Balancing cGMP vs. SOX

Compliance Guidances

Invensys Operations Management
Douglas L. Lively CQA, PMP
110 New Bingham Ct.,
Cary, NC
27513

Revision: New Document

Issue Date: July 16th, 2009
Balancing cGMP vs. SOX Compliance Guidances

TABLE OF CONTENTS
ABSTRACT .............................................................................................................................................................. 3
INTRODUCTION ..................................................................................................................................................... 3
ARE CGMP AND SOX GUIDANCES COMPATIBLE? ........................................................................................... 4
DO IT ORGANIZATIONS HAVE TO MAINTAIN TWO COMPLETE AND SEPARATE ORGANIZATIONS?........ 5
CAN SOX INTEGRATE WITH ACCEPTABLE CGMP COMPLIANT CONFIGURATION MANAGEMENT / CHANGE CONTROL POLICIES AND SOP’S?........................................................................................................................................................................... 5
DOES IMPLEMENTATION OF CGMP COMPLIANCE GUIDELINES AFFECT AN IT ORGANIZATIONS’ ABILITY TO QUICKLY RESPOND TO ISSUES? ................................................................................................................................. 9
CAN PAST VALIDATION EFFORTS BE LEVERAGED TO MEET NEW DEVELOPMENT EFFORTS YET MAINTAIN COMPLIANCE?..................................................................................................................................... 10
CONCLUSION ....................................................................................................................................................... 10
REFERENCES ...................................................................................................................................................... 11
ABOUT THE AUTHOR .......................................................................................................................................... 11

LIST OF TABLES
Table 1 – cGMP VS. SOX Requirements .................................................................................................................. 4

LIST OF FIGURES
Figure 1 – Quality System Leading To Compliance .............................................................................................. 6
Figure 2 – Leveraging Minor Releases against a Major Release Baseline ............................................................. 10
Balancing cGMP vs. SOX Compliance Guidances

Abstract
As government agencies increase scope of regulations, companies acquire diverging technologies, and IT responsibilities increase the need for balancing specific regulatory demands will also increase. In some cases regulatory demands may appear to be in conflict and cause resource planning issues within the IT department. FDA regulatory guidances verses Sarbanes-Oxley compliance demands can certainly be viewed as one such example. With good planning the two guidances can be balanced to complement each other. Thus reducing the strain on IT resources and facilitate common development, issue management, and validation efforts. This paper will explore an approach to resolving differences, balancing the two guidances, and focusing IT compliance efforts into one compliance effort.

Introduction
On June 1, 1997 the FDA stepped into the software validation arena with the implementation of 21 CFR Part 820 (1). Five years later the US Congress entered the same arena with the implementation of the Sarbanes-Oxley (SOX) act of 2002 (2). During the intervening years from 1997 to 2009 the FDA has implemented 21 CFR Part 11, 21 CFR Part 111, and 21CFR Part 211. Even though the FDA never specifically mandated a particular Software Development Life Cycle (SDLC) model, the Biotech, Pharmaceutical industries, and compliance auditors alike have accepted the V-Model as the defacto standard for all computer systems validations.

As cGMP’s began influencing SDLC’s in the Pharma and BioTech Industries and computing equipment became cheaper and software more powerful, corporations, in a similar vein, began relying on information and data provided by computing systems at all levels within their respective organizations. This necessitated the need for tighter financial reporting requirements as defined by SOX. In like manner, the FDA (and other regulatory bodies e.g. TGA), began requiring controls on reports generated by software. As a result, cGMP guidelines and SOX compliance requirements have been quietly squaring off within IT organizations. The issues raised by cGMP (current Good Manufacturing Practice) guidelines versus SOX compliance are as follows:

- Are cGMP and SOX Guidances Compatible?
- Do IT Organizations Have To Maintain Two Complete And Separate Organizations?
- Can SOX Integrate With Acceptable cGMP Compliant Configuration Management / Change Control Policies and SOP’s?
- Does Implementation Of cGMP Compliance Guidelines Affect an It Organizations’ Ability to Quickly Respond To Issues?
- Can Past Validation Efforts Be Leveraged To Meet New Development Efforts Yet Maintain Compliance?
Are cGMP and SOX Guidances Compatible?

