Top 10 Risks Third-Party Vendors Pose to Your Financial Institution

ncontracts
Risk Management Solutions

(888) 370-5552
info@ncontracts.com
www.ncontracts.com

EXECUTIVE SUMMARY: Vendor risk management is an ongoing process. It begins with due diligence before a contract is signed and continues with monitoring throughout the length of the relationship. Based on the inherent risk with the vendor, the financial institution should assess the potential risks of third-party vendors in some or all of these 10 risk categories: operational, transaction, compliance, credit, strategic, reputation, cyber, cloud, concentration and country.

When it comes to traditional lending risk, banks and credit unions have it down pat. They can look at customers and quickly determine whether they are a good risk. They carefully project interest rate risk. They can cite liquidity figures off the tops of their heads. But when it comes to vendor management, it gets trickier.

Third-party providers play a valuable role at financial institutions, allowing FIs to compete by offering a broader and more cost-effective mix of products and services, but they also pose risks. Every action (or inaction) a vendor takes has the potential to help or harm the FI. It is similar to hiring an employee, because the FI is responsible for the employee's actions or inactions. This responsibility makes proper due diligence and oversight of vendors a necessary part of the outsourcing process. FIs must be able to assess the potential risks a vendor poses and then measure how effectively that company mitigates risk.

This is an important task, and not just because regulators require it. Careful risk assessment and monitoring lets FIs know which vendors pose which risks, and whether the products and services a vendor provides deliver enough value to make up for the additional risk. It also reveals how much oversight and monitoring a specific vendor requires. Some FIs utilize labels to identify the inherent risk posed by a vendor like high, important, critical. It is certainly not a good use of resources nor a requirement to perform extensive due diligence before ordering a delivery from a sandwich shop. However, there is a big difference between the coffee vendor and the core processor.

If the financial institution policy is not well crafted, then it can easily create an enormous amount of work, which is not required by regulatory guidance. By comparison, a well-crafted policy will align inherent risk groups with control processes that align efforts with the risks that need to be mitigated. While the guidance from federal regulators is targeting critical, significant, or high risk vendors like core processors, each FI wants an inherent risk system that protects them from third party risk.

These risks from critical vendors come in many forms, with new threats regularly emerging. It's also a comprehensive process. Regulators expect FIs to address specific categories of risk for this type of vendor. Unfortunately, there is often overlap between the areas. FIs that choose to address risk in silos run the risk of duplicate efforts, contradictory results and missed connections that result in shortfalls. This is especially true since vendor risk management is an ongoing process, which begins with due diligence before a contract is signed and continues with monitoring throughout the length of the relationship.

FIs must be able to assess the potential risks a vendor poses and then measure how effectively that company mitigates risk.

Due diligence should cover all the major risks vendors pose. While different regulators use different names for different kinds of risk and some emphasize certain types more than others, these are the top ten risks:

1. **Operational risk**
2. **Transaction risk**
3. **Compliance risk**
4. **Credit risk**
5. **Strategic risk**
6. **Reputation risk**
7. **Cyber risk**
8. **Cloud risk**
9. **Concentration risk**
10. **Country risk**

Let's take a closer look at each of these areas to understand what steps FIs should take to investigate the risk exposure a vendor presents.

1. OPERATIONAL RISK

One of the broadest risks facing FIs that outsource is operational risk. Operational risk is the risk of financial loss when processes, people or systems fail. Sometimes it's the result of external events like a power outage, fire or flood. Other times it's the vendor's own internal issues, such as fraud, a hardware or software failure or an accounting error.

While it's impossible to guarantee that processes, people and systems are perfect, there are steps FIs can take to mitigate these risks. The key is ensuring that vendors carefully and consistently follow suitable and effective internal controls. Many vendors will provide the results of SOC 2 Type 2 audit tests to address non-financial business controls in areas such as security, availability, processing integrity, confidentiality and data privacy. This is a great starting point. Because operational risk is such a broad area, there are many areas to review. The good news is that many of these facets appear later when discussing other forms of risk. FIs that invest time in careful due diligence will see the benefit when that work can be applied to other areas.

