



Profiting from Compliance with SmartBPM™

Stop Treating Compliance as a Nuisance and Seize the Opportunity to Implement Real Business Controls.



Executive Summary

SmartBPM helps to minimize the impact of Sarbanes-Oxley by delivering the perhaps unintended dividends that come for addressing governance requirements with a tool that can learn from them and be used to build new agility across an organization.

Meeting governmental standards for financial probity, risk reduction, IT preparedness, and corporate governance is a tedious challenge that adds no intrinsic business value in and of itself. But, maybe these regulators are on to something. If you don't have the ability to design, execute, document, monitor, and optimize your critical business processes, why should they believe your financials? Following Enron, trust alone isn't a good enough standard for ensuring your company is operating the way you say it is. The same holds true inside the company. Should we trust that policies are carried out the way we expect them to be? Or, to look at it in a positive perspective, wouldn't it be great if we could implement new policies and be sure they would be adopted? Taking a business process management approach to compliance provides the tools to comply with government standards, and also provides the infrastructure you need to better execute the key processes that power your business.

The word *compliance* means both "adhering to standards" and "flexibility under pressure." Only an approach that fully fuses business rules with business processes can deliver true compliance.

This white paper will argue that if you're not using the best possible BPM Suite to address compliance mandates such as Sarbanes-Oxley, you're (1) doing it the hard way, unnecessarily (2) hemorrhaging far more staff time and audit fees than you need to, (3) institutionalizing a high-cost, isolated bureaucracy, and (4) forgoing the overall growth, competitive agility, and internal productivity benefits that spring from BPM's operational visibility and real-time process-enhancement.

Don't tackle compliance just for the auditors and regulators: do it for your customers, staff, and stakeholders. The right BPM does far more than help you comply with regulations: by closing the gap between mission and execution, between goals and activities, it gives you the tools you need to continually transform your business. Eventually, everyone will figure this out. Why not address the need now - at a corporate "nervous-system" level - and take control of your firm?

Compliance by the Numbers

12,000

The number of software product vulnerabilities catalogued by the National Institute of Standards and Technology. The list is growing by an estimated 10 per day.

(nvd.nist.gov)

45%

The percentage of all companies that experience fraud, the median cost of each incident being \$60,000.

(Association of Certified Fraud Examiners)

\$4,809,000

Average Sarbanes-Oxley audit fees, for S&P500 companies in 2004, a 19% jump over 2003. For S&P Midcap companies, the equivalent figure was \$1,135,000.

(Foley & Lander LLP, "The Cost of Being Public in the Era of Sarbanes-Oxley," 2005)

48

The number of disparate financial systems managed by a typical major public company. Each also averages 2.7 ERP systems in operation.

(eWeek, 2/16/04)

25,667

Estimated number of man-hours a company with \$2.5 billion in revenue will spend on Sarbanes-Oxley Section 404.

(Survey, Financial Executives International)

47%

The percentage of major firms that rely on stand-alone spreadsheets for financial reporting.

(eWeek, 2/16/04)

44% & 33%

Percentage budget allocations for internal labor and outsourced services, respectively, related to compliance. Only 19% is reserved for technology.

(AMR Research)

Control and Compliance Challenges

Forget compliance - for a moment, anyway. Think instead about an everyday business process - purchasing, for example - within your firm, one that is:

- driven by business (not technology) requirements
- computerized but with human intervention as appropriate
- able to be summarized in graphical flowcharts
- reducible to various types of rules (if/then, decision tables, etc.)
- measurable in a number of ways (speed, error rate, etc.)

Usually, but not always, business processes also involve:

- a history or audit trail
- documentation (in both senses: proof and paperwork)
- explicit management of exceptions
- testing and remediation
- a hierarchy of access, permissions, and approvals

Look this list over. Regulatory compliance - with SOX, HIPAA, FACT, or any other - is just another, albeit extremely challenging, business process.

The good news is that advanced BPM Suites now mean that it's possible for you to build complex compliance processes into a repeatable, measurable framework that all parts of your business can access and share, even for significantly different, yet-to-be-written regulations.

Regulatory compliance - with SOX, HIPAA, FACT, or any other - is just another, albeit extremely challenging, business process.



