

10 Steps To Business-Driven Compliance

A Zellerent White Paper

10 Steps To Business-Driven Compliance

A Zellerent White Paper

A fundamental fallacy is harming large, established businesses and threatening to destroy emerging ones. That fallacy is: when the regulators and their regulations come calling: (1) you must drop everything you're doing and (2) you must comply, comply, comply.

The second point is indeed true: you really had better comply. But the first point is not just false, but dangerous. The truth is that you should never drop anything, let alone everything. Rather, you should start using your compliance imperatives to serve your business objectives. Instead of submitting to the tyrannical rule of bureaucratic imperatives, squeeze every drop of value out of them.

Our experience is that turning compliance imperatives to your advantage isn't as hard as it sounds. Rather, it's a matter of perspective. If you start by viewing SOX, 21CFR11, HIPAA and other regulatory requirements as the death of your business, you'll never even stop to consider how you can simultaneously create best practices for your business. On the other hand, if you start by asking — even by demanding — maximum value from compliance imperatives, you'll end up making both the regulators and your stakeholders happy. This brief offers you a plain language roadmap to doing precisely that.

1. Identify & Align Core Business Objectives And Compliance Imperatives

Compliance imperatives never stand alone. They directly affect your business and your business processes. To achieve business-driven compliance, you first need to task two separate project managers or teams. One, unburdened by your business requirements, focuses on identifying your compliance objectives. The other, unburdened by your compliance imperatives, identifies your core business objectives and defines metrics that will objectively measure your success in meeting them. (Example of metrics range from downtime and availability to profitability, percentage of contracts won and IT spending increases.)

The result will be the clearest picture possible of what you need to accomplish. In contrast, assigning this task to one internal team will result in their constantly weighing compliance issues against business ones, precisely what you do not want to do initially. Only after you are armed with these parallel objectives will you be ready to consider trade-offs:

- First, review how meeting the compliance imperatives will improve your revenue potential. What contracts can you bid on as a result of your being compliant? What is their value?
- Second, identify those business processes that support your core business objectives. Ask how those processes can be modified to accommodate the compliance imperatives, while improving your metrics.
- Third, consider the additional information that you will gain from compliance and assess the value of this business intelligence, especially in terms of data mining.

Ultimately, you must take into consideration your business priorities and business-critical processes and look at adapting them to regulatory imperatives. This is the first part of a business-driven discovery process.

2. Identify Points of Leverage™: Assess Existing Internal Control Programs and IT-Enabled Compliance Reporting Processes

Very often, you can implement new or modified controls by leveraging your IT infrastructure. Therefore, you need to examine how to leverage existing controls and business infrastructure. Start with your existing internal control program and its compliance reporting processes. The goal is to maximize your ROI from the sunk costs of existing investments and to make new investments only when absolutely necessary. Identify those areas where alternatives exist (we call these Points of Leverage), so that you do not reflexively reach for your checkbook in order to comply.

There is an added benefit to this approach. Training your employees on new systems can be prohibitively expensive. When you instead leverage existing investments, you are also saving time and money because your employees already know how to use your existing applications and systems.

3. Choose A Business-Driven Framework For Establishing A Compliance Baseline

By now you know what you must accomplish business-wise and compliance-wise (Step 1), how to measure your success (Step 1) and what your Points of Leverage are (Step 2). Now, you must establish a baseline. This means creating policies, procedures, standards and guidelines for compliance (based on a framework consistent with your core business objectives), as well as documenting previously undocumented controls.

Here you must crystallize both your business and compliance objectives into policies and standards consistent with a framework. A productive approach is to adapt industry best practices and standardized frameworks (such as COBIT and ISO27001). This baseline would shield your business from disruptions while helping you fulfill your identified compliance imperatives.

4. Perform Compliance Gap Analysis Against The Baseline

This step is a standard gap analysis. Since you already have a baseline that enables you to implement business-driven compliance, you now need to assess your current state and identify the incremental work that you must complete to:

- Achieve that baseline; and
- Improve the results identified by your metrics.

5. Create Your Business-Driven Remediation Plan

You have moved from strategy to planning and execution. Armed with a gap analysis, your core business objectives and your compliance imperatives, as well as with your Points of Leverage, you can now create a remediation plan that is business driven.

- First, discuss the assessment findings with key stakeholders, including the people affected by and responsible for those areas in which you identified control deficiencies.
- Second, prepare a business-driven remediation plan that takes into account identified gaps, the input from stakeholders, your known business priorities, the existing negative impact that the identified deficiencies have on your business, and the scope of those deficiencies.

Note that, because of the earlier steps, your filling the gaps will automatically ensure that you address your compliance imperatives.

6. Execute Your Business-Driven Remediation Plan

Executing your remediation plan brings new challenges:

- You must design and implement controls that mitigate identified risks, plus be able to monitor their continued effectiveness.
- You must evaluate solutions, redesign existing controls, deploy new controls, handle project management and measure progress against often inflexible regulatory deadlines.
- Last, you must design and deploy instruments to measure and monitor, on a long-term basis, the effectiveness of your business and compliance imperatives.

Fortunately, by identifying Points of Leverage in Step 2, you will have considerably shortened not just your implementation schedule, but your timeline for employee compliance.

7. Document and Test Your IT Controls

By following the previous steps, you will have already ensured that you are dually satisfying your business objectives and compliance imperatives.

In this step, you must document all your deployed controls so that you satisfy all compliance mandates as well as all possible means of scrutiny. The best practice here is to use documentation templates recommended by your external auditors. Do not create your own, which will sow confusion in the auditors' minds. Give them what they want in the form they expect. Equally important, review all implemented controls for adequacy and test them for effectiveness.

