) [1]. P-CMM is an instrument for organizations to efficiently control their human resources. The combined effort of these three entities' information system validation and human resource control will allow us to carefully formulate a new "one stop" information system validation model.

2. Practices in Food and Drug Administration

The FDA currently regulates organizations and manufacturers that produce or are involved in producing the following: food products, drug products, medical devices, biologics, animal feed and drugs, cosmetics, radiation-emitting products, and combination products (http://www.fda.gov). Like as other business organizations, many of these organizations or manufacturers use their proprietary information systems for their business objectives. Because their end-products deal with public health, the FDA aggressively enforces quality control and maintenance on their business and manufacturing operations.

It is the FDA philosophy that the level of product quality is greatly influenced by the quality system that an organization exercises on its information systems [2]. Complying with this philosophy, the regulated organizations and manufacturers must validate their quality system. The focal point of the quality system is the information system or in FDA's terms, the computerized system. The FDA's definition of validation on the computerized system is "*the confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through the software can be consistently fulfilled*" [3]. The key phrases from this definition are "objective evidence," and "consistently fulfilled." Representing the American public in protecting every American citizen's health, the FDA will stretch the limit in assuring the safety and efficacy of food and drug products.

The FDA's philosophy is manifested in many of its regulations. The major ones are:

- FDA, Guide to Inspection of Computerized Systems in Drug Processing
- FDA, Guidance for Industry: Computerized Systems Used in Clinical Trials
- FDA, Guide to Inspections of Quality Systems
- FDA, Guideline on General Principles of Process Validation

- FDA, 21 CFR Part 11, Electronic Records; Electronic Signatures; Final Rule.
- FDA, Guidance for Industry: General Principles of Software Validation

We will explore briefly each regulation to understand the FDA's audit approach. The Guide to Inspection of computerized systems in drug processing poses questions on auditing the drug manufacturing plant. The hardware questions are: 1) Does the capacity of the hardware match its assigned function? 2) Have test conditions simulated "worst case" production conditions? 3) Have hardware tests been repeated enough times to assure a reasonable measure of reproducibility and consistency? 5) Has the validation program been thoroughly documented? 6) Are systems in place to initiate revalidation when significant changes are made? For software, the questions are; 1) Does the program match the assigned operational function? 2) Have tests been repeated enough times to assure consistent reliable results? 3) Has the software validation been thoroughly documented? 4) Has the software validation been thoroughly documented? 5) Are systems in place to initiate revalidation when program changes are made?

The most recent and outstanding regulation is Electronic Records; Electronic Signatures; Final Rule [4]. As more organizations migrate from the pencil-and-paper mode to the digital format, this regulation establishes a standard for which electronic records and signatures that can be utilized by organizations. The regulation covers controls for both open and closed systems, signature manifestation, and signature/record linking or audit trail. Among these areas, the most challenging area is the audit trail capability. It requires the electronic records to show who created the record, when was it created, if it was modified, what was modified, who modified it, when was it modified, and why was it modified. All these questions must be clear and accessible for an outside auditor.

As the software complexity level grows in par with the exponential business growth level today's software products challenge us in the areas of software development, implementation, and maintenance. The Guidance for Industry: General Principles of Software Validation regulation probes deeper into the software validation topic. Although the FDA does not prefer any particular software development model, many pharmaceutical companies exercises the waterfall model [5]. From the FDA's perspective, the typical activities in the waterfall model are quality planning, systems requirements definition, detailed software requirements specification, software design specification, construction or coding, testing, installation, operation and support, maintenance, and retirement. All the documentations that arise from each activity must be kept, preferably in a digital format, and made to be accessible.

Addressing the commercially-off-the-shelf software products, the FDA exempts major validation activities requirements from organizations. The organizations are only required to have functional testing documentation and evidence on the research activity of known software limitations, problems, and defect corrections. Examples are known spreadsheet applications such as Microsoft Excel or databases such as Oracle.

Many tend to forget or overlook the fact that both training personnel and standard operating procedures (SOPs) are equally important areas. The end-users or operators are integral parts of the system. Ensuring their system knowledge and standardizing their system use are essential requirements in meeting a high quality level. Securing proper and complete personnel training documents and availability of all required SOPs are additional auditing items.

Lastly, the FDA will evaluate if an organization has an in-house quality system that oversees and directs all the quality-related activities. Such as quality system must be in place to assure the quality system.

3. Practices in Securities and Exchange Commission

The less stringent, in general approach of the Security Exchange Commission (SEC) in the inspection and audit of financial systems has undergone a sharp change in recent.

Besides the Enron case [6], other corporate accounting scandals had U.S. government to act in more formal manner by stipulating the Sarbanes-Oxley Act of 2002 [7]. The name comes from two U.S. congressmen, Senator Paul Sarbanes and Representative Michael G. Oxley who proposed the legislation. The Act affects all accounting transactions by entities such as public company boards, management, and public accounting firms. The act also addresses in detail the high level of moral responsibilities expected of these entities and mandates the SEC to implement and enforce the Act.

