White Paper

Regulatory Compliance Needs Process Management

A Pathfinder Technology Solutions Whitepaper

October 22, 2004

Introduction

All businesses need to comply with government regulations, regardless of countries where they operate. The government can be local, state/provincial, federal and international. Often the mindset of company executive is that compliance for a certain regulation is complete when some documents are created. Compliance is a process – NOT a document.

Furthermore, compliance is rarely a single event exercise. Unlike certain event-driven control activities (e.g., Y2K), compliance to regulations such as Sarbanes-Oxley Act, usually continues as a routine part of doing business. It is therefore important to not just complete the initial compliance, but to sustain it as well. Since the cost of compliance is high, a well thought process not only will provide lower cost for initial compliance implementation, enforce compliance policy and subsequent compliance sustenance. It will also protect the company from potential censures from government regulators.

The compliance laws of the country of business typically apply to a company, regardless of its origin. For example, if a foreign company has to register with SEC in U.S., it will be subjected to the requirements for compliance of Sarbanes-Oxley act.

The compliance exercises, however painful they may be, have to meet the related regulations. The penalty for non-compliance can be high, with fines sometimes in millions of dollars as well as jail time (as in the case of Sarbanes-Oxley Act). Such an exercise therefore should not be pursued in an ad-hoc manner, addressing requirements as they emerge by carrying out one-off projects. A compliance process should be formal as well as routine. A well-executed compliance exercise will require relatively lower routine effort for its sustenance.

The Need

In order to meet the compliance requirements of increasingly complex legislation, the companies primarily need to:

- Provide transparency in corporate governance;
- Store and secure related documents and data; and,
- Provide an audit trail for approval.

The compliance process should also be flexible so that changes in company business as well as government regulations can be addressed. The compliance process also must be documented and the documents have to be managed adequately.

The Compliance Roadmap

In order to meet compliance, sufficient documented evidence has to be presented to regulatory bodies (such as SEC in US). To achieve this objective, a structured methodology needs to be adopted since compliance implies defined processes and appropriate rules. Without a structured methodology, there will be broken audit trails and organizations will be subject to censures by regulatory bodies. It also drives creation, format, maintenance and archival of necessary documents.

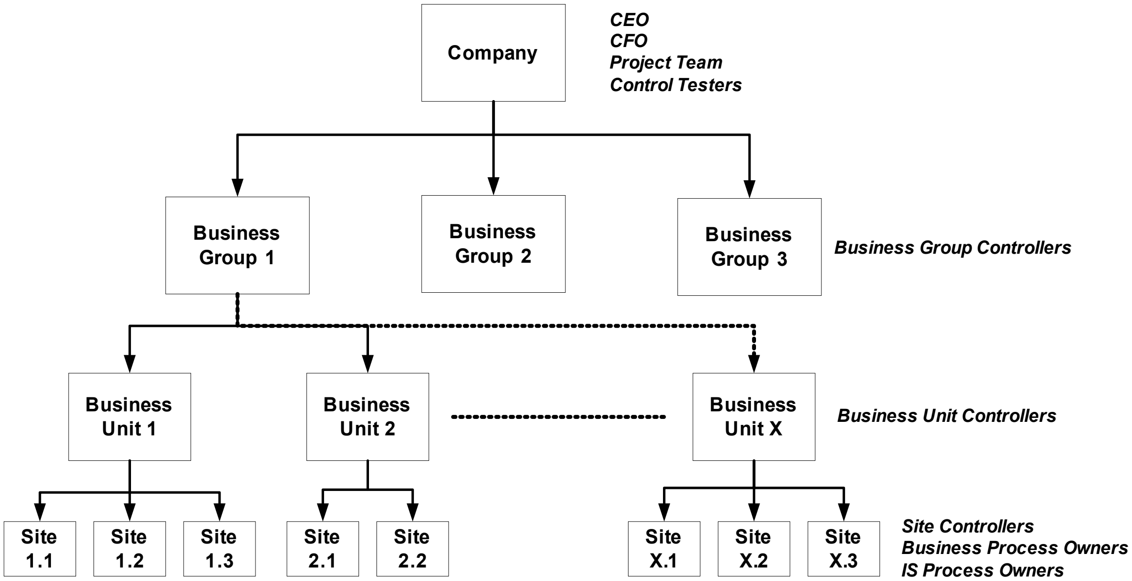
A compliance solution must include the necessary documents, but also a record of the process by which they were created — a trail to show when, how, where and by whom they were created, who last modified them, where they came from, where they are stored and what need they fulfill. Process documentation and control software can provide a means of assigning and documenting roles and responsibilities.

