Strengthening Your Information Technology Infrastructure to Meet CFPB Expectations Regarding Third-Party Service Providers: Getting Started
Any time the government employs sweeping reforms to prevent the recurrence of a crisis we find executives struggling to adapt in the new environment. Such was the aftermath of the Great Depression.

At that time, recently elected President Franklin D. Roosevelt signed the new administration’s showcase response to “the perceived shambles of the nation’s financial and economic system,” as financial historian George J. Benston put it. The Banking Act of 1933, wrote Benston, missed the fundamental weakness in the U.S. banking system — the preponderance of unit banks, most of which had less than $2 million in assets. Many of these small banks collapsed in a heap. The Act also failed to repair another fundamental weakness in the system, the historical prohibition against interstate banking.

Congress, meanwhile, reacted as it had in past crises. Rather than seeking to uncover root causes of the Great Depression, Congressional hearings too often focused on affixing blame, attributing the crisis to, “(t)he presumed leaders of American enterprise — the bankers and brokers — who were guilty of disreputable and apparently dishonest dealings and gross misuses of the public’s trust,” wrote Benston. With blame for the crisis firmly placed on the shoulders of financial industry leaders, Congress went to work on the Banking Act of 1933 as a means to reengineer financial regulations. The goal: to ensure that such a financial crisis never occurred again.

Now that we’re approaching the half-decade mark of the worst economic crisis since the Great Depression, we find our government embracing many of the same Depression era themes as they blame business, rewrite the rules of financial oversight, and vow that such a financial crisis never occur again.

The Obama administration (and the Bush administration before it), diagnosed the fundamental problem as bad actors doing unethical things, eerily reminiscent of Roosevelt’s administration’s conclusion. The solution, they maintained, is to punish the industry and re-engineer financial regulations, again. Others have stopped short of calling the actions that led up to the crash unethical, instead pointing to aggressive pragmatists engaged in capitalist opportunism. The prescription remained the same: burn down the system and replace it.

Since 2008, the nation has witnessed numerous government initiatives aimed at reversing one of the most insidious fallouts of the housing bust: the foreclosure epidemic. Sadly, foreclosure is not a property of the crash, but rather a symptom.

The foreclosure “crisis” was only a crisis because the system was never set up to handle the volume. Before the crash, foreclosure was just one method of allowing the home finance industry to work through the occasional bad loan or borrower crisis. Like an unfortunate but beneficial purging process, a relative few loans were foreclosed each year, removing the burden from borrowers who could no longer repay and returning the real estate to the market for resale. Few problems were reported in the process because everyone knew that this was the only possible outcome, under the circumstances. When 1 out of every 10 loans went into default, the system was instantly overloaded, with disastrous results.

It is clear that the Administration’s vision of transparency, regulatory oversight, and consumer protection is driving much of today’s regulatory activism. Mortgage banking executives must come around to the notion that the old way of doing business is gone, and prepare accordingly by coming back to a more rational mortgage lending process. This will start with a new view of Information Technology.

Timeline for CFPB Rules Implementation

This summer, the Dodd-Frank Wall Street Reform and Consumer Financial Protection Act passed its second anniversary. The Consumer Financial Protection Bureau, the new federal super regulator spawned by the Act in Title X, celebrated its first anniversary. Tasked with writing over 400 rules to support the Act, and then to police those rules, the CFPB has become one of the busiest government agencies. By the end of its first year, the Bureau’s work had barely begun.

Among the rules that has garnered the most industry comment are loan officer compensation, consumer disclosure reform and the definition of the Qualified Residential Mortgage. None of these rulemaking efforts is complete and it not yet clear when the Bureau will complete them. This uncertainty has had a destabilizing effect on the financial markets.

Of primary concern to readers of this white paper is likely to be the CFPB’s efforts to write new rules for third-party outsourcing. The Bureau has already begun its work here but a rule has not yet been completed. Once the rule is published, the industry will have between 60 and 90 days to respond during the formal comment period. After the CFPB digests these comments, the final rule will be published. We expect to see that final rule in late January 2013. But by then, any lender that is not fully prepared to comply will be at a severe disadvantage.

What Mortgage Industry Leaders Are Doing Now

Mortgage executives are huddling with legal and compliance professionals in an attempt to discern the meaning of the hundreds of new requirements packed into the 2400-page Dodd-Frank Act and the nearly 2000 pages of related documentation4. At this stage, supervised financial institutions and supervised non-bank financial institutions alike are forced to deliberate over generalities as the final rules have not been made available. This may not be time wasted, however. For once the industry has its arms around the big-picture implications of the ACT, attention can be focused on an assessment of internal policies and procedures, contracts, training, due diligence, and ongoing monitoring of operations for compliance to consumer protection laws—all of which are likely to change as the new rules are published.