Traditional Technologies Have Difficulty Addressing Control and Compliance

Now that you've grappled with your first compliance cycle - and the thought of "muddling through" again gives you heartburn - you have three options:

1. **Configure an enterprise mega-application to "do" compliance.** You already own the software, which is supposed to do everything (given enough customization).
2. **Acquire a purpose-built Sarbanes-Oxley product.** This appealing out-of-the-box solution promises to tackle every compliance issue by specializing in internal controls.
3. **Get serious about BPM.** But be careful; the architecture of most BPM systems fails to fully integrate rules and processes.

There's more than one way to deal with compliance, but some ways are far better than others. How do these options stack up?

Configure an Enterprise Mega-Application to "Do" Compliance

Enterprise Resource Planning (ERP), Enterprise Content Management (ECM), document management, and project management systems are fine at what they're designed to do. But they are not designed to meet the demands of compliance with the universality, flexibility, and audit-friendliness found in Business Process Management (BPM).

While an ERP system, for example, may be tailored to accumulate, organize, and report vast amounts of financial and production information, it incorporates little knowledge of the firm's operating procedures, security provisions, and other areas vital to compliance. Each highly-customized and hard-coded ERP module covers a single area of the company's business and doesn't "play well" with non-ERP areas. In contrast, compliance can and does involve almost every department.

By the same token, content-focused applications shine at the creation, categorization, and versioning of documents, which are obviously crucial at compliance audit time. But these document banks are essentially static storehouses that have nothing to do with the dynamics of daily operations, corporate policies, and managerial decision-making. Like project-management systems, they were never designed to automate and streamline work or distribute accountability, let alone trigger appropriate, best-practice actions.

In short, although these systems generate and track much of the raw information that compliance efforts require, they don't effectively bridge operational silos, nor are they built for rapid change and mounting complexity. They are no substitute for a SmartBPM system.

Acquire a Purpose-Built Sarbanes-Oxley Product

Vendors in this new software category have considerable subject-matter expertise, and their product interfaces appear more directly relevant to your pressing need for controls testing, audit procedure support, and financial statement certification.

For the most part, however, these high-level shells depend on external content management, workflow, and collaboration technologies - with all the attendant integration and synchronization overhead. Most vendors offer detailed, spreadsheet-style reports on the status of controls, and some can attach or map process flows, but they are unable to coordinate the controls-testing process or track and remediate exceptions. Certainly, they facilitate the audit process by gathering and structuring information, but they fall short in their capacity to actually design, control, and improve the compliance effort.

What are the other drawbacks? These applications have limited utility outside of their narrow scope, and as Sarbanes-Oxley evolves, customers are on the vendor's timetable (not to mention existence) for critical updates. You also risk creating a permanent internal bureaucracy focused on compliance but reporting to no department: far better to distribute accountability throughout the organization and make compliance part of everyone's normal job. Lastly, they are focused on compliance, pure and simple, and are very limited solutions. If you want to take business controls seriously to get a better handle on your processes or risk, these solutions aren't going to help.

The Ostrich's Guide to SOX Compliance

Wash. Rinse. Repeat. Pray.

A complicated manual approach worked last year, didn't it? Your auditors will be happy to hold your hand (and your wallet) every year, and your IT staff won't mind the numbing repetition of test-scripting procedures and nagging users. Just don't tell your CEO and CFO that you're depending on a manual process to keep them out of jail.

Blame Section 404 for your company's disappointing results.

Moan about this onerous requirement and demand relief from your congressman. Your shareholders will cut you lots of slack - after all, they don't have anywhere else to invest. And the board is certain to endorse your rationale.

Treat compliance reluctantly as a "cost of doing business."

Of course, there's little business upside to this focus on mundane processes. If only Asian and European companies had the same ridiculous regulations, then we'd have a level playing field.

Think departmentally and locally.

If you can limit the impact to Finance and IT, perhaps the nuisance won't spread to areas like human resources, production, and legal. View each mandate in every country you do business as a brand new hurdle.

Believe your ERP, CRM, document management, project management, business analytics, or traditional BPM vendor when he tells you, "Don't worry, we do compliance, too."

SOX does require a lot of reports, after all, and it's a major project. How can you go wrong with a tool you already have in-house? So what if the document repository isn't integrated with email approval hierarchies, your rules engine runs on its own platform, or your project dashboard doesn't know how to make a Gantt chart out of internal controls?