From the 12 provisions of the Sarbanes-Oxley Act of 2002 (hereafter SOX), the more notable provision is *"a requirement that public companies evaluate and disclose the effectiveness of their internal controls as they relate to financial reporting, and that independent auditors for such companies "attest" (i.e., agree, or qualify) to such disclosure"* This provision is very similar to the spirit of FDA regulations. In dealing with the information technology audit, the SEC refers to following entities;

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- Control Objectives of Information and Related Technology (COBIT).

A private-sector initiative, the objective of COSO is to detect the possible causes of the fraudulent financial

reporting. COSO provides a framework of eight interrelated components: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. Based on these components, organizations may plan and develop their own quality control infrastructure. The framework is active and live. In other words, the framework may be updated according to changes in general accounting practices. Additionally the SOX key phrase, *"internal control"* is achieved in the categories of effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

As COSO offers instruction for setting up an organization's quality system, COBIT offers guidelines in information technology compliance. COBIT allows an organization to be in compliance with SOX, relating to areas in general information controls, application controls, real-time disclosure, records retention, and spreadsheet controls.

4. Comparative Analysis

In comparing the practices of the FDA and the SEC, there are differences in experiences in regulating its respective industry, the enforcement entities, and the details of regulations. The obvious difference in experience between the two agencies is that the FDA has a long history of regulating and directing food and pharmaceutical products manufacturers whereas the SEC is in its embryo stage in regards to standardizing its practices. This difference in background and experience has the two agencies in different enforcement leverages. The FDA leads and directs with its full authority. The ample knowledge database of the FDA provides not only the base for new regulations, but for industry guidelines as well. In contrast, the SEC has just announced SOX and its implementation is in progress. An active enforcement and direction of financial institutions with substantial results is expected in near future.

Despite the fact that both the FDA and the SEC have regulations, each agency's enforcement practice slightly varies from each other. The enforcement entity on food and drug manufacturing companies is the FDA, but COSO is a consortium of five main professional accounting associations and institutes: American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives Institute (FEI), The Institute of Internal Auditors (IIA) and The Institute of Management Accountants (IMA). With COSO and COBIT, the federal government is in a somewhat passive mode compared to the FDA in regulating its industry. This may influence the future path of some SEC major decisions since the interest from the private sector may vary from the interest of public sector

Both FDA regulations and SOX require "moral divine" in an organizations' digital transactions. Simply said, it asks for an organization to "do the right thing". The underlying philosophy of both agencies is well manifested in each and every regulation. One regulation that stands out in illustration is the audit trail: FDA, 21 CFR Part 11, Electronic Records; Electronic Signatures; Final Rule, and SOX 802. These two regulations state that on every digital transaction, there must be a record of who executed it, what was changed, when it was changed, and why it changed. As much as creating this technology in information system is challenging, it is a crucial aspect in auditing information system.

5. A Comprehensive Model from Both Practices

The FDA provides a detailed list of computerized system validation regulations and the SEC provides a framework that encompasses business transactions. Based on these two practices, we may propose a new information systems validation model (fig.1).

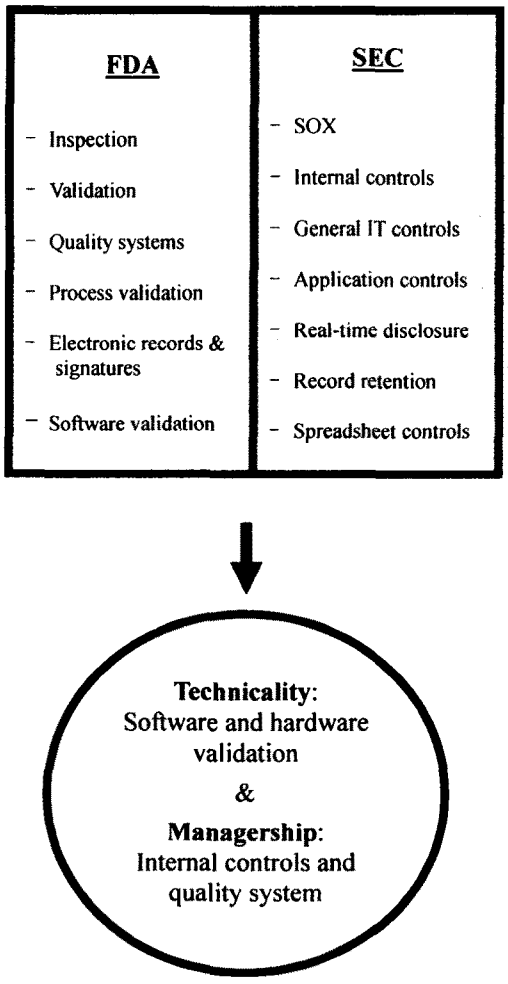
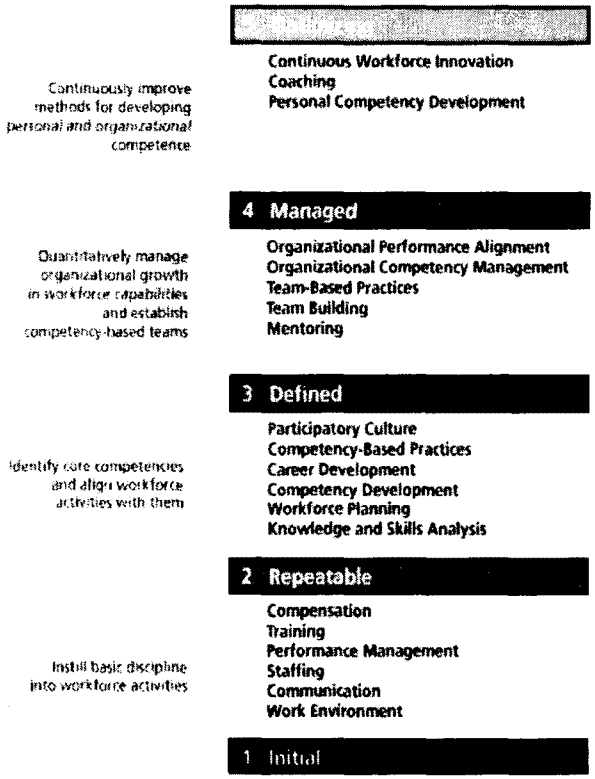