The CFPB has made clear its intent to hold supervised banks and nonbanks accountable for service providers’ compliance with federal consumer financial protection laws. In CFPB Bulletin 2012–03 the Bureau lays out its expectations regarding service provider oversight. The consensus opinion among mortgage industry observers we visited with for this paper is that compliance with these expectations will be daunting, expensive, time consuming, and in many cases require significant upgrades in information systems technology and data mining capabilities. Some have put the cost for the industry in the billions of dollars.

At Accenture, our research and experience in process reengineering and executing on business process outsourcing initiatives leads us to recommend that financial institutions do not settle for a wait-and-see approach to CFPB expectations for managing third-party relationships. Many lenders have taken that advice. Accenture has played an integral leadership role in many recent reengineering projects, helping numerous mortgage institutions analyze and overhaul their value chains to close gaps in reporting and compliance operations, productivity, internal cost controls, third party supplier quality, service, and price controls, among others.

Our experience clearly indicates that doing nothing to prepare for CFPB mandates is not a viable option. In fact, it invites significant risk. On the other hand, adequate preparation based on impact assessments that factor in multiple potential outcomes will always provide a better foundation from which to build future success.

Third-Party Risks

CFPB is not focusing on third-party suppliers solely in an effort to uncompliate the compliance process. The Bureau sees bona fide risk involved in these relationships and expects supervised institutions to take a very active role in mitigating those risks for the sake of consumers. These are the specific types of risk the Bureau has identified.

Strategic risk. Risk arising from deliberate activities by vendors aimed at taking advantage of clients. A vendor’s appraisals or service quality doesn’t match the client’s strategic goals; failure to provide benefits or to avoid the very risks a customer expects in utilizing an appraisal.

Shirking, or the Principal–Agent Problem. A form of strategic risk caused by a supplier’s deliberate under–performance while claiming full payment for agreed-to services. Occurs when the agent perceives an under–incentive to complete the job as agreed, and the client has insufficient information to monitor agent’s performance.

Poaching. Misuse of information provided to the supplier for legitimate contractual purposes. Poaching entails deliberate attempt’s to create unauthorized revenue streams at the client’s expense.

Opportunistic renegotiation. Unilateral change to terms of a contract after its inception when the client discovers that it has no alternative supply source(s) beyond those controlled by the vendor.

Operational risk. Risk of unintentional breakdowns in the supplier’s operations due to inadequate internal controls, production backlogs, under staffing, improper training, insufficient scaling up of operations during peak periods, etc.

Reputation risk. Risk of negative public opinion. Third-party actions resulting in dissatisfied customers; actions inconsistent with institution policies; inappropriate recommendations; security breaches resulting in the disclosure of customer information; violations of law and regulation that could harm the reputation and standing of the client organization in the eyes of the community it serves.

Transaction risk. Risk arising from problems with service or product delivery. This includes a third party’s failure to perform as expected, lack of an effective business resumption plan and appropriate contingency plans, weak control over technology used in the third-party arrangement, and/or unauthorized transactions or the inability to transact business as expected.

Credit risk. Risks that third party, or any other creditor in the third-party relationship is unable to meet the terms of the contractual arrangements with the financial institution or otherwise financially perform as agreed.

Compliance risk. Risk arising from violations of laws, rules, or regulations, noncompliance with internal policies or procedures, or with the institution’s business standards.

All of these risks can be mitigated by the institution if both the bank and the third-party service providers have implemented the right IT infrastructure. Without the right technology, no manual process will protect institutions from non–compliance.

In these early stages of compliance readiness, Accenture recommends to our clients that they conduct internal audits of each link in their value chain to identify real and potential areas of risk as it concerns the expectations delineated in CFPB 2012-03. This includes analyzing current processes and procedures in light of the anticipated reforms, assessing how these processes and procedures are likely to stand up to the new legislative and regulatory environment, and assessing how well the firm’s information technology and data storage and retrieval infrastructure(s) match up to anticipated CFPB expectations.