Subjects to review include:

Data privacy. Governing access to electronic data and systems containing confidential client data is essential. Policies and controls should ensure the consistent security and confidentiality of customer information, including secure data disposal, data classification and confidentiality or non-disclosure agreements. There should be physical access restrictions at buildings, computer facilities and records storage facilities where customer data is stored. Customer information should be encrypted whether it's in transit or storage.

Threat assessment. There should be procedures to identify, assess and mitigate reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or systems.

Governance. Both the board and management should play a role in oversight. That includes defining roles and responsibilities, segregating duties and work environments and maintaining change management controls over software changes, application development and system maintenance.

User access. Policies and procedures should be in place to limit system access and eliminate non-active users or those who violate policies.

Employee evaluations and training. Background checks should be conducted before hiring. Personnel responsible for the design, development, implementation and operation of the system should be reviewed annually. There must be documented mandatory training and escalation procedures to address staff who fail to take training.

While it's impossible to guarantee that processes, people and systems are perfect, there are steps FIs can take to mitigate these risks.

Monitoring. Systems should be monitored with controls to detect actual and attempted attacks and intrusions into customer information systems. They should also protect data systems from theft and corruption. Penetration tests and/or vulnerability scans should validate the integrity of system security, and findings should be promptly investigated and resolved.

Incident response. There should be a plan of action when unauthorized access to information systems or facilities is suspected. Protocols should define the customer breach notification process along with a process for addressing customer requests and complaints.

Data security. Measures should protect confidential customer information and systems from destruction, loss or damage due to environmental hazards, failures or disasters. There should be periodic evaluations and/or ongoing monitoring to validate the operational effectiveness of information security policies and internal controls, including management reviews, internal audits and external examinations.

Data processing and transactions. Policies and controls should ensure that processing and data transmissions are complete and accurate through reconciliations, edit checks, system entry configurations, dual controls, job monitoring and management review. Processing and data transmissions/transactions should be validated through authentication protocols with inputs authorized through implementation reviews and management approvals. Timely job scheduling and transactions based upon predetermined schedules is necessary along with procedures and protocols to ensure that exceptions and issues are identified, escalated, tracked and addressed.

Subcontractor oversight. Due diligence, monitoring and oversight of critical third-party vendors is necessary.

2. TRANSACTION RISK

Sometimes networks go down. Yet no matter whether an outage or other business problem is caused by a natural disaster, cyberattack, equipment failure, fraud or other event, vendors must have plans and procedures in place to ensure service and product delivery is quickly restored.

While a vendor might not be able to fully disclose the details of its business continuity plan for security reasons, there are still plenty of ways to assess a vendor's preparedness and potential risk.

It's all a part of managing transaction risk, or the risk that a third party will fail to provide products and services as expected, adversely impacting the institution or its customers. Transaction risk differs from operational risk in that it focuses on contingency planning, but the two share many overlapping areas.

Mitigating transaction risk isn't just good business. It's a requirement of the FFIEC IT Examination Handbook Business Continuity Planning and Appendix J: Strengthening the Resilience of Outsourced Technology Services and other regulatory guidance. That why an FI must evaluate a vendor's business resilience controls to minimize financial loss and mitigate adverse effects of service interruptions. It must be certain that vendors will be able to meet service level agreements and recovery time and point objectives (RTOs).

This is best accomplished by addressing the following areas with vendors:

Planning. While a vendor might not be able to fully disclose the details of its business continuity plan for security reasons, there are still plenty of ways to assess a vendor's preparedness and potential risk. The vendor should review and test its business continuity planning/disaster response plan annually and share the results with clients. That includes the date of the last disaster recovery test of the production environment. Vendors should share the results, letting FIs know whether testing objectives were met and communicated to the board of directors.

