



***20/20 Vision for Vendor Management & Oversight***

2013 WBA Technology Conference  
September 17, 2013

Ken M. Shaurette,  
CISSP, CISA, CISM, CRISC, IAM  
Director IT Services

COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---

---

---


---

---

---

---

---



**Disclaimer**

The views set forth are those of this presenter and do not necessarily reflect the views of the Federal Financial Institutions Examination Council, or those of the Federal Deposit Insurance Corporation.

The presenter is not an examiner nor has he ever been and does not intend to ever be. He does provide almost 30 years experience from listening to people complain about various regulations.

» "Ken M. Shaurette"

2

COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---

---

---


---

---

---

---

---



**Bank Service Company Act - FIL-49-99**

Section 7(c)(2) of the Bank Service Company Act states that any FDIC-supervised institution that has services performed by a third party "shall notify such agency of the existence of the service relationship within 30 days after the making of such service contract or the performance of the service, whichever occurs first."

Section 3:

- Check or deposit item processing.
- Core processing.
- Preparation and mailing of checks, statements, or notices.
- Any other clerical, bookkeeping, accounting, statistical, or similar functions.

COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---

---

---


---

---

---

---


---

**Vendor and Third-Party Management** 

Financial institutions should establish and maintain effective vendor and third-party management programs.

**WHY?**

Source: NIST Special Publication 800-30.



COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---


---

---


---

---

---

**Why?** 

- because of the increasing reliance on nonbank providers
- complex nature of arrangements with outside parties; and
- ensure adequate due diligence for the **engagement** of the relationship and **ongoing** monitoring.



COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---


---

---

---

---

---

**Risk Assessment** 

The first step in the risk assessment process is to ensure that the proposed relationship is consistent with the Bank's strategic planning and overall business strategy.

Risk assessment is fundamental to the initial decision of whether or not to enter into a vendor relationship.



COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---

---

---

---

---

---

**Managing Third-Party Risks** 

Four Elements of Managing Risk

- Risk Assessment.
- Due Diligence.
- Contract Structuring.
- Oversight.



COMPLIANT. CONSISTENT. CONFIDENT

---

---

---

---

---

---

---

---

**Board and Management Policy Responsibilities** 

- Establish and approve risk-based policies
- Policies must recognize risk from outsourcing
- Appropriate to size and complexity



COMPLIANT. CONSISTENT. CONFIDENT

---

---

---


---

---

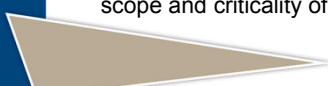
---

---

---

**Factors to consider include:** 

- Ensuring each outsourcing relationship supports the institution's overall requirements and strategic plans;
- Ensuring the institution has sufficient expertise to oversee and manage the relationship;
- Evaluating prospective providers based on the scope and criticality of outsourced services;



COMPLIANT. CONSISTENT. CONFIDENT

---

---

---

---

---



---

---

---

**Factors to consider include:**

- Tailoring the enterprise-wide, service provider monitoring program based on initial and ongoing risk assessments of outsourced services; and
- Notifying its primary regulator regarding outsourced relationships, when required by that regulator.



COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---

---

---

---



---

---

**Due Diligence**

Third-Party Evaluation Criteria:

- Financial Condition.
- Experience.
- Business Reputation.
- Strategies and Goals.
- Complaints, Regulatory Actions, or Litigation.
- Ability to perform using current systems.



COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---

---

---

---



---

---

**Due Diligence**

Third-Party Evaluation Criteria (continued):

- Use of Subcontractors.
- Scope of Controls, Privacy Protections, and Audit Coverage.
- Business Continuity Plans.
- Knowledge of Consumer Protection Laws and Regulations.
- Management Information Systems.
- Insurance Coverage.



COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---

---

---

---

---


---

**Policy Handout - Discussion**



Policy

- Third Party Vendor Management Policy



COMPLIANT. CONSISTENT. CONFIDENT

---

---

---

---

---

---


---

---

**(1) Third Party Vendor Management Policy**



To comply with the Bank Service Company Act any vendor meeting requirements of FIL-49-99 will require reporting to the Bank's federal banking agency in writing of contracts or relationships. (Refer to Notification of Performance of Bank Services form in the Vendor Management Program for more information.)



COMPLIANT. CONSISTENT. CONFIDENT

---

---

---

---


---

---

---


---

**(1) FIL-49-99 Info Form - Discussion**



Federal Deposit Insurance Corporation

- NOTIFICATION OF PERFORMANCE OF BANK SERVICES Form



COMPLIANT. CONSISTENT. CONFIDENT

---

---

---


---

---

---


---

---

**(2) Third Party Vendor Risk Rating** 

Vendor Management Program

(2) The Bank will maintain a Vendor Management Program that requires all vendor's to have undergone a basic risk assessment that will classify the vendor as CRITICAL, IMPORTANT or INCIDENTAL (high, medium or low risk). High risk vendors will include all vendors that are Critical to the Bank's continued operations and/or have access to confidential information (i.e. nonpublic personal customer information - NPI).



