

THIRD-PARTY & VENDOR RISK MANAGEMENT

MANAGING THE RISKS RELATIONSHIPS CREATE

October 28, 2020

Stephen J. Bowe



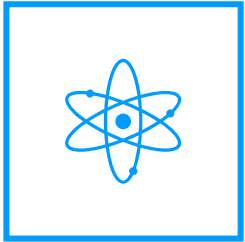
AGENDA

| | |
|----|--|
| 01 | Introduction to Third-Party Vendor Risk Management |
| 02 | Risks associated with using third-party/vendors |
| 03 | Protections for your institution |
| 04 | Regulators' expectations |
| 05 | Enforcement Actions |

The background of the slide is a dark gray network diagram. It consists of numerous circular nodes, each containing a light gray silhouette of a person. These nodes are interconnected by a web of thin, light gray lines, creating a complex, interconnected pattern that suggests a global or organizational network.

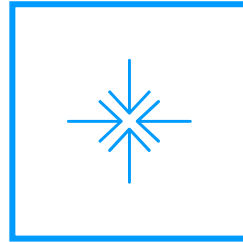
THIRD PARTY & VENDOR RISK MANAGEMENT BASICS

INTRODUCTION TO THIRD-PARTY/VENDOR RISK MANAGEMENT



Common Services Outsourced

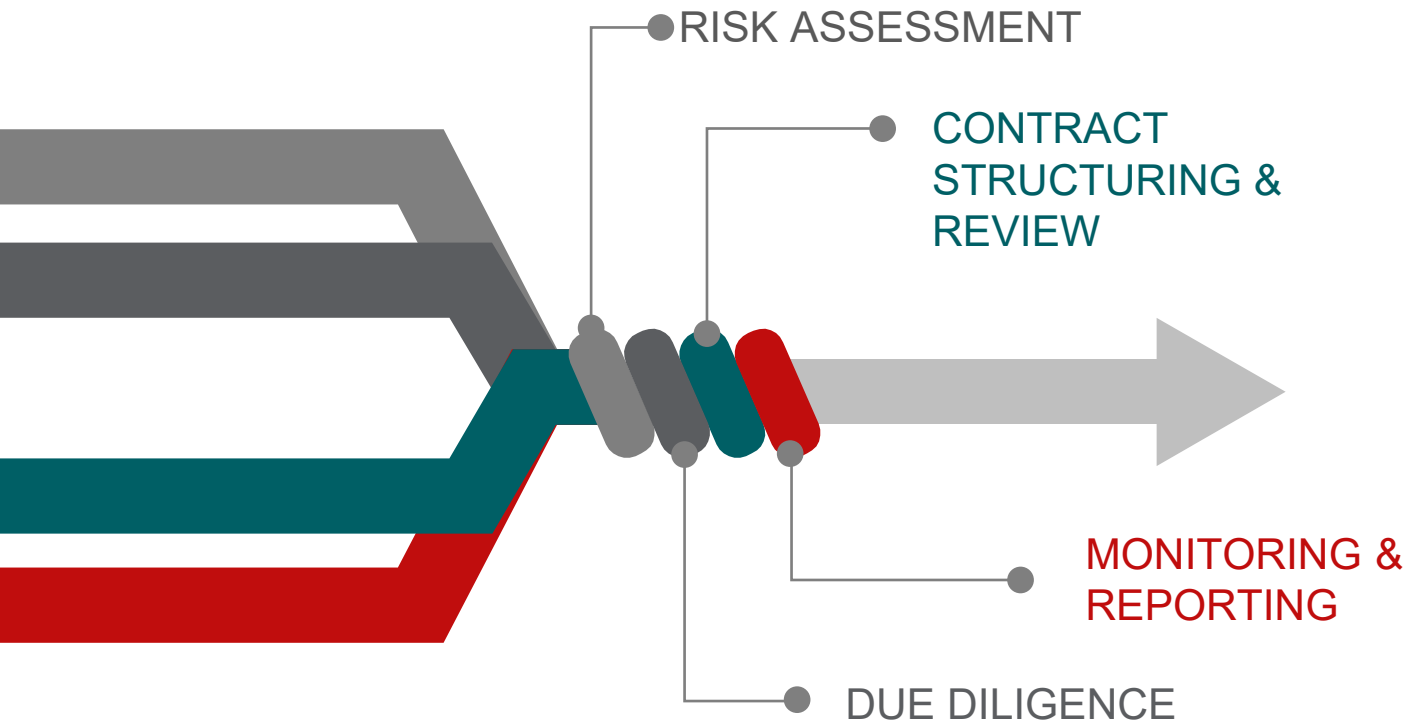
- Auditing
- Accounting
- Information Technology
- Marketing
- Wire transfers
- ATMs
- Servicing