Threat management. Vendors should conduct a periodic business impact analysis to identify and assess the likelihood and impact of threats that could interfere with their ability to meet service level

agreements. They should have clearly defined recovery time and point objectives (RTOs) for critical services, which may include mirrored backups and dual processing sites. Roles and responsibilities for disaster response (such as initial assessment, crisis management and communications) should be assigned. Pandemic planning is a must.

Recovery. Recovery capabilities should be assessed and monitored commensurate with the criticality of services provided. There should be redundant, backup or alternate power sources in place (such as generators). Alternate facilities for resuming critical services should be identified and critical data should be regularly backed up, mirrored and/or replicated.

Data protection. Data should be meticulously protected. There should be physical security controls and protocols to prevent unauthorized access to facilities or areas housing confidential customer information systems and data. These preventative controls include secure coding, firewalls, a demilitarized zone, secure network configurations, network segmentation, secure VPN's and logging. There must also be detective controls such as monitoring, intrusion detection systems and anti-malware software. Corrective measures such as patch management and risk and vulnerability remediation protocols should be defined and implemented. Vulnerability and/or penetration scans must be performed periodically.

Incident response. Another key element is an incident response and management policy or plan, which outlines how the vendor would manage and address a confidential data security breach or cyber-security incident. That includes a protocol to notify affected clients.

Subcontractors. Reliance on third-party providers, key suppliers, or business partners may expose FIs to points of failure that may prevent resumption of operations in a timely manner. Vendors should conduct their own risk assessments of all major risks, including credit, liquidity, transaction and reputation risk, among others.

3. COMPLIANCE RISK

Financial institutions must follow laws, regulations and rules, and should require their vendors to comply as well. Compliance risk is the risk that a third-party vendor will violate one of these orders or fail to follow the institution's own internal policies. This can have reputational, financial and regulatory consequences for the financial institution.

According to the OCC's Third-Party Relationships Risk Management Guidance,[1] compliance risk commonly occurs when:

- products, services, or systems associated with third-party relationships are not properly reviewed for compliance;
- the third party's operations are not consistent with laws, regulations, ethical standards, or the bank's policies and procedures;
- a third party implements or manages a product or service in a manner that is unfair, deceptive, or abusive to the recipient of the product or service;
- a bank licenses or uses technology from a third party that violates a third party's intellectual property rights;
- the third party does not adequately monitor and report transactions for suspicious activities to the bank under the Bank Secrecy Act or Office of Foreign Asset Control;
- a bank's oversight program does not include ap propriate audit and control features, particularly when the third party is implementing new bank activities or expanding existing ones;
- when activities are further subcontracted;
- when activities are conducted in foreign countries;
- when customer and employee data is transmitted to foreign countries;
- conflicts of interest between a bank and a third party are not appropriately managed;
- transactions are not adequately monitored for compliance with all necessary laws and regulations; and
- a bank or its third parties have not implemented appropriate controls to protect consumer privacy and customer and bank records.

[1] OCC Bulletin 2013-29. Risk Management Guidance. Subject: Third-Party Relationships. Appendix A: Risks Associated with Third-Party Relationships https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html#append-a.

It's not enough for a company to say it doesn't disclose breaches to third parties unless they are affected—agreements must spell out that clients will be notified.

Once again, compliance risk abuts several other types of risk including operational, reputation, country, transaction and cyber risk.

To assess compliance risk FIs should determine whether vendors are aware of both new and existing regulations and have policies and procedures in place to implement them. Audit and control features should demonstrate their compliance. This include logs and best practices for monitoring transactions for suspicious activity and compliance with others laws and regulations.

Data privacy is of particular interest to regulators making it important to ensure compliance with laws, regulations and best practices from OFAC, the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act, the Fair Credit Reporting Act and the Health Insurance Portability and Accountability Act. Vendor controls should be designed with these specifically in mind.

FIs can find information about these controls in vendor documents such as annual due diligence questionnaires, SSAE 16 reports and independent third-party reviews during annual SOC 2 audits.