This last component, information systems and data infrastructures, deserves special attention. Relying exclusively on manual procedures, or even manual procedures combined or augmented by off-the-shelf financial, order tracking, or contact management software may only work for the smallest institutions and BPO providers. For the most part, the size and scope of the CFPB mandate will require automation — very likely sophisticated technology — to keep track of basic supplier information, due diligence processes and results, training and oversight programs, contracts, internal controls, and violation investigation and enforcement.

Capitalizing on IT to Manage to CFPB’s Expectations

CFPB Bulletin 2012-03 cites four basic elements of third party supplier scrutiny the supervised bank and nonbank are expected to consider: Due diligence, training and oversight, compliance contracts, internal controls/monitoring, and enforcement. It makes sense, therefore, to begin building an initial compliance audit around these elements now.

Taking a closer look at specifically what the regulator will focus on, we find:

Due Diligence. Conducting thorough due diligence to verify that the service provider understands and is capable of complying with federal consumer financial law;

Training and Oversight. Requesting and reviewing the service provider’s policies, procedures, internal controls, and training materials to ensure that the service provider conducts appropriate training and oversight of employees or agents that have consumer contact or compliance responsibilities;

Compliance Contracts. Including in the contract with the service provider clear expectations about compliance, as well as appropriate and enforceable consequences for violating any compliance-related responsibilities, including engaging in unfair, deceptive, or abusive acts or practices;

Internal Controls/Monitoring. Establishing internal controls and on-going monitoring to determine whether the service provider is complying with federal consumer financial law; and,

Enforcement. Taking prompt action to address fully any problems identified through the monitoring process, including terminating the relationship where appropriate.6

5. As presented in CFPB Bulletin 2012-03
6. CFPB Bulletin 2012-03
7. This scenario was developed by Jeff Schurman, CAE, Executive Director of Leading Causes LLC, an expert in third-party supplier relationship management, based on his conversations with mortgage and settlement services professionals.
8. Which could include, among others, Realtors, contract loan underwriters/processors, title agencies, appraisal management companies, credit reporting bureaus, home inspectors, and others who come into contact with consumers as the agent(s) of the mortgage lender.

The CFPB Compliance Audit: A Scenario

Several consultants in the mortgage banking and real estate settlement services industries worry, in reading between the lines of CFPB 2012-03, that a disconnect exists between what CFPB envisions as the technological capabilities of mortgage lenders to store and call up transaction-level data, reports, and related documentation, and what transaction management system technology (homegrown or ASP) currently has to offer. In fact, we have found that there is no sector of the mortgage business that is completely ready, from a technological standpoint, to meet the demands of a regulator such as CFPB.

This is not to suggest that the following scenario, selected as something of a “best case” scenario for conducting audits in a robust information technology environment, couldn’t happen. Surely, lenders, service providers, and IT vendors will attack the problem in anticipation of the January 2013 implementation of CFPB final rules. Yet it can be useful to envision in advance what a CFPB audit might look like as we begin our preparations.

The Audit

A compliance team assigned by bank management to work with the CFPB auditor escorts the official (most likely an attorney with prior mortgage banking experience) into a control room adjacent to the loan production operations floor. The control room will be well lit, air conditioned, and absent any personal materials, paper files, and non-essential supplies, but there will likely be a somber tone to the affair.

The auditor and (bank) compliance teams will take their seats at the conference table to discuss the purpose, agenda, and length of the visit. The auditor then interviews the team to acquaint herself with the firm’s compliance environment, training, internal controls, etc. The meeting adjourns and the auditor and team leader move to a large black consol reminiscent of a television or film production facility. On the wall there are six large flat screen monitors tied into a PC.

The bank’s team leader clicks a few buttons and brings on-screen a tutorial covering the functionality, report generation, document imaging, phone notes, and other electronic materials available to the auditor for review. Finished with the orientation they get to work. At the auditor’s request, they begin to look at randomly selected supplier files to assess the firm’s due diligence process and effectiveness. All or most of the images, notes, documents, and reports that the lender undertook to conduct due diligence of service providers appear on screen. So far, so good.

They move to employee training and oversight. They review training programs, results, personnel training records, and related materials. They bring up a diagram of the distribution of information to (FCFL) subject matter experts, what and how it is analyzed and conclusions of the impact rendered (and documented), and how it is used to affect day-to-day operations of the service organization. The team leader pulls up policy, procedures and compliance manuals (updated of course), training manuals, internal updates and various memoranda dealing with FCFL topics, internal audit data and results, training program attendance, cumulative and individual measures of compliance comprehension, periodic retraining schedules, etc. Not only will the auditor want to see records pertaining to consumer-interfacing employees but also their agents.8 She takes notes and asks questions. Then they move to the next CFPB expectation.