Pros and Cons

- Institutions save time and resources
- Enables institutions the ability to offer their customers things they would otherwise be unable to offer at an affordable cost
- May carry risks even the vendor is not aware of
- Vendor may have a change in control or morals

PRINCIPAL ELEMENTS OF A GOOD VENDOR MANAGEMENT PROCESS



Emphasis and content for each varies depending on:

- Vendor under consideration
- Criticality of the service or product
- Magnitude and frequency of the activity
- Other risks identified within the relationship

“IMMC” risk management model

- Identify
- Measure
- Monitor
- Control

RISK ASSESSMENT CONSIDERATIONS



Strategy

Are you outsourcing for a product or a service?
Who is vulnerable in the relationship?



Risks

What are the risks associated with each relationship?



Required Resources

Consider the resources you will need to properly manage and supervise the relationship.

CONSIDER POSSIBLE UDAAP IMPLICATIONS

RISK ASSESSMENT

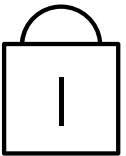
“What Could Possibly Go Wrong?”

Considerations



Multi-Specialist Group

To generate your list of hazards

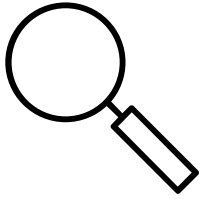


Compliance Officer

Involved in the process from the beginning

RISK ASSESSMENT

Addressing Risk Issues Related



Identify the Hazards

- Identify all possible worse-case scenarios
- Examples include: settlement failures, loss of customer information, public embarrassment, lawsuits, regulatory write-ups, and natural disasters



Control these Hazards

- Establish expectations and specifications for the new product
- Establish internal controls, reports, and requirements for the contract with the vendor
- Set your information security expectations
- Review your institution's plan for oversight



Estimate the Long-Term Financial Effects

- Review all the numbers provided to determine if they stand up
- Are the projections realistic?
- Take into account the cost of managerial resources required to monitor and other costs associated with singing on with vendor

DUE DILIGENCE



Identify Who The Potential Vendor Is



Request certified copies of articles of incorporation or other formation documents from a secretary of state where the company is set up



Obtain financial statements (audited if possible)

Pull reports from the Securities and Exchange Commission website for publicly-held companies

- Form 10-K – audited financial statements and reports of material litigation
- Form 8-K – unscheduled material events like enforcement actions, major operational problems, new lawsuits, etc.