Important areas to review include:

Privacy policy. Vendors need an information privacy policy and an information security program that's reviewed and/or updated periodically. It should include a risk assessment process to identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of information and assets. These threats must be evaluated, managed and monitored. There should also be secure disposal measures to properly dispose of unneeded consumer information.

Information security controls/practices. Vendors should encrypt all highly confidential information and authentication credentials, use VPN, appropriately segregate duties and require acknowledgement and acceptance of confidentiality/non-disclosure agreements before permitting access to confidential data or systems.

Security for personnel who will have access to confidential consumer information. This includes pre-employment background investigations and initial and ongoing information security training.

Physical security protocols and controls to safeguard facilities containing confidential data. All desktop-computing devices should be physically secured with locking devices. There should be a visitor access policy with 24/7 security personnel on site, closed-circuit surveillance throughout the facility and card-key access control with permissions assigned based upon job responsibility.

Security protocols and controls to safeguard electronic data. All desktop computers should require an individual identification and authentication at log on with formal policies to define password parameters. Access should be restricted based on job responsibilities and access rights should be reviewed periodically. There should also be termination protocols and checklists.

Network security protocols and controls to prevent and/or detect unauthorized access and cyber-security incidents. Look for anti-virus software on desktops, servers and host, with patches obtained from secure sites. Anti-malware software should be installed on critical servers and on end-point devices, with signatures updated nightly. There should be a defense in-depth program, including intrusion detection/intrusion prevention systems and

semi-annual threat and vulnerability testing and attack and penetration tests. Centralized monitoring via security incident and event management (SIEM) and perimeter firewall systems is necessary. So is an incident reporting and response program to address and manage confidential data security breaches and/or cybersecurity incidents. That includes client notification. It's not enough for a company to say it doesn't disclose breaches to third parties unless they are affected—agreements must spell out that clients will be notified.

4. CREDIT RISK

It doesn't matter how compliant, effective or technologically sound a vendor's product or service is if the company won't be in business very long. An FI that partners with a financially unsound vendor may find itself suddenly cut off from a critical product or service if that firm goes under.

That's why it's important to focus on credit risk, or the strength and ability of a company to manage debt and stay in business to ensure continued operations. The FDIC says that FIs should evaluate third-party vendor's financial condition at least annually[2] and that the review "should be as comprehensive as the credit risk analysis performed on the institution's borrowing relationships."

The good news for bankers and credit union professionals is that the board and management should be very experienced in evaluating businesses, audited financial statements and publicly available documents.

It doesn't matter how compliant, effective or technologically sound a vendor's product or service is if the company won't be in business very long.

Areas to look at include:

Financial condition. A company's liquidity and leverage figures reveal the strength of its condition. Assess the viability of an operation by noting cash, debt, debt to equity, interest coverage ratio and auditor's opinions of ongoing concerns.

Financial performance. Reviewing profitability and cash flow are essential. That includes revenue, gross margin, operating income or loss, operating margin percent, net income or loss, net margin percent, EBITDA, EBITDA margin percent, operating cash flow and free cash flow.

Litigation. Claims for punitive or exemplary damages from pending or threatened litigation can wreak havoc on the bottom line. Be aware of any legal action on the horizon, the potential fallout and what, if any, plans the company has to cover the damages.

Acquisitions. Acquisitions can expand a company's offerings, spread its resources too thin or rapidly increase the debt load. Look into pending acquisitions or sales and how that may impact the company's financial condition as well as other unfunded liabilities.

5. STRATEGIC RISK

Strategic risk is the possibility that a company doesn't make decisions that support its long-term goals. This can happen when risks aren't properly assessed; not enough thought and due diligence are put into new products, business lines or activities; or when the company undertakes an action that's not consistent with the company's goals or doesn't provide the expected return on investment, according to the OCC.[3]

Strategic risk impacts the viability of a business in the same way credit risk does. But instead of focusing simply on numbers, it involves reviewing how decisions are made and implemented and how a company responds to changing market conditions. A company that isn't managed well may not stay in business long or provide quality products and services.