Both cGMP and SOX SDLC’s share similar scope mainly to demonstrate control, ensure quality, and be independently auditable, exhibit signoff. Some other similarities are listed below (1, 2).

<table>
<thead>
<tr>
<th>Guidance Requirements</th>
<th>cGMP(1)</th>
<th>Sarbanes-Oxley(2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demonstrate Control</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ensure Quality</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Must be Independently Auditable</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Must be Quickly Accessible</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Must have Signoff</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Assure No Material Weakness Exists</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Provide for evaluation (verification) of Financial Reporting Methods</td>
<td>☐</td>
<td>✓</td>
</tr>
<tr>
<td>Provide for Verification and Validation of Requirements</td>
<td>✓</td>
<td>☐</td>
</tr>
<tr>
<td>Enhance Quality of Financial Information</td>
<td>☐</td>
<td>✓</td>
</tr>
<tr>
<td>Quality Assurance thru Risk based approach to validation</td>
<td>✓</td>
<td>☐</td>
</tr>
<tr>
<td>Increase Confidence in Financial Improvements</td>
<td>☐</td>
<td>✓</td>
</tr>
<tr>
<td>Provide and Early Warning of the Need for Improvements</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

As can be seen from the table above, compatibility exists among the guidances. However, the implementations of each are very different. Additionally, the cGMP goes a step further by introducing safety as the dominant issue for all software validations and by defining software validation as:

“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 software can be consistently fulfilled.” (1)

As a result IT organizations are faced with few alternatives. Either, split their departments / computer between validated and non-validated systems or adopt a balanced approach to FDA vs. SOX Compliance.
Do IT Organizations Have To Maintain Two Complete And Separate Organizations?

Today’s IT departments face many challenges among them are:
- Tightening budget constraints
- Fewer human resources
- Increased/flexing business demands
- Fluid software / hardware technologies
- Increasing compliance issues

Most IT organizations have been able to deal with tighter budgets, resource issues, business demands, and fluid technologies; however, managing multiple compliance methodologies is another story. Additionally, many of them, for the most part, have everything they needed to meet cGMP compliance requirements, but, the information has not been organized into auditable documentation. As a result, IT departments may be unprepared to address issues of safety and patient risks with respect regulatory compliance in computing systems raised during a compliance audit. This has resulted in a tendency to create a “new department” to specifically handle cGMP compliance issues.

However, there is no need to create a separate department or organization within the IT department. IT organizations can handle “seemingly” divergent SDLC methodologies and guidances. It does involve planning and a will to manage change within the IT organization, adherence to stricter design controls, as well as, a partnership / alliance with the Quality Assurance department to guarantee that compliance issues are met, documented, and resolved.

Can SOX Integrate With Acceptable cGMP Compliant Configuration Management / Change Control Policies and SOP’S?

The answer is a simple, yes. Configuration management / change control can be leveraged to integrate divergent life cycle development methodologies. To accomplish this, however, requires some changes in the IT Structure.

- Modification of corporate documents to provide justification for computer systems cGMP validations
- Formation of a regulatory compliance review team comprised of IT and Quality Assurance professionals
- Implementation of a balanced Change Control / SDLC Model
- Development, Training, Documentation of Training, and adherence to departmental SOP’s
- Adherence to Configuration Management / Change Control Standard Operating Procedures

To start, IT should develop a partnership with Quality Assurance. This usually means a modification of corporate documents to define the need for regulatory compliance validations for computing systems.
Balancing cGMP vs. SOX Compliance Guidances

A regulatory compliance review board, comprised of IT and QA Management, should be established to manage incoming system change requests. This team will be able to effectively assess and route requests to the proper type of validation to take place.