The CFPB Compliance Audit: A Scenario

Several consultants in the mortgage banking and real estate settlement services industries worry, in reading between the lines of CFPB 2012-03, that a disconnect exists between what CFPB envisions as the technological capabilities of mortgage lenders to store and call up transaction-level data, reports, and related documentation, and what transaction management system technology (homegrown or ASP) currently has to offer. In fact, we have found that there is no sector of the mortgage business that is completely ready, from a technological standpoint, to meet the demands of a regulator such as CFPB.

This is not to suggest that the following scenario, selected as something of a “best case” scenario for conducting audits in a robust information technology environment, couldn’t happen. Surely, lenders, service providers, and IT vendors will attack the problem in anticipation of the January 2013 implementation of CFPB final rules. Yet it can be useful to envision in advance what a CFPB audit might look like as we begin our preparations.

The Audit

A compliance team assigned by bank management to work with the CFPB auditor escorts the official (most likely an attorney with prior mortgage banking experience) into a control room adjacent to the loan production operations floor. The control room will be well lit, air conditioned, and absent any personal materials, paper files, and non-essential supplies, but there will likely be a somber tone to the affair.

The auditor and (bank) compliance teams will take their seats at the conference table to discuss the purpose, agenda, and length of the visit. The auditor then interviews the team to acquaint herself with the firm’s compliance environment, training, internal controls, etc. The meeting adjourns and the auditor and team leader move to a large black consol reminiscent of a television or film production facility. On the wall there are six large flat screen monitors tied into a PC.

The bank’s team leader clicks a few buttons and brings on-screen a tutorial covering the functionality, report generation, document imaging, phone notes, and other electronic materials available to the auditor for review. Finished with the orientation they get to work. At the auditor’s request, they begin to look at randomly selected supplier files to assess the firm’s due diligence process and effectiveness. All or most of the images, notes, documents, and reports that the lender undertook to conduct due diligence of service providers appear on screen. So far, so good.

They move to employee training and oversight. They review training programs, results, personnel training records, and related materials. They bring up a diagram of the distribution of information to (FCFL) subject matter experts, what and how it is analyzed and conclusions of the impact rendered (and documented), and how it is used to affect day-to-day operations of the service organization. The team leader pulls up policy, procedures and compliance manuals (updated of course), training manuals, internal updates and various memoranda dealing with FCFL topics, internal audit data and results, training program attendance, cumulative and individual measures of compliance comprehension, periodic retraining schedules, etc. Not only will the auditor want to see records pertaining to consumer-interfacing employees but also their agents.8 She takes notes and asks questions. Then they move to the next CFPB expectation.
Compliance Audit Readiness

Our research and experience gives Accenture a deep perspective on best practices in complying with fluid statutory and regulatory frameworks. It is neither an easy nor a necessarily formulaic process. It requires conjecture about the future regulatory landscape based on insights and assumptions extrapolated from official government policy and guidance documents, interviews with industry experts, and tools and techniques in reengineering and business process outsourcing honed through many years and multiple large-scale engagements. It will also require a keen understanding of the bank’s IT capabilities, limitations and required enhancements. With this in mind, we offer clients the following roadmap for completing an internal audit for compliance with CFPB Bulletin 2012-03.

Compliance Self-Audit Step 1: Education and a List of Required Reading

The CFPB has and will continue to issue documentation of its policies, procedures, and compliance requirements, in addition to the proposed final rule, and ultimate final rule. Many of these documents are instructive and offer glimpses of the Bureau’s expectations of supervised mortgage lenders and supervised service providers. No single resource can prepare an institution effectively as most of the rules have yet to be written. If you choose to tackle this part on your own, refer to the sidebar for a partial reading list.

Compliance Self-Audit Step 2: Upgrade Information Technology, Data Storage, Retention and Reporting Infrastructure

CFPB Bulletin 2012-03, although anticipated by the mortgage industry, was surprising in regard to the extent of authority the Bureau claimed for overseeing third-party supplier relationships. Not only was the bulletin issued as an announcement of the Bureau’s “expectations” of supervised financial institutions, thus allowing it to circumvent the Administrative Procedures Act as it applies to new rules, but it also, as we have pointed out, assumed a level of technological ability that many supervised institutions do not possess.