[2] Financial Institution Letter. Guidance for Managing Third-Party Risk. June 6, 2008. https://www.fdic.gov/news/news/financial/2008/fil08044a.html.
[3] Risk Management Principles for Third-Party Relationships. A Telephone Seminar for Community Banks. Handout. August 2002. https://www.occ.gov/static/past-conferences-and-seminars/vmts-final-handouts.pdf.

Strategic risk is the possibility that a company doesn't make decisions that support its long-term goals.

The key areas to look at when assessing strategic risk include:

Background. It begins with basic background that includes the age of a company and the size of its market. Large nationwide providers tend to be stronger than smaller competitors. And the larger the client base, the more likely the company is to be stable.

Leadership. Determine who is responsible for achieving corporate objectives, oversight of operating functions and compliance with applicable regulatory requirements. You want to see that senior management and the board of directors are meeting to ensure business strategies are aligned with operations across the organization. At larger companies, executive management committees may provide oversight.

Operational controls and audits. It's not enough to have operational controls. They must be monitored through management reviews and internal and external audits. Annual independent audits should demonstrate the suitability and effectiveness of internal controls. Lines of authority and responsibility should be established. Managers should monitor reports and controls to provide reasonable assurances that activities are performed in a secure, complete, accurate and timely manner, and exceptions are identified, tracked, recorded and resolved.

Vendor management. FIs need vendor management programs and so do vendors. The risk assessment process/program should identify and mitigate risks that might affect a vendor's continued ability to provide reliable services to its users. This includes third-party oversight and monitoring, and identification and resolution of information security-related risks.

Business continuity. There should be protocols to mitigate or prevent business interruptions, and to respond, recover and resume critical business functions after an unplanned business disruption.

Outsourcing and offshoring. The vendor should know whether or not all operations and personnel are all located within the U.S. and whether or not it outsources to foreign/offshore service providers or subcontractors.

Notice that transaction, operational, country and cyber risks are all included when assessing strategic risk. Any method used to conduct a strategic risk assessment should leverage these overlaps to maximize efficiency.

6. REPUTATION RISK

Reputation is hard to earn and easy to lose. Whether its lawsuits, fraud or data breaches, consumers notice bad headlines and take their business elsewhere.

Consider the headache $18.4 billion-asset First National Bank of Omaha faced earlier this year when it came out that its credit card add-on vendor charged customers for credit monitoring services they didn't receive. Neither customers nor regulators differentiated between the bank and its vendor when assigning blame for ripping off customers. Not only did the bank pay millions in penalties to the CFPB and OCC, the bad publicity of newspaper headlines created costs that are not easily calculated from loss of goodwill.

Vendor mistakes like this can hurt a bank's reputation, the FDIC[4] and OCC[5] say, when they cause:

- Dissatisfied customers/poor service
- Frequent or prolonged service disruptions
- Interactions not consistent with institution policies
- Inappropriate sales recommendations
- Security breaches resulting in the disclosure of customer information
- Violations of consumer law and regulation
- Negative publicity involving the third party

[4] Financial Institution Letter. Guidance for Managing Third-Party Risk. June 6, 2008. https://www.fdic.gov/news/news/financial/2008/fil08044a.html.
[5] OCC Bulletin 2013-29. Risk Management Guidance. Subject: Third-Party Relationships. Appendix A: Risks Associated with Third-Party Relationships https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

While there is no way to guarantee that vendor actions won't damage an institution's reputation, thorough due diligence can help an institution gauge the risk a particular vendor poses. It just takes some digging.

Go beyond the documents the vendor gives you and seek out publicly available information. Determine if the vendor is registered and in good standing with the proper authorities, including the state where it operates. Find out how many and what types of complaints it has filed against it with the CFPB website, and keep in mind that these claims are unsubstantiated. See how the business ranks with the Better Business Bureau and conduct a search of news stories to learn of any past problems.