DUE DILIGENCE



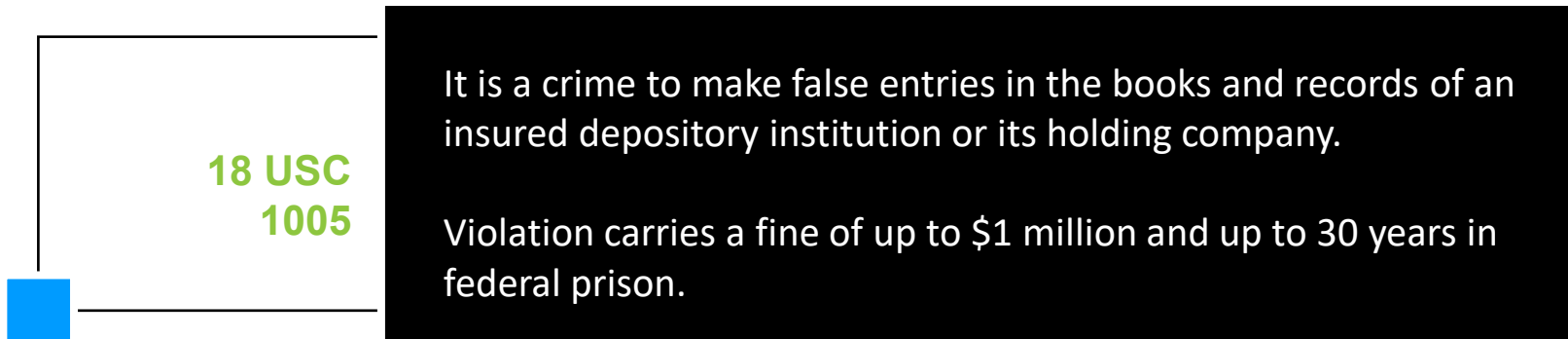
Identify Who The Potential Vendor Is

- ✓ Search websites of all the federal and relevant state regulators for any enforcement actions and similar items
- ✓ Call your regulator and inquire about the vendor
- ✓ Get references from the proposed vendor, and contact those references
- ✓ Perform web searches on vendor, its divisions and subsidiaries, and variations of their names

Document it all to the file!

DUE DILIGENCE

Document Accurately



DO

Paraphrase, as long as you do so accurately

Use estimates, opinions, or guesses as long as they are labeled as such

Be truthful and honest

DO NOT

Mischaracterize what you were told when you checked references

Put anything into your due diligence file you know to be inaccurate

DUE DILIGENCE

Vendor Staffing

Research vendor's personnel who will work on your project

- Look for experience in the particular field and regulatory knowledge
- Check out the accessibility and skills of the vendor employees who will deal directly with your customers

Look at the vendor's experience with turnover amongst key people

- If there is constant turnover, find out why
- Consider each side of the story:
 - The vendor
 - Regulators
 - Other users
 - Former employees

Have your Compliance Officer meet with the vendor's Compliance Officer

- Ask questions to bring out their knowledge, acceptance, and incorporation of the relevant laws, regulations, and current hot topics that affect the product

DUE DILIGENCE

Additional Resources and Personnel Requirements

Determine what, if any, additional equipment and personnel will be required to carry out your side of the contract

- Modems
- Additional communication lines
- More computers and software

Be sure to have the details approved and documented by the necessary personnel before signing the contract

- May need Board approval
- Hold officers responsible by documenting who tells you what

DUE DILIGENCE

Vendor Use of Subcontractors

Consider the following:



General Use

Whether the vendor uses, or intends to use, or is contractually allowed to use subcontractors



Limitations

Limitations that may apply when using subcontractors



Locations

What countries they are located in and what information (both on your institution and its customers) can be sent there.

- Know the laws on privacy, data protection, and related subjects for these locations.

DUE DILIGENCE

Vendor Disaster Recovery or Business Resumption Plan

Does it pass the credibility test?

Is the backup site in a location that will remain unaffected by the same disaster that affected the primary site, but close enough to allow for easy access to resources?

Are the resources there sufficient to handle the volume and deadlines applicable to the work?

Are the systems kept up to date to the same degree and as promptly as those at the primary site?

