Digital
White Paper
March 2015
Page 1

BLM Bulletin

THIRD-PARTY Contract Elements

According to the FFIEC, vendor risk assessment is a critical component of a financial institution's Information Security Program but,

"the contract is the single most important control in the outsourcing process."

The review of these contracts by regulators is not a new part of the examination process but has become an area of increased scrutiny and regulators are looking for specific elements to these contracts. Following are 18 elements that should be included or considered in all vendor contracts:

- Scope of service
- Performance standards
- Security & confidentiality
- Controls
- Audit
- Reports
- Business resumption & contingency plans
- Sub-contracting and multiple service provider relationships
- Cost
- Ownership and licensing
- Duration
- Dispute resolution
- Indemnification
- Limitation of liability
- Termination
- Assignment
- Foreign-based
- Regulatory Compliance

Not all contracts, even with critical vendors, will contain all of these elements. But each of them represents an important factor for consideration as contracts are negotiated (or re-negotiated). Required elements will be determined by a financial institution's vendor risk assessment program.[1]

~Tom Hinkel, Complianceguru.com

VENDOR Management

OVERVIEW

Outsourcing services through experienced third-party vendors, allows financial institutions (FIs) to quickly **improve the quality of its services**, **increase its operational or financial efficiencies**, and, often times, **reduce costs**. FIs outsource to take advantage of many different benefits such as expanding the availability of services, and accelerating the delivery of such services which allows management to increase its focus on their core business functions.[2]

In most cases these third-party vendors are seen as an extension of the FI; and the FI may be branding these products and services with the FI's name but if a problem occurs such as a data breach, a disruption in company services, or the failure of a new product or service, customers are likely to point to the FI, not the vendor. As the benefits of using a third-party vendor may be great, so is the increased possibility of risk. Because there is no way to outsource the risk and, in the end, the FIs are ultimately responsible — the impact on their reputations, financial viability and customers may be significant.[3] As a result, examiners are increasing their scrutiny of third-party vendors and expect FIs to proactively identify potential risks, verify compliance and monitor changes through their vendor management program.

Each agency (OCC, FDIC, FRB and NCUA) of the Federal Financial Institutions Examination Council (FFIEC) have all issued updated rules and bulletins that require FIs to strengthen their vendor management program on third-party vendors deemed **critical** to their operations. Today, the definition of critical has expanded to include anything that might affect a loan, an ability to meet a consumer law, the company's brand or reputation, or its ability to defend itself against cyber-attacks, to name just a few.[4]

While a single vendor may provide several different services, the risks associated with each arrangement can be quite different. Plus, not all vendors are created equal — some services and relationships may be more critical than others and some vendors may have more robust risk management than others.[5] Based on the type of operation or service they are providing it can help to divide third-party vendors and their associated risks into categories. There are a number of risk categories FIs may want to consider when dealing with third-party vendors — including:

- **Strategic risk:** can arise from adverse business decisions and may result in adverse effects to earnings and capital. Not choosing the correct third-party service provider may result in unnecessary costs to the institution.
- **Reputational risk:** this can result from poor service from third parties or from customer interaction that is not consistent with the overall standards of the FI. Sometimes third-party practices and activities may not be in line with the FI's practices or desired images.
- **Compliance risk:** when consumer or legal compliance controls are inadequate, or if an outsourced provider has inadequate control systems, compliance risk may occur.
- **Operational risk:** may result from technology failure, inadequate financial capacity to fulfill obligations or provide remedies, and fraud or error.[6]

FIs can expect examiners to ask to see their entire vendor management program, not just the third-party

Continued on other side

BLM Bulletin

reviews and financials, and not just on select vendors. Any vendor that could have access (even incidental access) to non-public information (yours and your customers) must be risk-ranked by your vendor management program.[7] And the process of evaluating vendors is far more detailed and should include risk-scoring them, micro-analyzing their numbers (financial stability, debt, revenue, profitability, their cost structure, and product strategy), conducting onsite audits, monitor them and be extremely thorough in drafting contracts and service level agreements.[8,9] But the complexity doesn't stop there; one requirement is the expectation that financial institutions (FIs) apply every control they would apply to their own third-party agreements to their vendors' third-party agreements. This means that FIs must ensure that not only their vendors are conducting background checks but that their vendors' vendors are as well.[10]

Current guidance is clear, however, as to where the responsibility lies. As summarized by the Federal Deposit Insurance Corp. (FDIC) in FIL-44-2008,

> *"An institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution."*

The board of directors must maintain effective oversight and ensure that effective controls are in place. Management must maintain effective oversight but must also effectively manage any outsourcing relationships.[11] Due to the risks and regulatory compliance requirements the FI's upper management deems vendor management to be a company-wide issue.

Seven suggested principles for engaging in business with third-party vendors:

- **Implement a comprehensive policy** to guide the assessment of whether and how activities can be outsourced appropriately
- **Establish a comprehensive outsourcing risk management program** to address outsourced activities and relationships with service providers

- Ensure that **outsourcing arrangements** do not diminish the FI's ability to **fulfill obligations to customers or regulators**
- Conduct **appropriate due diligence** in selecting third-party providers
- Ensure that outsourcing relationships are **governed by written contracts**
- **Develop and maintain contingency plans**, which should also provide for periodic testing of back-up facilities
- Take appropriate steps to require that service providers **protect confidential information**[12]

An effective vendor management program can yield additional value far beyond reducing risk and satisfying regulatory requirements. A well-constructed vendor management program can increase net profits, improve contract terms, reduce costs from audits, and encourage better performance from vendors.[13] But if FIs don't comply, they could take a hit to their reputation and incur significant fines and other penalties.

BLM can help streamline your operation through the many hardware and repair services we provide. You can decrease the number of vendors you use for these services by working with only one company: **BLM Technologies**. Our solutions help you to save resources, sustain systems/processes, secure customer information which will strengthen your customer relationships. We work with many FIs throughout the USA including 2 of the top 5 and have strict protocols for **information/data security, physical site security, background checks** and **vendor viability** — all compliant with your vendor management program. Our leadership is well recognized through the strong relationships we have with our world-class technology vendors, our customers and competitors. All it takes is one call to BLM because we have the *solutions you can bank on*.

VENDOR Management

BLM Headquarters & National Service Center
15300 25th Ave N, Ste 600
Plymouth, MN 55447

To Learn More:
www.blmtechnology.com

Contact Us Today:
Tel: 1-877-287-6435

Sources Cited within this BLM Bulletin: 1 from the Compliancegru.com/2012/02/single-most-important-control-in-the-outsourcing-process/. 2,6,11,12 from Outsourcing and Vendor Management – Partnership for Progress. 3, 5 from Deloitte: Managing Vendor Risks: Three Lines of Defense for Banks. 4,8,9,10, from a five part article series by Penny Crosman on vendor management published online in the American Banker: Bank Technology News. 7 from the Compliancegru.com/2011/12/2012- compliance-trends-part-2-vendor-management/. 13 from the ITM Corporation: Vendor Management by Banks – Beyond Compliance.

BLM TECHNOLOGIES
Solutions you can bank on.