Other good reference checks include the Federal Trade Commission, state attorneys general offices, state consumer affairs offices and the U.S. Securities and Exchange Commission. The OCC also recommends FIs "Review the third party's Web sites and other marketing materials to ensure that statements and assertions are in-line with the bank's expectations and do not overstate or misrepresent activities and capabilities. Determine whether and how the third party plans to use the bank's name and reputation in marketing efforts."[6]

These materials help an FI identify potential reputation risks and find out what, if any steps, the vendor has taken to remediate past problems. Then an FI can decide if the risk can be mitigated with careful follow up and clarifying protocols to ensure oversight with service level agreements or if that vendor just isn't worth the risk.

7. CYBER RISK

In a world of increasingly sophisticated cyber threats, it's essential that vendors are able to prevent, detect and respond to cyberattacks. Cyber risk is about having the tools, policies and procedures to identify and mitigate internal and external cyber threats and vulnerabilities.

Some people might argue that cyber risk is already covered by operational, transaction, strategic and compliance risk, and it may be covered based on the depth of your internal review. But the growing number of hacks, attacks and other threats make it clear more effort is needed.

It's a message that comes from the top, beginning with President Barack Obama's Executive Order–Promoting Private Sector Cybersecurity Information Sharing in 2015.[7] Later that year the FFIEC released its Cybersecurity Assessment Tool to help banks and credit unions evaluate potential cyber risks and understand inherent risk and cyber maturity. Now the Fed, OCC and FDIC have released an advanced notice of proposed rulemaking for enhanced cyber risk management standards.[8]

Rather than lump cyber risk in with other categories, it's important for banks and credit unions to directly address this critical risk with vendors, using the FFIEC Cybersecurity Assessment Tool as a guide. Chances are most institutions are already engaging in many of the activities recommended by the assessment in different departments and during different risk assessments. The FFIEC's exercise will ensure information from these different silos will come together and ensure vendors are prepared.

While there is no way to guarantee that vendor actions won't damage an institution's reputation, thorough due diligence can help an institution gauge the risk a particular vendor poses.

[6] Ibid.
[7] Executive Order – Promoting Private Sector Cybersecurity Information Sharing. February 13, 2015. https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.
[8] Department of the Treasury. Enhanced Cyber Risk Management Standards. Advanced Notice of Proposed Rulemaking. October 19, 2016. https://www.fdic.gov/news/board/2016/2016-10-19_notice_dis_a_fr.pdf.

Cyber risk is about having the tools, policies and procedures to identify and mitigate internal and external cyber threats and vulnerabilities.

Here are the areas where FIs should be focusing their cyber due diligence:

Identify high-risk activities. A vendor poses a greater cyber risk and requires increased management oversight when it:

- Houses confidential data in a cloud-based system
- Houses or outsources confidential data offshore
- Outsources sensitive activities and/or a number of critical operations
- Uses web-based services to conduct business transactions with customers
- Permits access of confidential data to third-party providers

Controls from the top. Just like an FI, third-party vendors should have controls and protocols to identify cyber risks. The vendor's board or one of its committees should directly review and approve its cyber program. Regular monitoring of the program is a must, identifying threats and vulnerabilities with a periodic risk assessment that estimates the likelihood and impact of cyber risks.

Protect systems. All system activity and events should be logged and monitored, and physical access controls should be monitored to detect suspicious activity. E-mail should be filtered for common cyber threats. Vendors' vendors with access to data should meet defined data protection standards.

Incident response. Third-party vendors must have an incidence response policy that clearly defines a protocol for informing affected stakeholders, regulators and law enforcement officials of a cyber incident where confidential data was likely compromised.

Internal controls. Vendors must implement controls to prevent or mitigate the severity of a cyberattack. Network security controls such as anti-malware, firewalls, intrusion prevention and detection software, and segmented networks should be in place to reduce the likelihood of unauthorized users, devices, connections or software. There should be configuration, network and system change control processes and protocols. Protocols for anti-malware software updates/patch management must be defined and implemented. Periodic vulnerability scans and/or penetration testing should be performed, and the vendor should have cyber insurance coverage.