COMPLIANT. CONSISTENT. CONFIDENT

---

---

---

---

---

---

---

---

**(2) Vendor Risk Rating Handout** 

Vendor Risk Rating List



COMPLIANT. CONSISTENT. CONFIDENT

---

---

---


---

---

---


---

---

**(3) Vendor Selection Policy** 

New Vendor / Product Selection:

(3) Vendor Management requires that on vendor selection a minimum of two (2) vendors are evaluated during any product/service selection (three (3) preferred). If it is not possible to review at least two vendors the exception must be justified, documented and board approved. Vendor risk assessment will be included as part of the new product risk assessment process. Selected vendor will be risk assessed and assigned a risk classification - CRITICAL, IMPORTANT or INCIDENTAL.



COMPLIANT. CONSISTENT. CONFIDENT

---

---

---

---


---

---

---

---

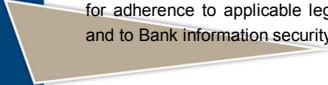
**(4) & (5) Vendor Risk Rating Handout**



Vendor Risk Rating List

(4) The Bank's third party vendor service agreements or contracts must include standards and provisions for auditing, monitoring and reviewing services that meet applicable legal and regulatory requirements. (e.g. control audit reports, security reviews and vulnerability testing (e.g. web application & network))

(5) The Bank must evaluate the associated information security risks and when reasonable, assess a third parties environment for adherence to applicable legal and regulatory requirements and to Bank information security policies and standards.



COMPLIANT. CONSISTENT. CONFIDENT

---

---

---

---


---

---

---


---

**(6) Risk Assess Vendors Handout**



Vendor Risk Assessment Survey

- What's Your Process?
- How do you decide a vendor is High Risk versus Medium?
- Do you reassess all vendors annually?



COMPLIANT. CONSISTENT. CONFIDENT

---

---

---

---


---

---

---


---

**(7) Risk Assess Vendors List Handout**



GLBA Customer Data Security

(7) High risk vendors and vendors with access to confidential information will be required to illustrate compliance to workforce clearance (e.g. background checking) equivalent to the policy established by the Bank. Control environments for vendors that store confidential information at their facilities must be equivalent to the controls that the Bank is expected to maintain if that information were stored onsite at the Bank.



COMPLIANT. CONSISTENT. CONFIDENT

---

---

---


---

---

---


---

---

**(8) Data Confidentiality**   
COMPLIANT. CONSISTENT. CONFIDENT.

Non-Disclosure Acknowledgement

- Non-disclosure
- Data Confidentiality Language
- Acknowledgement evidence



COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---


---

---

---


---

---

**Third Party Vendor Management Program & Procedures**   
COMPLIANT. CONSISTENT. CONFIDENT.

What Else

- Four Elements of Managing Risk
  1. Risk Assessment
  2. Due Diligence.
  3. Contract Structuring.
  4. Oversight.
- FDIC – Regulatory Supervision



COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---

---

---

---

---

---

**Contract Structuring & Review**   
COMPLIANT. CONSISTENT. CONFIDENT.

- Scope.
- Cost/Compensation.
- Performance Standards.
- Reports.
- Audit.
- Confidentiality & Security.

Legal Review?



COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---

---

---

---

---

---



**Oversight**



- Board and Management are Responsible.
- Monitoring.
- Reporting to the Board.



COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---

---

---

---

---

---

**FDIC Supervision of Banks' Third-Party Relationships**



- Board and Management Responsibility.
- Examination Procedures.
- Report of Examination Treatment.
- Corrective Actions.



COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---

---


---

---

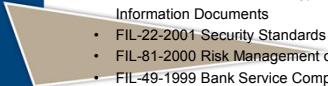
---

---

**Resources**



- FIPCO Website : [www.fipco.com/itservices](http://www.fipco.com/itservices)
- FDIC Compliance Manual — August 2012 : Third Party Procedures
- FIL-127-2008 Guidance on Payment Processor Relationships
- FFIEC IT Handbooks
  - Outsourcing Technology Services
  - Supervision of Technology Service Providers
- FIL-105-2007 Revised IT Officer's Questionnaire
- FIL-52-2006 Foreign-Based Third-Party Service Providers
- FIL-27-2005 Guidance on Response Programs
- FIL-121-2004 Computer Software Due Diligence
- FIL-23-2002 Country Risk Management
- FIL-68-2001 501(b) Examination Guidance
- FIL-50-2001 Bank Technology Bulletin: Technology Outsourcing Information Documents
- FIL-22-2001 Security Standards for Customer Information
- FIL-81-2000 Risk Management of Technology Outsourcing
- FIL-49-1999 Bank Service Company Act



COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---

---



---

---

---

---

**Questions?**



Ken Shaurette  
FIPCO  
Director IT Services  
kshaurette@fipco.com  
608-441-1251

COMPLIANT. CONSISTENT. CONFIDENT.

---

---

---

---

---

---

---

---