The SmartBPM Alternative

For all its pain and prominence, SOX isn't a one-time episode like Y2K: it's just another filament in a web of emerging corporate regulations, both here and abroad. In an environment of ever-changing compliance standards, the only practical approach is one that empowers your own people to quickly adapt a core set of best-practice rules and processes to new circumstances and risks. With a well-designed BPM system, nothing is hard-coded; every rule resides in a centralized "rulebase" that's accessible throughout the organization.

Simply put, a BPM system converts management intent - goals, decisions, and policies - into business execution - operations, procedures, and systems. In the compliance setting, it addresses questions such as:

- Why? With what regulation are we complying? What's the objective?
- What work needs to be done? On what schedule?
- Is the geographical location relevant?

Companies should invest in a SmartBPM platform that can accommodate *both* the all important compliance rules imposed from without as well as the day-to-day operational processes.

- Who does the work? Who approves assignments? Who is backup?
- How is this work tested, tracked, and secured?

In other words, the rules abstract the organization's policies and best practices and apply them to daily workflow. By that definition, it makes little sense to embed rules and processes in disparate applications - even ones purportedly dedicated to compliance activities - because you're just creating more technology "silos."

Instead, companies should invest in a SmartBPM platform that can accommodate *both* the all important compliance rules imposed from without as well as the day-to-day operational processes. SmartBPM abstracts both from applications, rendering them transparent and accessible, and keeping them under the close scrutiny of on-going activity monitoring. By doing this, it can help you roll out rule and process changes without altering application code anywhere.

The bottom line: Instead of constructing a patchwork of point fixes for compliance, use this opportunity to develop a new, immensely valuable, foundational corporate asset, one that (1) captures how the best people in your organization think and work; (2) facilitates better human-to-human workflow; (3) more tightly aligns your execution with your goals; (4) supports continuous change and improvement; and (5) leverages and extends your legacy assets. Take this approach, and you'll come to see compliance as more a blessing than a curse.

We can break compliance down into two types of issues (1) managing corporate policy and controls - this involves defining processes, testing processes, diagnosing failures to tests and (2) managing day-to-day processes in a compliant way.

Companies need to do the first for things like SOX and Basel II explicitly, but should also take this same kind of approach for other compliance mandates that are less explicit in how the process is to be audited. For example, USA Patriot or Privacy laws impose strict fines for breaches of the law. There are similarly stringent governance controls for financial advisors and clinical trial management both of which require rigorous and regular reporting. Companies currently take it upon themselves to document their policy and process and self-test, as they now must do for SOX or Basel II.

With SmartBPM, however, they can make a virtue of necessity, and extend their use of the technology to non-compliance areas. For example, if they have a policy that they return all customer calls in 24 hours, they should document the process and self-test against it and use the same infrastructure and diligence, emphasizing the more palatable goals of revenue growth rather than the punitive aspect of governmental

Regulation's a River, Not a Pond

Consider this. The federal tax code occupies two volumes, each thicker than the Bible. But the Code of Federal Regulations is much larger; it now occupies over 20 feet of shelf space. And it is growing. In 2004, the federal government printed 78,851 pages of new rules and announcements in the daily Federal Register. At four minutes per page, that would require 2.5 people reading eight hours per day for a year, just to keep up with the new rules and pronouncements (to say nothing of actually complying with them)."

– Susan E. Dudley, Director, Regulatory Studies Program,
Mercatus Center at George Mason University

- Electronic Signatures in Global and National Commerce Act
- Fair and Accurate Credit Transaction Act (FACT)
- Financial Services Modernization Act (Gramm-Leach-Bliley Act)
- Data Quality Act (DQA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Notification of Risk to Personal Data Act
- Freedom of Information Act (FOIA)
- Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley Act)
- USA PATRIOT Act
- Regulation FD (Fair Disclosure)
- Customs-Trade Partnership Against Terrorism (C-TPAT)
- Paperwork Reduction Act
- Family Educational Rights and Privacy Act (FERPA)
- Cadbury and Turnbull Reports (UK)
- European Union Directive on Data Protection
- International Convergence of Capital Measurement and Capital Standards: A Revised Framework (Basel II)

compliance.

SmartBPM in Action

Frameworks for Compliance

To ensure compliance, you must approach it as a set of linked control processes, each subject to configurable rules, assigned roles, and continuous monitoring. In a top-drawer BPM system, which frameworks assist in compliance? Pegasystems' Control and Compliance Framework is an example of a BPM framework that can help address compliance issues immediately.

Control and Test Management

Scope: Automates the creation, management, and documentation of financial and IT controls, policies, procedures, risk assessments, and self-tests.