Human resources. Access controls should be role-based and granted based upon job function. Personnel should be screened before hiring and employees should undergo data safety training.

Data security. There should be protocols and multi-factor authentication during data transmissions and storage and protocols for securely destroying data.

Cloud risk. Vendors that rely on a cloud-based system require additional scrutiny. (See Cloud Risk below.) With this information, FIs can identify cyber risks, deciding if the level of risk presented can be mitigated through protocols and service level agreements or if the risk is just too great.

8. CLOUD RISK

Perhaps there's no buzz word more confusing to bankers and credit union executives than "the cloud." It evokes an ethereal image of data floating safely and serenely overhead, able to materialize on screen with the press of a button.

But the cloud is a place on earth. Actually, it may be many places on earth.

The cloud means someone else's computer. It is typically a bunch of data centers. Using the cloud is buying space on someone else's infrastructure (or data center) to store and/or process data which you can then access via the Internet. Sometimes these

computers are used exclusively by one institution, known as a private cloud. Other times, several clients use the same computers at a data center, known as a shared cloud.

The cloud faces all the same risks as any other third-party IT vendor, which include cyber risk, reputation risk, operational risk, etc. After all, it's a physical location with all the same inside and outside threats any organization faces. But's is growing use and importance is undeniable—and it's starting to attract regulator attention.

For now, the only agency to release something official on cloud risk is the FFIEC and its 2012 statement on Outsourced Cloud Computing in 2012, but this shouldn't create a false sense of security. Regulators are looking closely to see that institutions are aware of cloud risk and are taking steps to mitigate or lower the risk.

The FDIC[9] has highlighted it as an existing and emerging risk, which is a sign that cloud risk is not to be ignored.

Specifically, the FDIC suggests institutions ask:

- What is the type of cloud?
- Who has access to the data?
- Where is the data?
- Is the data backed-up?
- What is the third-party's control structure?
- Can you perform effective/on-going due-diligence?
- How difficult is it to disengage?

Smart FIs are going beyond cyber risk to include cloud risk among their best practices for evaluating third-party vendors. When evaluating cloud-based vendors, an institution should pay mind to existing vendor management and cyber guidance paying special attention to:

Compliance. Ensure the provider is in compliance with privacy laws. Specific responsibilities for data protection must be defined and communicated, often in the service level agreement portion of the contract.

Cyber. There should be clearly defined procedures for responding to and reporting security incidents and notifying customers and regulators of any breaches.

Data security. Access to cloud data should be defined and restricted. Audit logs should be maintained to monitor and detect changes. Data should be encrypted at all times—both at rest and during transmission. When using shared clouds, an institution's data must be segregated from other client data.

Country risk. All cloud data should be housed in the United States. If a vendor won't tell you where data is stored, find another vendor.

Smart FIs are going beyond cyber risk to include cloud risk among their best practices for evaluating third-party vendors.

9. CONCENTRATION RISK

When most bankers and credit union executives think of concentration risk, they think of lending. But concentration has a different meaning when talking about third-party vendors, as the Fed notes in its Guidance on Managing Outsourcing Risk. It specifically mentions concentration risk as something that should be considered when seeking out and managing vendors.

The two main sources of third-party concentration risk are:

Overreliance on a single vendor. This is a classic case of putting all your eggs in one basket. If an institution relies heavily on a single provider for many products and services that institution might be unable to conduct business if something catastrophic happens to that vendor.

[9] FDIC presentation. Information Technology. A Current Perspective on Risk Management. February 25, 2014. https://www.fdic.gov/news/conferences/kc_region/2014-02-25.pdf.

That's not to say an FI can't choose to outsource many major functions to a single vendor, but it just better have an airtight backup plan in place.

Geographic concentration. If both an institution and its third-party vendors and subcontractors are in the same region, it's possible the same event could impact everyone's operations since they all rely on the same power and telecommunications infrastructure.