When the overall compliance exercise is part of a singular framework, it makes it easier for enforcement of rules and meeting audit needs. Formulating the rules also forces enterprises to think through and standardize business logic. In the long term, this process always saves time and money. All documents, correspondences, even discussion bulletin boards can be stored in such a manner that will make an easy future search and access.

In order to meet the above requirements in a singular framework, the compliance steps need to follow a workflow. Well-designed workflow software ensures that everyone follows the same procedures, proper approvals are granted, appropriate documents are created, compliance process testing is adequate and the final sign-off is easy.

The process to achieve and ensure long-term compliance has many elements. If compliance – such as the one for Sarbanes-Oxley act – is a critical requirement, the organization has to name individuals responsible for the process. A team has to be formed for initial implementation. It will be prudent to hire a consultant familiar with such compliance process. The compliance team will interact with various parts of the organization. A large organization will have business units, divisions, sites, plants or offices. There are business processes at each level in the organizational hierarchy. Each business process has to go through the same exercise for the company to achieve compliance.

Example of a Business Organization Structure



Steps in a Compliance Exercise – Sarbanes-Oxley Example

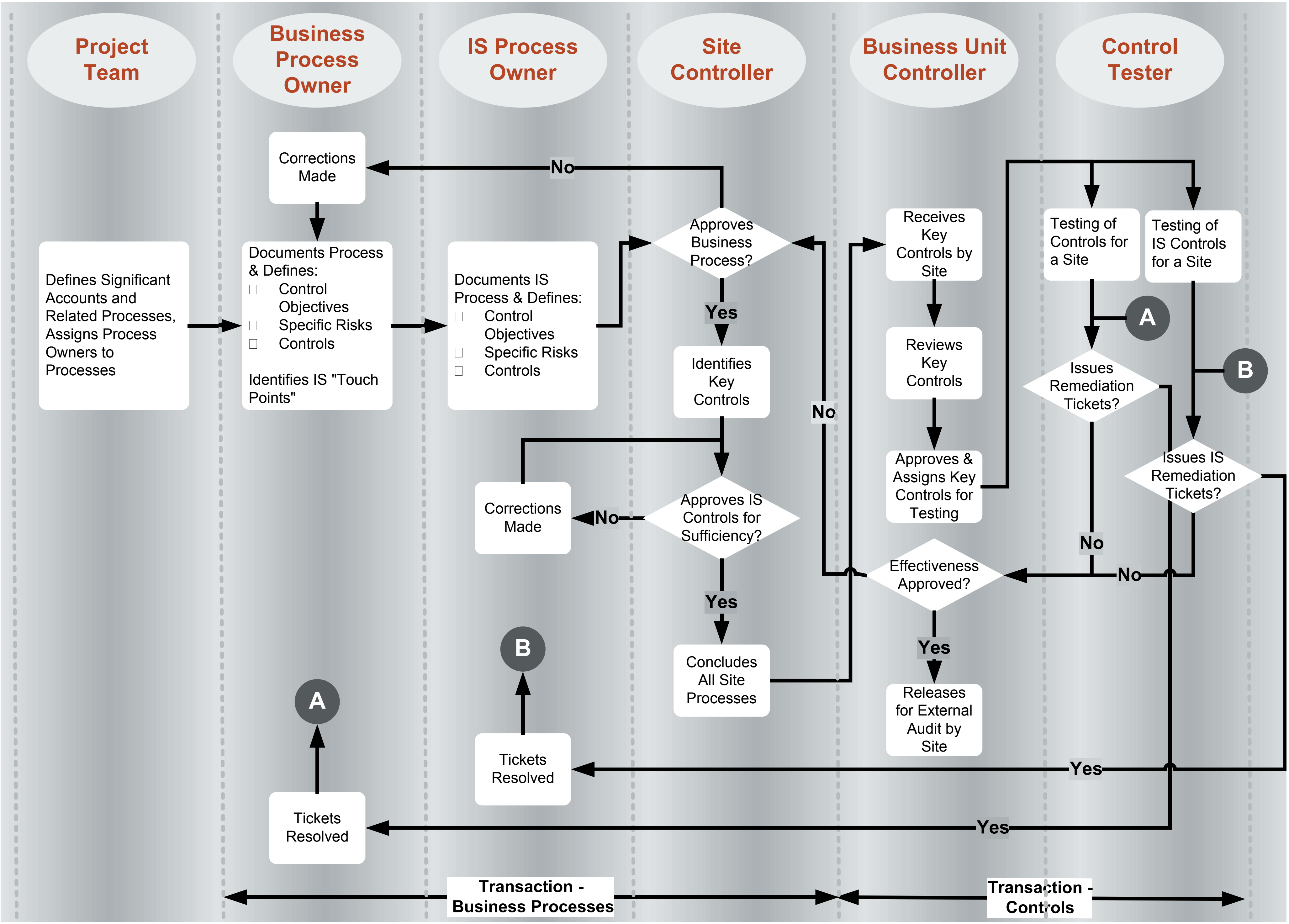
Specific compliance means specific steps. As an example, the steps to be taken for Sarbanes-Oxley (SOX) act compliance are being discussed here for a business organization with a structure shown above. The steps for initial compliance are the following:

1. Develop a SOX steering committee comprised of senior managers.
2. Develop a SOX project team comprised of team leader, business unit controllers, site controllers, Information Systems representative and possibly others.
3. Identify significant accounts that contribute to company annual financials;
4. Determine business processes that lead to significant accounts.
5. Identify "process owners" who will analyze business processes, which are subsequently assigned to them. The process owners perform the following for each business process:
    - Maps the process (described below)
    - Determines control objectives for a process.
    - Identifies the financial risks or "what-can-go-wrong" by considering likelihood and impact in the process.
    - Assigns controls to mitigate the financial risks in the process.
    - Defines the key controls by assigning likelihood and impact.
    - Documents all of the above steps – through Workflow software.
    - Hands over to site controller for verification.
6. Site controller reviews process owners' work as well as a list of key controls. A process may be sent back to a process owner if sufficiency criterion for process analyses and documentation is not met.
7. Identify IS process owners (can be done earlier).
8. Processes meeting business sufficiency criterion are passed to the IS process owners who perform IS steps mentioned later.
9. All site processes are then passed over to Business Unit (BU) controller.
10. BU controller reviews all key controls, by site, and provides needed approval for control testing.
11. Control Testers are identified (can be done earlier). Testing for a site need to avoid "conflict of interest" issue by choosing a control tester from another site.
12. Testers – both business and IS, but not necessarily together – test key controls and provide reports on their compliance.
13. Site controllers ensure the remedial actions are taken based on deficiencies found in control testing.
14. BU Controller approves the compliance process for external audit.
15. CFO approves the overall compliance.

The above is a representative example and is not meant to be all-inclusive. Also, for smaller organizations, certain functions can be combined.

The following figure depicts the above in a workflow.

Flow of Responsibility


Project Team
Business Process Owner
IS Process Owner
Site Controller
Business Unit Controller
Control Tester
Defines Significant Accounts and Related Processes, Assigns Process Owners to Processes
Corrections Made
No
Documents Process & Defines:
□ Control Objectives
□ Specific Risks
□ Controls
Identifies IS "Touch Points"
Documents IS Process & Defines:
□ Control Objectives
□ Specific Risks
□ Controls
Approves Business Process?
Yes
Identifies Key Controls
Corrections Made
No
Approves IS Controls for Sufficiency?
Yes
Concludes All Site Processes
No
Receives Key Controls by Site
Reviews Key Controls
Approves & Assigns Key Controls for Testing
Effectiveness Approved?
Yes
Releases for External Audit by Site
Testing of Controls for a Site
Testing of IS Controls for a Site
A
Issues Remediation Tickets?
B
Issues IS Remediation Tickets?
No
No
B
Tickets Resolved
A
Tickets Resolved
Yes
Yes
Transaction - Business Processes
Transaction - Controls

Business Process

What is a business process? It is essentially who-does-what-when-and-why. In order to understand first and subsequently analyze a process well, one has to create a graphical map. Once a process is drawn in a map (as opposed to a description in text form), it is also easier to visualize it and allows further improvement through analysis. Even though a compliance process does not necessarily require an improvement of business processes, such improvements will be desirable if they reduce costs while meeting required compliance.

Business processes are not typically well understood – mostly because they have not gone through the steps mentioned earlier. Quite often business processes cut across various functions. Complex business processes should at first be created at a higher level

- Show high-level business process example and then drill down to a more detailed process.
- Sarbanes-Oxley needs to cover ALL business processes that involve financial transactions.

Process definition and monitoring are the heart of compliance. Enterprises with complex compliance needs should consider using business process management tools to build compliance solutions that are flexible and that can be used to build processes to comply with any existing or future legislation.

Definition of a Process
A systematic sequence of steps or activities, that converts resources into a product or service is a process. At times there may be a decision to select such steps or activities, where necessary, based on a certain criteria. Input Resources may be any combination of people, equipment, methods, materials, energy, knowledge, capital, etc. Business processes are the organization's mechanism of creating and delivering value to its stakeholders.