Implement a balanced Change Control / SDLC that embraces both V-Model and SOX SDLC. In the example below the V-model SDLC is used when “Major” Regulatory Compliance Validations are required and SOX SDLC for “Minor” Validations requiring Regulatory Validations or for systems requiring SOX compliance.

Figure 1 – Quality System Leading To Compliance
Balancing cGMP vs. SOX Compliance Guidances

The Regulatory Compliance Review Board (RC / RB) would review incoming change requests and perform an impact analysis to determine if A) The system change request should be assessed with respect to risk, B) If they are to be performed on a cGMP compliant validated system, and C) if it is a major or minor validation. In cases where there is no cGMP validation required SOX should be implemented as the SDLC of choice. Where a cGMP compliant system is involved, major validations should go through the V-model and formal validation. Minor validations for cGMP systems would occur as a SOX level validation with a cGMP view.

Simply defined “Major” releases of software are to be treated as new development projects and follow all phases of the SDLC. Major releases are to be created when a software system is first implemented or when a service request would include changes, which add new features to a software system causing a rewrite of the operator’s manual, SOP, alter the way the system operates, or risk analysis of the request would indicate harm to the patient, customer, process or operator.

Additionally, “Minor” releases of software are to be used when a small number of changes or fixes are to be added to a previously released software system. As a guideline, minor releases should not affect the operator’s manual or SOP. Minor releases are established as a way to rapidly respond to unforeseen circumstances effecting customers. Service requests received for a software system, which simply improve functionality and would be considered as an upgrade should be included in a Major release with other similar change requests. Minor releases should be reserved for changes where a specific problem is being addressed, a rapid turn around time is essential, and a risk analysis of the request indicates that the level of impact to the patient, customer, process, and / or operator is minor.

The RC / RB is tasked with continually monitoring project progress and acts as the final decision maker when it comes to approving a system release or mandating a revalidation.

In the past there has been resistance to implementing a shorter life cycle development model. However, for small validations and minor changes a SOX model could be used:

“Another aspect of software testing is the testing of software changes. Changes occur frequently during software development. These changes are the result of 1) debugging that finds an error and it is corrected, 2) new or changed requirements (“requirements creep”), and 3) modified designs as more effective or efficient implementations are found. Once a software product has been baselined (approved), any change to that product should have its own “mini life cycle,” including testing. Testing of a changed software product requires additional effort. Not only should it demonstrate that the change was implemented correctly, testing should also demonstrate that the change did not adversely impact other parts of the software product.” (1 - pg24)
Balancing cGMP vs. SOX Compliance Guidances

This puts the responsibility on SOX to be stricter when it comes to cGMP development, testing, and implementation. Some areas addressed by the SOX guidance but are often overlooked are as follows:

1. Implementation of Risk Management as part of any project documentation (this is a SOX requirement).

2. Completion a final Summary Report
   - States release version
   - Summarizes verification / validation activities
   - Contains team signoff including QA

3. Application of cGMP Good Documentation Practices:
   - Initial and date all corrections noting the error with a single horizontal strikethrough and writing the correction to the side.
   - Implement Sequential Numbering of all pages
   - Note major sections in SOX document with exact wording used on the SOX Contents page
   - Single blank cells should contain N/Ap (not applicable) with initial and date.
   - Multiple blank lines should contain a right facing slash, N/Ap, initial and date.
   - Number pages consecutively throughout packet.
   - Do not write on the SOX document after it has been approved.
   - Develop an implementation plan.

4. Addition of Quality Assurance to the SOX packet signoff where applicable

5. All SOX major sections should contain approval with signoff or a justification as to why it is absent.

6. Do not use checkboxes or checks in test cases.

7. Write verification / validation test cases – This demonstrates documented control, reproducibility, stability, and measurability.

8. Always use signatures for signoff by team members

9. Only use blue or black pen for signoff.

9. Implement deviation reporting

10. Always implement a post implementation and monitoring plan.

11. Identify the validation team; define the responsibilities of each, accompanied by Signatures, initials, dates, and statement of training.