CONTRACT STRUCTURING & REVIEW

Contract Considerations

Vendor agreement needs to be a formal, written contract

Consider how big the proposed contract is going to be for the vendor

Legal counsel must be involved


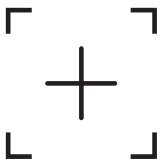


Rights and responsibilities must be spelled out in the contract

Agreement needs to specify:

- Term
- Details of the product or service to be provided, including quantified service levels and any additional services the vendor is to provide
- Regulatory compliance duties of the vendor

CONTRACT STRUCTURING & REVIEW

Service Level Agreements

| | | |
|---------------------------------|--|--|
| Formal Policies |  | <ul style="list-style-type: none">• That define their service level agreement policy |
| Monitoring Process |  | <ul style="list-style-type: none">• Formal and written• Documented recourse process to activate when a vendor doesn't meet its service level agreement |
| Escalation Process |  | <ul style="list-style-type: none">• For disputes about whether the service level agreement has indeed been breached• With a resolution process attached |
| Termination of Agreement |  | <ul style="list-style-type: none">• For failure to meet the requirements• Is the last resort |

CONTRACT STRUCTURING & REVIEW

Authorization to Audit Vendor

Contract should authorize the following personnel to have access to vendor records and personnel to assess its compliance with contract:

- Institution's regulators
- Compliance Officer
- Counsel
- Other necessary institution personnel

Contract must state:

- Who will be responsible for providing consumer-level disclosures?
- What use of the institution's premises, employees, and equipment are allowed to the vendor and its subcontractors?

AGENCIES RECOMMENDATION



Long-Term Performance

Contract be structured to reward long-term performance in a safe, sound, compliant way



Short-Term Incentives

Short-term incentives should be “strictly controlled”



Compensation Arrangement

Discourage the use of arrangements that might inappropriately steer borrowers into higher cost products

Contract Structuring & Review

Financial Information

Contract Requirements:

- How much will be paid, by what method, and upon what events or schedule
- Clear standards the vendor must meet to earn the compensation
- Management must periodically review the performance standards

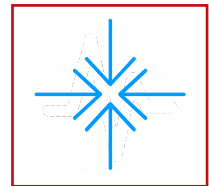
CONTRACT STRUCTURING & REVIEW

Other Contractual Obligations

Required management information reports need to be specifically detailed in contract by:



TYPE



FREQUENCY

Information security:

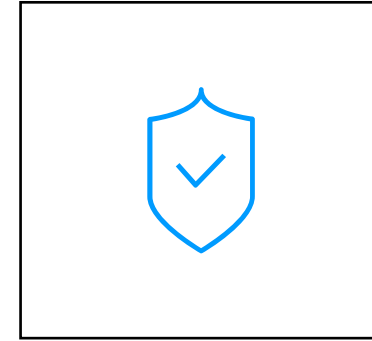
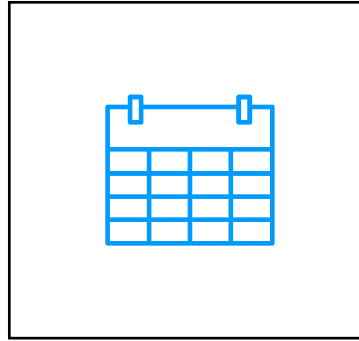
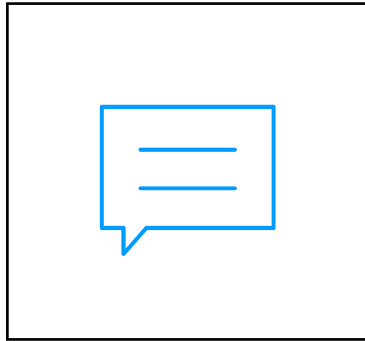
- Institution's information should be prohibited for **ANY** purpose other than that which is necessary for vendor to perform its duties under the contract
- Compliance Officer should ensure vendors adhere to the institution's privacy policy
- There should be a requirement that any known or suspected breach of information security be reported to the institution **IMMEDIATELY**



No Exceptions!

CONTRACT STRUCTURING & REVIEW

Customer Complaints



Complaints Come In

Have procedure in place for handing over complaints to vendor.

