



## Gearing Up for the Complicated Worlds of Outsourcing and Offshoring

### Outsourcing for Financial Institutions After Dodd-Frank: Regulation, Risk and Governance

The global economic crisis has powerfully re-taught a lesson that we have understood for some time — the whole world is economically connected. In response, the Dodd-Frank Act (DFA) has created new regulatory structures such as the Financial Stability Oversight Council (FSOC), and put more regulations in place to improve market transparency and to consolidate reporting in the hope that more information and more monitoring and more diligence will prevent the next economic crisis, or at least provide a longer lead time to try to avoid a crash or perhaps achieve a softer landing. The legislation was drafted in an intensely emotional climate and, as a result the DFA is imperfect. In some places, it is too complicated. However, in other places, for instance in its focus on transparency, financial stability and mitigation of systemic risk, it is praiseworthy.

Per Ben Bernanke, “Systemic risk can be broadly defined as the risk of the possibility that the failure of a large inter-connected firm could lead to a breakdown in the wider financial system.” The DFA uses the word “interconnectedness” many times in the statute when addressing financial stability. The DFA creates an analytical regulatory environment with a very strong focus on risk. In this context, risk means the possibility of an unexpectedly bad outcome from an event or events, which may or may not have been foreseen. “Interconnectedness” throughout the financial system means that risk cannot simply be evaluated as to the impact on a single company. Because all risk evaluation is contextual, financial services companies will need to create a number of methodologies for risk assessment.

So, how does outsourcing in financial services companies play a role in financial stability? A typical outsourcing transaction takes a function or operation that a company would have controlled and operated for itself, and puts that function or operation in the care and control of a third party. Risks arise because an outsourcing transaction connects a third party to the financial system through the contracting company. Under the Bank Service Corporation Act, third parties providing outsourced services to FDIC-insured banks are subject to examination and oversight by the Federal bank regulators. Third-party servicers also may be deemed to be “institution-affiliated parties” under the Federal Deposit Insurance Act, making them subject to the enforcement jurisdiction of the federal bank regulators. In other settings, the third party may not be regulated at all. In all cases, the third party has the potential to introduce risk to a financial institution and also to the financial system as a whole.

The outsourcing transaction itself involves something of a leap of faith. How much faith depends upon how critical the outsourced function or operation is to the primary business; how much diligence the company has performed prior to entering into the transaction; and, critically, how rigorously the company’s needs and expectations have been set out in the contract. In advance of every outsourcing transaction, a company needs to ask and answer the threshold question, “What happens to my company if the supplier or service provider fails?” Even more faith, diligence and documentation are required when the outsourcing transaction contemplates that the work is accomplished in another country. (This is commonly known as an “offshoring” transaction.) Each country has its own infrastructure, its own form of government, its own legal and political system and its own customary “way of doing things.” Consequently, there is more uncertainty when operating businesses in different locations, and that variable — call it “country risk” — is a further and very important consideration.

Generally, companies in the financial services industry broadly depend on their relationships with third parties. Because a single failure can have a profound impact on the enterprise, and present risk to the financial system, bank and securities regulators have had outsourcing guidance in place for many

years. However, the frightening and extensive domino experience of the global economic crisis has caused new emphasis on strengthening existing rules. For example, the Financial Industry Regulatory Authority (FINRA) has proposed FINRA Rule 3190, Use of Third-Party Service Providers, which emphasizes initial and continuing third-party due diligence, on-point contract terms, compliance with existing and specific function-related regulations and oversight control.

When the DFA addresses threats to financial stability in Section 113(a)(1), it provides factors to consider when evaluating risk. They include: nature, scope, size, scale, concentration, interconnectedness, and the mix of activities of the company.

Additionally, if the company is a bank holding company with total consolidated assets of \$50 billion or more, or a non-bank holding company supervised by the Board of Governors of the Federal Reserve System (or any subsidiary of such company), it will need to be prepared to submit certified reports to the FSOC regarding, among other things, “systems for monitoring and controlling financial, operating and other risks,” and “the extent to which the activities and operations of the company, and any subsidiary thereof could, under adverse circumstances, have the potential to disrupt financial markets or affect the overall stability of the United States.”

Financial services companies may need to take action to create or enhance their supplier governance programs in order to comply with the DFA, and to provide correct data for the necessary reporting. In addition, financial services companies must review existing agreements and relationships to assure that risks have been evaluated in context, and appropriately addressed in the outsourcing contract terms. New outsourcing contracts will require more specific compliance language for a successful result in a regulatory examination, investigation or litigation.