12. Fully complete SOX forms and note which forms are templates.

13. Do not include “scratch notes” in final packet.

14. Do not include information from other projects. If the project contains a subproject then this should be noted in the plan and labeling on the packet.

15. Traceability should reflect user requirements. It should also trace User Requirements to Functional Requirements to Design Requirements to Risk Mitigations, to Test Cases meeting requirements / mitigations.

16. SOX packets should contain enumerated list of user requirements with signoff for users and Quality.
17. Avoid open ended language. E.g. “Looks Correct”, “Seems to work”, etc in actual results. Rather state what the result appeared for each test step was executed. This is the measure of “Correctness”.

18. Test Cases at a minimum should contain:
   - Step Number
   - Procedural sub-steps to produce an expected result
   - One expected result
   - A place to record the actual result.
   - An overall summary of the results

Some other compliance points to consider when introducing cGMP compliance to a SOX environment are as follows:

- Validate against a controlled environment.
- Assess requirement risks
- Control execution activities during verification
- Information and communication (Reporting)
- Monitoring (Post Implementation)
- Quality review and signoff
- Audit controls must be in place for the following
  - Change Management
  - Version Control
  - Software Development Life Cycle
  - System Security
  - Incident Reporting
  - Support

**Does Implementation of cGMP Compliance Guidelines Affect an IT Organizations’ Ability to Quickly Respond to Issues?**

This has been a stigma associated with cGMP validations. The bottle neck occurs from validation programs that mandate a full validation for each and every change no matter how large or how small. When a balanced program is implemented, as previously suggested, the turn-around time for IT departments is much improved. As a result, achieving and maintaining compliance becomes much more manageable without compromising responsiveness.
Balancing cGMP vs. SOX Compliance Guidances

Can Past Validation Efforts be Leveraged to Meet New Development Efforts Yet Maintain Compliance?

Maintaining compliance (once it has been achieved) is key especially when considering the amount of money and human resources expended during a “full” validation. However, as already noted, full validation on every new release is costly, time consuming, and weakens IT responsiveness. Knowing how to leverage previous validations will save your organization money and lessen the amount of time required to validate systems. Validations should be leveraged in the following manner:

- Full validation using V-model, for initial release
- Utilize SOX SDLC for minor release
- Reference previous baseline validation in minor release documents
- Use V-model only when a full validation is necessary e.g. major release

Figure 2 – Leveraging Minor Releases against a Major Release Baseline

Conclusion

cGMP compliance and SOX compliance programs are beginning to encounter each other in the workplace. Instead of maintaining cGMP compliance separate from SOX compliance, IT Departments should adopt a balanced approach to managing SDLC’s. SOX SDLC’s should be improved to embrace cGMP. However, care should be taken to assess risks and with respect to patient safety, operator safety, and labeling (operator manuals, user guides, and SOP’s), and level of validation for any system change request. Implementation of a balanced approach to validation will save IT department’s time and money without sacrificing responsiveness or compliance requirements. If planned well the IT organization should be able to balance both cGMP and SOX SDLC’s.
Balancing cGMP vs. SOX Compliance Guidelines

References

1. General Principles of Software Validation; Final Guidance for Industry and FDA Staff  
   January 11, 2002 – U.S. Department Of Health and Human Services Food and Drug  
   Administration Center for Devices and Radiological Health Center for Biologics Evaluation  
   and Research

2. Sarbanes-Oxley Act of 2002  
   January 23, 202 One Hundred Seventh Congress of the United States of America

About the Author

Douglas L. Lively works as a Project Manger for Invensys Operations Management and is based in  
Cary, North Carolina. He is a Certified Quality Auditor through the American Society for Quality  
(ASQ) and his Project Management Certification is through Project Management Institute (PMI). Mr.  
Lively has more than 10 years experience in regulatory software compliance and has managed  
regulatory projects ranging from medical devices to LIMS and ERP systems.