Handling of Complaints

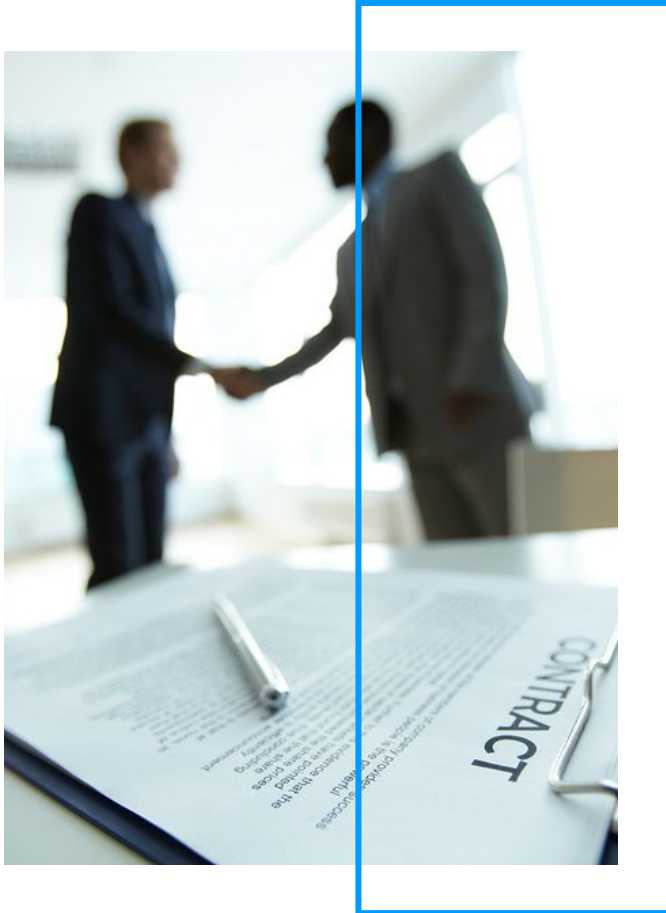
Copies of written complaints and written reports of oral complaints (and responses to them) must be provided to financial institution promptly.

Quality Assurance

Financial institution should review those complaints for quality assurance.

CONTRACT STRUCTURING & REVIEW

Operational Failures



Clearly identify in the contract:

- Who is responsible for fixing operational issues and getting the system back up and running again?
- Maximum timeframes for doing so
- Other vendor responsibilities:
 - Back-up responsibilities
 - Contingency plans
 - Back-up site locations
 - Other related vendor details

CONTRACT STRUCTURING & REVIEW

Monitoring and Insurance

Monitoring

Change management

- Have procedures in place on how to handle change management and any interruptions this change may cause

Access management

- System access reports should be reviewed periodically to ensure everyone who has access to the contracted service is authorized

Transaction monitoring

- Exactly what, when, and by whom will depend on the product itself

File backup

- What gets backed up?
- For how long?
- With what accessibility?
- By whom?

Insurance

Determine what kinds of insurance will be required of the vendor

- Look back to your hazards that you identified initially to help determine magnitude and likelihood of each instance
- Senior management should then decide whether a policy is required to cover some or all of that risk
- Deductibles and policy limited need to be considered

CONTRACT STRUCTURING & REVIEW

Contract Redux

Contract Default

Things to consider:

- What constitutes a default?
- Are there any “cure” periods before a default matures?
- Remedies for defaults
- Monetary payments and timeliness of those payments
- Procedures for termination of contract (if an option)
- Notice requirements for default
- Return of any institution property

Indemnification and Hold Harmless Provisions

Contractual structure needs to be followed and enforced

Provisions may not protect you:

- If the vendor does not have the financial means to repay
- The vendor’s insurance policy has lapsed
- From any violation of consumer protection laws and regulations which will go on your record and may require you to pay hefty fines to consumers or agencies for civil money penalties