Upgrading today’s IT infrastructure will be a requirement for virtually ever firm in our industry, if for no other reason than automating as such of the compliance regime as possible will be necessary in order to prevent the new rules from becoming an undue burden on the firm’s normal operations. Migrating IT to the next level should be an organization-wide objective.

Because supervised financial institutions and their suppliers will both be under scrutiny, we expect these organizations to work together in collaborative efforts to upgrade the IT that serves both companies. We may even see different suppliers to the same supervised financial institution working together to upgrade their IT infrastructure to make compliance easier on their client, in fact, we expect this to emerge as a best practice.

The auditor is shown on-screen copies of executed contracts between the lender and service providers. This may also include contracts between the service provider and their agents. They will review a random selection of contracts for “clear expectations about compliance” and “enforceable consequences for violations.” The auditor pulls out a short list of a targeted selection of contracts with which the CFPB has specific questions. Once again the auditor takes notes about any instances of non-compliance with contractual requirements regarding consumer protections.

The auditor then brings on screen documentation showing that the mortgage lender has internal controls and monitors for FCFL compliance. Another screen displays documentation about several compliance problems identified through the monitoring process. The auditor analyzes the enforcement proceedings and the outcomes; in some cases, violators were terminated; others were issued written warnings.

Finally, the auditor assesses both the quantity of enforcement actions and the quality of those actions performed by the institution and its service providers.

A few clicks of the mouse later and a comprehensive report is created, including charts and graphs, statistical analyses, lender-rating scores for individual and overall performance to CFPB expectations, and canned commentary based on the auditor’s numeric ratings throughout the onsite visit. In this imaginary case, the institution survives the audit to lend another day, but we expect to see few if any lenders experience a 2013 post-QM, post full DFA implementation audit unscathed.

It won’t be enough to have your data ready, viewable and manageable internally. Lenders must be ready to comply with the regulator’s demand for full transparency, which will likely mean full access to all of the bank’s information technology. A daunting proposition.

Here is a partial bibliography of required reading:

CFPB Supervision and Examination Manual | October 2011.

Supervision and Examination Manual Updates.


Secure and Fair Enforcement (SAFE) for Mortgage Licensing Act | March 7, 2012.

FDIC – 6500 – Consumer Protection PART 226—TRUTH IN LENDING (REGULATION Z)

Bank Holding Company Act of 1956

Bank Holding Company Supervision Manual

Federal Deposit Insurance Act

9. Ibid.

10. Of both the mortgage lender and its service providers.
Accenture's experience in process automation suggests the following scenario to illustrate CFPB's likely (or hoped-for) vision of a typical on-site audit. What the nearby scenario suggests (see sidebar) is an audit environment featuring on-demand information call-up, onscreen review, state-of-the-art analytics, searchable policies, procedures and compliance programs, and customized on-screen report generation. Mortgage lenders should prepare their organizations for the initial round(s) of CFPB audits by upgrade their information technology and data storage, retention, and reporting infrastructure(s) accordingly.

For more information pertaining to the responsibilities of supervised bank or nonbank that has business arrangements with service providers, please review the CFPB’s Supervision and Examination Manual: Compliance Management Review and Unfair, Deceptive, and Abusive acts or Practices.


Conclusion

We hope we’ve demonstrated in this series of white papers that mitigating the risk of non-compliance with CFPB’s regulations regarding third-party suppliers is not a simple matter of dotting a few i’s and crossing some t’s. Many institutions will fail to meet these requirements and the consequences will be dire. The CFPB has already made it clear that penalties of up to $1 million per day of non-compliance will not be considered excessive. Non-compliance costs in that range can easily put firms out of business permanently.

All regulated institutions should begin now to assess their readiness, implement initiatives designed to ensure full compliance, discuss these changes with their third-party suppliers and, where appropriate, engage advisors to help them in this important process. Waiting for the rules to become crystal clear will be a serious mistake and institutions that adopt this approach will be lucky to survive. Proactive firms can be expected to thrive, even in this highly regulated environment.

Anatomy of a Robust Supplier Management IT Platform

- Organization-wide deployment
- Dashboards and compliance reports readily available to lender’s Board of Directors, senior managers, and compliance and FCFL enforcement staff
- Dashboards and compliance reports readily available to CFPB auditors/attorneys for review during on-site audits
- Analytical tools and automated techniques for monitoring compliance performance and red-flagging potential non-compliance issues and/or activities
- On-screen images of contracts, notepads, and documentation aimed at FCFL compliance
- Random-number generators to select individual service provider files for periodic audit