Years ago, the bank regulators, under the banner of the Federal Financial Institutions Examination Council (FFIEC), issued extensive guidance concerning outsourced relationships. Financial institutions were advised to conduct multi-factor diligence on their suppliers at the outset of the relationship. Often diligence was performed, a contract signed, or perhaps the company refreshed the analysis on an annual basis and then put the contract in storage. That level of governance will no longer suffice. In addition, in December, 2011 the Federal Reserve Board (FRB) issued its proposed enhanced prudential requirements, which includes new risk committee and enterprise-wide management requirements for covered companies. These requirements would apply to nonbank companies supervised by the FRB, bank holding companies with greater than \$50 billion in assets and publicly traded bank holding companies with greater than \$10 billion in assets.

In order to meet a company’s obligations under the existing and proposed bank and broker-dealer regulations, DFA, or prudential risk management requirements, active monitoring and management of third party relationships is required, and well-drafted contracts are essential.

The question arises, “How do you take account of outsourcing controls in the new regulatory environment?” In addition to the DFA, FINRA, existing bank regulations and post-DFA guidance above, in June of 2011, the Basel Committee on Banking Supervision provided guidance when it published, “Principles for the Sound Management of Operational Risk.” In the context of outsourcing, the Basel Committee suggests:

“Outsourcing policies and risk management activities should encompass:

- a) Procedures for determining whether and how activities can be outsourced;
- b) Processes for conducting due diligence in the selection of potential service providers;
- c) Sound structuring of the outsourcing arrangement, include ownership and confidentiality of data, as well as terminations rights;
- d) Programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider;
- e) Establishment of an effective control environment at the bank and the service provider;
- f) Development of viable contingency plans; and
- g) Execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.”

For examination and reporting purposes, the financial service company needs to demonstrate that:

- It has an inventory of all of its third-party relationships; (since contracts are signed or may expire on a daily basis, the procedures supporting the inventory will need to be frequently refreshed);
- Risks in each transaction have been identified, evaluated and documented; procedures are in place to monitor each transaction and its risks regularly, to ensure that levels of risk tolerance have not

deteriorated;

- Actions taken toward risk mitigation or risk transfer are clearly articulated in writing (e.g., contract terms, insurance, contingency plans);
- A process or processes are in place to actively monitor third party performance to support the company's various reporting obligations; and
- Risks in transactions have been evaluated at the individual level and have also been examined in the aggregate (e.g., are there too many eggs in one basket?).

At the end of the day, the financial services company will need to demonstrate that it has command of its third-party support. There is no doubt that such a governance program is a significant undertaking. However, if done correctly, the required diligence efforts will prevent or mitigate the impact of an unexpectedly bad outcome to the franchise. In addition, the work can be repurposed internally so that the same information from governance programs, contract review and creation feeds DFA financial stability reporting, proposed FINRA requirements, SEC CF Disclosure Guidance: Topic No. 2, Cybersecurity (October 13, 2011) as it relates to outsourcing, and resolution planning and reporting (a.k.a. living wills).

Beyond bank and broker-dealer regulation, outsourcing strategy must also consider other variables such as the Patriot Act (Pub. L. No. 107-56, 115 Stat. 272 (2001), *reauthorized* by Pub. L. No. 109-177, 120 Stat. 192 (2006), Pub. L. No. 112-3, 125 Stat. 5 (2011)), regulations of the U.S. Treasury Office of Foreign Asset Controls (OFAC), the Foreign Corrupt Practices Act (15 U.S.C. § 78dd-1, et. seq. (2011)), U.S. export controls regulations, privacy (*see*, for example Gramm-Leach-Bliley Act at 15 U.S.C. § 6801 (2011) and Securities and Exchange Commission Reg. S-P), each of which has its own requirements. These are all “gears” in the outsourcing strategy machine that must be properly meshed in order to preserve transaction validity and transaction economics.

All of these regulations represent a simple recognition that the world has become more complicated as it has become more “interconnected.”

Governance programs and outsourcing contracts need to be carefully structured so that they are not so burdensome that business stalls or stops. There is a delicate balance between being nimble enough to stay competitive in your business and smart enough to know, understand and account for risk.

[Return to Table of Contents.](#)