Look for:

- Forms-driven workflow to gather information about objectives, risk assessments, and so on
- COSO and COBIT control frameworks already incorporated, plus flexibility to address other frameworks
- Excel™ self-test forms to support offline test execution, spreadsheet import, export, and validation
- Automatic creation of exception cases from failed test cases
- Based on process frequency, automatic test sample-size calculation
- Linkage of compliance objective to individual job specifications (tasks, goals, metrics, and incentives)
- Protection of rule forms from inadvertent or malicious changes
- Rule storage and retrieval, enabling processes to re-run under different rules (e.g., Q4/04 transactions under Q4/04 rules, even in Q1/05)

Compliance Exception Management

Scope: Manages the recognition, tracking, and resolution of identified compliance exceptions before they can become material weaknesses.

Look for:

- Management of the complete lifecycle - exceptions reporting,

- exceptions review, deficiency evaluation, and remediation tracking
- Identification of duplicate exceptions to cut down on unnecessary work and to locate systemic issues
- Guided determination of ICFR exception status - anomaly, deficiency, significant deficiency, or material weakness
- Creation of remediation plans as well as the delegation of necessary tasks

Change Tracking

Scope: For both applications and infrastructure, centralizes all enterprise requests and approvals for system modifications.

Look for:

- Release management that bundles and routes all changes associated with a single release, facilitates the shifting of changes between releases, and provides versioned release notes
- Automatic approval process that obtains the appropriate signoffs for different systems and types of releases (new/upgrade/patch)
- Automatic generation of alerts and triggers by service level agreement (SLA) for each application, escalations through multiple communications channels (even by minute, if necessary) depending on urgency level
- Enforcement of legitimate channels for emergency changes

Access and Permission Tracking

Scope: Tracks all requests for system access and creates a documented history of authorized approvals.

Look for:

- Customized approval processes for different systems
- Workflows for time-bound access authorization and automated notification when access is to be terminated
- Periodic business-owner review of all access privileges for audit compliance



About Pegasystems Inc.

Pegasystems Inc. (Nasdaq: PEGA) provides software to automate complex, changing business processes. Our Business Process Management (BPM) solutions provide organizations with the agility critical to managing growth, productivity and compliance. Our solution unifies pure-play BPM software with a sophisticated Business Rules Engine to drive business effectiveness. This patented technology enables organizations to "build for change" and overcome the execution gap that occurs as evolving business objectives outpace the ability of business systems to respond.

Pegasystems' award-winning BPM suite is complemented with best-practice solution frameworks based on more than 20 years of experience helping Fortune 500 and other leading corporations in the financial services, insurance, healthcare, manufacturing and government markets.

Headquartered in Cambridge, MA, Pegasystems has regional offices in North America, Europe and the Pacific Rim. For more information, visit www.pegacom.com.

Conclusion: The Future Of BPM and Compliance

As we have seen, there is no escaping that compliance is a fact of life not just in corporate America but around the world. The need for transparency and accountability in an ever increasing global economy is as important as prescriptive legislation. While BPM is becoming increasingly popular, it is entirely likely that the fact that so many organizations struggling to document processes and manage auditable change controls across multiple functional areas, may mark the tipping point for BPM to go mainstream. The time has come to both address compliance head on while acquiring a new path to agility.



For more information about Pegasystems, or to attend a SmartBPM Technical Briefing, call us at 1-866-PEGA-BPM. Visit us on the web at www.pegacom.com or e-mail us at info@pegacom.com.

Copyright © 2005 Pegasystems Inc. All rights reserved. PegaRules, Process Commander, simply smart BPM, SmartBPM and the Pegasystems logo are trademarks or registered trademarks of Pegasystems Inc. All other product names, logos and symbols may be registered trademarks of their respective owners. Some features noted in this document may not be available in the current version of PegaRULES Process Commander but are planned for subsequent versions. In addition, changes may be made from time to time at Pegasystems' discretion. This document does not imply any commitment to offer or deliver products or services or any warranty of capability or performance in a specific customer environment. This document remains the property of Pegasystems and must be returned to it upon request.

Corporate Headquarters

Pegasystems Inc. 101 Main Street, Cambridge, MA 02142-1590 USA
PHONE: 617.374.9600 FAX: 617.374.9620 WEB: www.pegacom.com

International Offices

Australia Canada France United Kingdom