Not always required or possible from some vendors, but be prepared to justify reasonableness if one does not appear in contract

CONTRACT STRUCTURING & REVIEW

Exit Strategies

Work with counsel to ensure contract:

- Is realistic
- Practical to implement
- As protective of your institution and customers as possible

Be sure the contract specifies
your rights in both cases

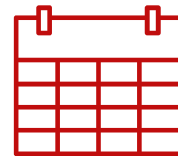
01

Normal
Termination



02

Early
Termination





Monitoring & Reporting

Who is Responsible for Oversight

- Compliance Officer should include consumer compliance issues in your oversight programs
- Board of Directors is required to be involved

Oversight includes:

- Service Quality
- Risk
- Financial Condition
- Controls and Reports

MONITORING & REPORTING

Oversight

Service Quality

- What is the customer's experience when dealing with this vendor?
- Is that experience representative of your financial institution's standards?

Risk

- How good are the vendor's risk management practices?

Financial Condition

- Run vendor's financial statements through the usual analysis that we do on borrowers
- Issues should be documented and action taken to remedy the problem

Controls and Reports

- Do they have them, and are they satisfactory? Be persistent with vendor until you have what you need to be satisfied and comfortable with what they provide you.
- Ensure their "controls" are sufficient – as they "control" the process, results of the process, and the potential liabilities arising out of that process
- Be sure to review their Service Organization Control (SOC) Reports and their SSAE 16 Reports (where available), and **DOCUMENT YOUR REVIEW!**

MONITORING & REPORTING

Your Risk Assessment

Risk assessment should be a **“living document”** that continually adapts to changes in the environment, and modified to keep your institution on top of the issues.

Vendor's general control environment:

Include provisions in contract that allow you to review their external and internal audit reports

Check the level of training and experience of their auditors

Document everything you find

MONITORING & REPORTING

Bank Service Company Act

Bank Service Company Act – 12 USC 1867

Obligations Under the Act:

- When an insured depository institution has certain services performed by a third-party, the institution must notify its principal federal regulatory agency
- Within 30 days after making of the contract or the performance of the service (whichever comes first)

What's Covered:

- Check and deposit sorting and posting
- Computation and posting of interest and other credits and charges
- Preparation and mailing of checks, statements, notices, and similar items
- Any other clerical, bookkeeping, accounting, statistical, or similar functions


Agency Vendor Guidance



CFPB Guidance

Bulletin 2012-03 (as amended by 2016-02)

- Conduct thorough due diligence to verify the service provider understands and is capable of complying with Federal consumer financial law
- Request and review the service provider's policies, procedures, internal controls, and training materials to ensure the provider conducts appropriate training and oversight
- Include in the service provider contract clear compliance expectations and consequences for violating those responsibilities
- Establish internal controls and on-going monitoring to determine compliance with Federal consumer financial law
- Take prompt action to address fully any problems identified through the monitoring process, including terminating the relationship where appropriate



“ The Bureau wanted to clarify that the depth and formality of the risk management program for service providers may vary depending upon the service performed – its size, scope, complexity, importance and potential for consumer harm – and the performance of the service provider in carrying out its activities in compliance with Federal consumer financial laws and regulations. ”

Compliance Bulletin and Policy Guidance 2016-02, October 31, 2016

AGENCY VENDOR GUIDANCE

CFPB Guidance

Under Title X, the CFPB has supervisory and enforcement authority over supervised service providers, which includes the authority to examine the operations of service providers on site.

CFPB has given fair warning that they may soon exercise this right and examine third party service provider operations as part of your examination.