By definition, a process has several key characteristics: it has specific standards which determine if it's done correctly, and which let it be repeated by others; and it responds to quality control mechanisms that can help the process be done more efficiently. A more efficient process should result in steps or activities – as well as the process itself – being done faster, cheaper, or result in the creation of a better product or service.

A process map is a graphical representation of a process. In its simplest form, it has four elements: start point, tasks, decision point (based on a criterion) and stop point. The sequence of tasks along with decision points defines a process flow on how above mentioned resources formulate a product or a service – which is a "transaction" flowing through the process.

Once an existing process is graphically depicted, one can determine if a certain step adds to the value of the transaction. If it does not, it may be possible to eliminate such a step, thereby resulting in the transaction being processed faster and/or cheaper and in a more efficient process as well.

The workflow shown above is a process map for achieving Sarbanes-Oxley Act compliance.

Information System (IS) Function and Processes

Every business process that has an IS touch point (or function) needs to identify it. Due to the prevalence of IS in businesses, it is hard to imagine a process that does not utilize an IS function. Since a compliance process such as that for Sarbanes-Oxley act needs to identify risks in financial transactions (in the form of WCGW or what-can-go-wrong) and its controls, related IS processes also have to be described along with the WCGWs and their controls.

ISACA (Information Systems Audit and Control Association), in its IT Control Objectives for Sarbanes-Oxley document states the following:

“The PCAOB* standard includes specific requirements for auditors to understand the flow of transactions, including how transactions are initiated, authorized, recorded, processed and reported. Such transactions’ flows commonly involve the use of application systems for automating processes and supporting high volume and complex transaction processing. The reliability of these application systems is in turn reliant upon various IT support systems, including networks, databases, operating systems and more. Collectively, they define the IT systems that are involved in the financial reporting process and, as a result, should be considered in the design and evaluation of internal control.”

*PCAOB - Public Company Accounting Oversight Board is a private-sector, non-profit corporation, created by the Sarbanes-Oxley Act of 2002

Due to high dependence of business processes on IS, a variety of challenges are to be met in executing controls for such processes. In addition to business controls, IS controls also need to be in place. There are following essential steps for IS controls, once a business process is completed by the business process owner:

1. Map relevant IS process, if needed;
2. Determine IS risks or “What-can-Go-Wrong”;
3. Identify significant controls
4. Document the above

Just as in business controls, since long-term viability is key, sustainability also has to be built in while going through initial compliance processes.

Compliance Workflow Software

Achieving compliance is a process in itself. Performing tasks within the workflow mentioned above is impractical without the use of workflow process management software. Without such software, coordination of:

- Multiple business functions (project team, process owners, site controllers, etc.),
- Many (even several hundreds) business processes,
- Even many more controls,
- Perhaps many hundreds of documents (process maps, miscellaneous documents, discussion threads, etc.),
- Email notification, etc.,

become unrealistic. Such software will also allow quick checks to the compliance process itself, checking transactions, documents, events and statuses. It will act as a repository of all embedded documents as well as in the form of attachments. It will provide a bulletin board for discussion threads that will also be archived for future references.

The workflow software will allow appropriate hand-over of transactions, once processing of a transaction is completed by a business function. If a certain individual is no available at a certain time, appropriate delegation will allow progression so as not to delay the process. Conversely, if a transaction is held up at a certain stage, it can be traced very easily. Transaction statuses can be determined with ease.

Finally, the software will provide an accurate and complete audit trail for further investigation by external auditors. It will also allow easy processing of future changes in business – by adding or deactivating (nothing is to be deleted in the software, only deactivated for any future audit) new or obsolete business processes, respectively. This permits easy sustainability of compliance, thus avoiding potential censures by regulatory bodies.

Precise Rendering of Compliance has Advantages

Compliance means definitions of processes and related rules that not only have to exist but are consistent as well. All guesswork is removed when these criteria – existence and consistence – are met. This not only helps to avoid censures by regulatory bodies, it also forces enterprises to have discipline. Once business processes have been mapped, one can analyze them for improvement to make them more efficient.

Adherence to compliance will also lead to cost savings by the enterprise in the long term. Absence of a structured compliance is not only risky – perhaps even illegal – but will also cost money.

In the case of Sarbanes-Oxley act, such compliance also has similarity with well known, albeit more stringent, business improvement methodologies such as Six Sigma. As in Six Sigma, business processes are mapped (ideally improved where necessary, as well), “risks” (“defects” in Six Sigma) are identified and controls are established and subsequently monitored.