Figure 1 – The Comprehensive Model

By combining both agencies' practices, we may come up with an ideal information system validation and audit model. The System-driven FDA approach and The transaction-driven SEC approach will complement each other in full information system auditing. Along with this model, incorporating the People Capability Maturity Model (P-CMM) (fig.2) would add yet another dimension: the human factor. As much as the awareness of the importance of the human factor is increasing in many software and system development, validating and auditing the human factor is equally important. P-CMM is an instrument for organizations to efficiently control their human resources. Through its five maturity levels, P-CMM shows the path for organizations to incrementally transform into P-CMM organization.



Source: Software Engineering Institute
http://www.sei.cmu.edu/cmm-p/

Figure 2 – P-CMM Five Levels

Although not extensively as P-CMM, both the FDA and SEC do address the human factor to a certain degree. Adding P-CMM does require synchronization of the human factor from all three models (fig.3). Redundancy must be avoided for uniformity and consistency.

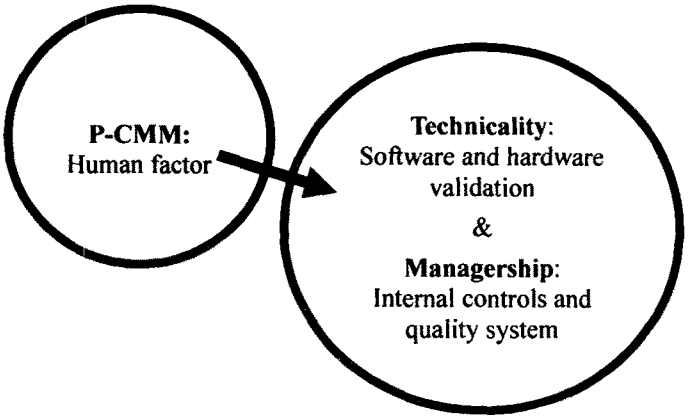


Figure 3 – The addition of P-CMM

The benefit of this new model would be convenience, time-saving, and synchronization of regulations. The convenience would mean that an organization does not have to apply three separate occasions for each model. The time-saving benefit is a consequence of the convenience factor. Lastly, the synchronization of regulations refers to the streamlined process of the regulations of all three models into one standard.

6. Future Work and Conclusion

Continuing this proposal, an empirical study is in order. Currently, this new "P-CMM+FDA+SEC" combined validation model needs continuous refinement areas where all three models have common ground would be consolidated and areas where each model has its strength it would be highlighted. The second phase is devising an experiment to test the model. The experiment objectives must be clearly defined and stated. A likely scenario is executing this on a number of professional software manufacturing or system development organizations. It may be a pharmaceutical company or financial institution where both are regulated.

Information system validation and audit processes have been very specialized according to the industries, which is perfectly understandable. But in a case where an organization wants to review and update their processes in all categories, then this type of model would efficiently serve the purpose. It is expected that the new "P-CMM+FDA+SEC" combined validation model would bring another level of information system validation. This comprehensive validation model truly encompasses every dimension of information system from its hardware to documentation.

References

[1] Curtis, Bill; Hefley, William E., and Miller, Sally People Capability Maturity Model (People CMM), Version 2,

July 2001, Pittsburgh, PA, Software Engineering Institute, CMU/SEI-01-MM01

[2] FDA, General Principles of Software Validation; Final Guidance for Industry and FDA staff, January 11, 2002.

[3] FDA, Guidance for Industry, Computerized systems used in clinical trials

[4] Guidance for Industry, Part 11, Electronic Records; Electronic Signatures – Scope and Application

[5] Boehm, B., (1976) "Software Engineering," IEEE Transactions on Computers, C-25(12), December 1976, pp. 1226 - 1241.

[6] Department of Justice Website http://www.fbi.gov/dojpressrel/enron103103.htm Date retrieved, May, 2007.

[7] House of Representatives, Sarbanes-Oxley Act of 2002, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_reports&docid=f:hr610.107.pdf