Now you can confidently meet your business objectives and your compliance imperatives. Unlike firms taking a compliance-driven approach, you will not have sacrificed business success at the altar of compliance. Still, your job is not yet done. Three key steps remain: communicating your strategy to employees, continuously monitoring your compliance and actually getting through the audit. It is to these steps that we now turn.

8. Train Employees To Be Compliance Aware and Business Driven

The focus now shifts from internal IT processes to the human factor. It is human nature to want to get things done quickly. Even the most honest and ethical individual would rather fill out one form than 20. And this is where a business-driven approach to compliance pays unexpected dividends.

When an employee understands that filling out 20 forms (instead of one) is going to increase profitability and revenue as well as ensure high compliance, you have changed the employee's motivation from "command and control" to "this will help me and the company."

Therefore, when it comes to complying with controls, your training philosophy should incorporate these principles:

- Emphasize how the implemented controls contribute not just to the company's bottom line, but also to individual performance goals
- Emphasize that compliance is mandatory and that these controls ensure the required level of compliance
- Explain that noncompliance is unacceptable. By not complying, the company is risking severe fines and sanctions and second, by not implementing the compliance controls, the company is losing valuable business information that will help make it more successful.

9. Use Metrics To Continuously Monitor Business-Driven Compliance

Creating a business-driven compliance program and training your employees on it are not sufficient to ensure your future business or compliance success. To do this, you need to be able to continuously monitor, report and improve your compliance program in light of:

- Your evolving business objectives; and
- Evolving, changing and sometimes contradictory regulatory imperatives.

Therefore, after you have deployed your controls, you must ensure they continue to function as designed (as a whole) and to fulfill objectives (per each control). This means using metrics you have previously defined to measure the controls' effectiveness and objective business benefits. This demonstrates your commitment to managing future risks and satisfying external scrutiny. There are additional benefits: by analyzing your data, you can further improve efficiency and productivity, identify redundancies and reduce costs.

10. Breeze Through The Audit

By this step, you already have a working system that implements business-driven compliance, well-trained employees who support that system and monitoring that will alert you to business- and compliance-sensitive events.

The last step is for you to report and demonstrate compliance to external entities. You must produce all the narratives needed to satisfy regulatory mandates. Here it can be helpful to have an experienced, independent, objective party who can assist your organization through the external audit process by helping to:

- Identify and extract requested evidence; and
- Respond to inquiries and requests for explanations.

Such an organization can also conduct pre-audit assessments that help you prepare for the external audit and review. The result will be satisfied regulators and happy stakeholders.

Conclusion

When faced with the daunting challenges of compliance, it can be very tempting to seek shortcuts that satisfy the regulators but disregard your strategic goals. This relieves short-term pain, at the expense of long-term damage to productivity, profits and, often, employee morale.

At Zellerent, we advocate a different approach: Business-Driven Compliance. By starting with parallel inventories of your compliance requirements and strategic imperatives, you can extract maximum value from compliance activities and establish IT processes that improve productivity, profits and morale. Well after the audit is over, you'll be giving your employees better and faster visibility into the information they need to perform their jobs best and to make your entire business more efficient.

About the Author:

Kalyan Dishingia, CISA, CISSP, is the Vice President of Professional Services and a Principal Consultant for Zellerent. He has directed security and compliance engagements with organizations such as ING, Columbus Regional Hospital, Toyota Financial Services, and Fidelity. A trained ISO17799 Lead Auditor, he was also the Delivery Manager for the North American eSecurity Practice of an international IT services leader. He may be contacted at kalyan@zellerent.com.

About Zellerent:

Zellerent was formed by a team of seasoned industry executives whose combined experience spans several continents, multiple Fortune 500 companies and hundreds of successful engagements over two decades. Zellerent offers Business-Driven consulting expertise in the areas of IT Compliance, IT Security and IT Risk Management. Our practices include Regulatory Compliance (SOX, HIPAA, 21CFR11), Standards Compliance (ISO 27001, PCI DSS/VISA CISP), Security Deployments and Security Monitoring.

Zellerent's Business-Driven Compliance™ practice first assesses where you stand. Having identified the gaps between your current compliance status and your compliance and business imperatives, *remediation* can help you close that gap. With that problem solved, the solution, its associated controls and the in-compliance status need to be *documented*. Nevertheless, compliance that works today will not necessarily work tomorrow. *Monitoring* ensures that you will be prepared to address new regulations as they are introduced. Finally, *audit readiness* exercises give you a "dry run" before the auditors come calling.

Zellerent's Business-Driven Security™ practice *audits and assesses* the internal and external security threats to your organization. Next, armed with the proper requirements, we create an optimal security *architecture* for your enterprise, select the appropriate applications, and deploy your controls across it. As part of this effort, we also provide *awareness training* to ensure that your employees and stakeholders understand their responsibilities. Finally, we recognize that security threats change constantly, so we continuously *monitor* your deployed applications and controls to ensure they function as intended.

Zellerent is strictly vendor agnostic, identifying and deploying scalable best-of-breed solutions regardless of their source (public domain, 3rd party vendors, custom implementations).

Zellerent Inc.

39355 California St., Suite 309
Fremont, CA 94538

510-742-7400

www.zellerent.com
compliance@zellerent.com

Copyright ©2007 Zellerent Inc. All rights reserved. Reproduction or transmission without this notice is expressly prohibited. Zellerent, Business-Driven Compliance and Business-Driven Security are trademarks of Zellerent Inc. All other trademarks are the properties of their respective companies.