OCC Guidance

OCC Bulletin 2017-7

- Tailored examinations commensurate with the level of risk and complexity of the bank's third-party relationships
- Assess the quantity of the bank's risk associated with its third-party relationships
- Assess the quality of the bank's risk management of third-party relationships involving critical activities
- Determine whether there is an effective risk management process throughout the life of the cycle of the third-party relationship

Enforcement Actions

ENFORCEMENT ACTIONS

CFPB

- The CFPB found that a financial institution's telemarketing vendor deceptively marketed the overdraft services and signed certain of the bank's customers up for overdraft services without their consent.
- CFPB ordered the financial institution to pay a \$10 million fine for illegal overdraft service practices.
- Additionally, the financial institution was ordered to cease using telemarketers to:
 - contact consumers about overdraft services;
 - improve its oversight of telemarketing vendors;
 - and contact all consumers who the financial institution's telemarketer enrolled to ask if consumers want overdraft services.

ENFORCEMENT ACTIONS

CFPB

- CFPB's examiners discovered a financial institution's call-center vendors engaged in deceptive tactics to sell the company's credit card add-on products.
- Consumers with low credit scores or low credit limits were offered these products by the financial institution's call-center vendors when they called to have their new credit cards activated. As part of the high-pressure tactics the financial institution's representatives used to sell these add-on products, consumers were:
 - Misled about the benefits of the products: Consumers were sometimes led to believe that the product would improve their credit scores and help them increase the credit limit on their financial institution's credit card;
 - Deceived about the nature of the products: Consumers were not always told that buying the products was optional. In other cases, consumers were wrongly told they were required to purchase the product in order to receive full information about it, but that they could cancel the product if they were not satisfied. Many of these consumers later had difficulty canceling when they called to do so.
 - Misled about eligibility: Although most of the payment protection benefits kicked in when consumers became disabled or lost a job, some call center representatives marketed and sold the product to ineligible unemployed and disabled consumers. Despite paying the full fees, they could not get all the benefits of payment protection; some later filed claims that were denied because their "loss" (e.g. loss of job or onset of disability) occurred prior to enrollment.
 - Misinformed about cost of the products: Consumers were sometimes led to believe that they would be enrolling in a free product rather than making a purchase.
 - Enrolled without their consent: Some call center vendors processed the add-on product purchases without the consumer's consent. Consumers were then automatically billed for the product and often had trouble cancelling the product when they called to do so.
- The financial institution had to pay approximately \$140 million to all of the estimated two million affected consumers.

RESOURCES

1. **FDIC – Exam Procedures –**
<https://www.fdic.gov/regulations/compliance/manual/complianceexaminationmanual.pdf>
.....
2. **FRB – Guide on Managing Outsourcing Risk**
<https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf>
.....
3. **FFIEC – Appendix J to the IT Examination Handbook –**
<https://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-j-strengthening-the-resilience-of-outsourced-technology-services.aspx>
.....
4. **NCUA –** <https://www.ncua.gov/Resources/Documents/LCU2007-13ENC.pdf>
.....
5. **CFPB – Bulletin 2012-03 –**
http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf
.....
6. **CFPB – Compliance Bulletin and Policy Guidance 2016-02, Service Providers –**
https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/102016_cfpb_OfficialGuidanceServiceProviderBulletin.pdf
.....
7. **CFPB – Supervisory Highlights, Issue 15 – Spring 2017 -**
https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/201704_cfpb_Supervisory-Highlights_Issue-15.pdf
.....
8. **OCC – Bulletin 2017-7: Third Party Relationships –** <https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-7.html>

QUESTIONS

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and investment management, finance, risk & compliance and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our website at www.capco.com or follow us on Twitter, Facebook, YouTube, LinkedIn, Instagram and Xing.

WORLDWIDE OFFICES

Bangalore • Bangkok • Bratislava • Brussels • Charlotte • Chicago • Dallas • Dusseldorf • Edinburgh • Frankfurt • Geneva • Hong Kong • Houston
Kuala Lumpur • London • New York • Orlando • Paris • Pune • Sao Paulo • Singapore • Toronto • Tysons Corner • Vienna • Warsaw
Washington, D.C. • Zurich

CAPCO.COM      