The good news is that because concentration risk overlaps with other areas including operational, credit and transactional risk, due diligence and supporting documentation shouldn't require much extra effort as long as the risk management team is working cohesively. In fact, the OCC includes concentrations under operational risk.[10]

10. COUNTRY RISK

Speaking of overlapping risks, country risk is another example—touching everything from cloud and reputation risk to transaction and operational risk. Country risk is "an exposure to economic, social, and political conditions in a foreign country that could adversely affect a vendor's ability to meet its service level requirements," according to the FFIEC's Appendix C: Foreign-Based Third-Party Service Providers.[11] In extreme cases, country risk might result in loss data loss.

It's not always obvious when a company poses country risk. For banks and credit unions the threat is most pronounced when it comes to data centers and the cloud, but can affect any overseas operation. Many data centers store their data on the other side of the world in foreign countries to ensure their systems are always running, which is the extreme opposite of geographic concentration.

While this sounds good on the surface, it's a challenge for FIs that must then answer questions about the country where their data is stored. Topics to address include: political and economic stability; infrastructure such as the power grid; and local regulatory and legal oversight such as background checks and authorization.

The FDIC warns, "Managing country risk requires the ability to gather and assess information regarding a foreign government's policies, including those addressing information access, as well as local political, social, economic, and legal conditions."[12] The Fed encourages ongoing monitoring of these risks.[13] Managing these risks "should include the establishment of contingency, service continuity, and exit strategies in the event of unexpected disruptions in service," says the FFIEC. The OCC also addresses the topic.[14]

CONCLUSION

There's no shortage of risks when it comes to outsourcing to third-party service providers, but it still frequently makes sense to outsource critical operations. The key is to carefully assess vendors and, when it comes to the most critical vendors, choose the ones that are most effective in helping FIs mitigate those risks.

The overlapping nature of these risks makes it essential for FIs to have a comprehensive, top-down approach to enterprise risk management and vendor management. By taking a broad view of risk management, FIs can leverage the risk assessment and mitigation work performed by various departments throughout the institution, streamlining the process to make it more effective and more efficient.

In extreme cases, country risk might result in loss data loss.

[10] OCC Bulletin 2013-29. Risk Management Guidance. Subject: Third-Party Relationships. Appendix A: Risks Associated with Third-Party Relationships https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.
[11] FFIEC IT Examination HandBook InfoBase. Appendix C: Foreign-Based Third-Party Service Providers. http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/appendix-c-foreign-based-third-party-service-providers.aspx .
[12] FDIC Compliance Examination Manual. Unfair and Deceptive Practices–Third Party Risk. https://www.fdic.gov/regulations/compliance/manual/7/VII-4.1.pdf.
[13] SR-02-5. Federal Reserve Interagency Guidance on Country Risk Management. March 8, 2002. https://www.federalreserve.gov/boarddocs/srletters/2002/sr0205.htm.
[14] OCC Bulletin 2002-16. Risk Management Guidance. Bank Use of Foreign-Based Third-Party Service Providers. May 15, 2002. https://www.occ.gov/news-issuances/bulletins/2002/bulletin-2002-16.html.

The overlapping nature of these risks makes it essential for FIs to have a comprehensive, top-down approach to enterprise risk management and vendor management.

Ncontracts provides a variety of tools to help FIs face this challenge in a methodical, organized way. Nvendor is a secure, feature-rich, online vendor and contract management solution that enables financial institutions to achieve and maintain regulatory compliance in their third-party vendor relationships. Features include assistance with vendor policies and procedures, vendor classification, vendor due diligence, risk assessment and vendor monitoring.

Ncyber guides institutions through the FFIEC's Cybersecurity Assessment Tool, helping analyze inherent risk and cybersecurity maturity levels.

Ncontinuity is a flexible, scalable, and secure online business continuity planning solution. Its interactive dashboard, tools and support strengthen business continuity needs throughout your organization and in your third-party vendor relationships.

Nrisk is a secure, online risk management solution that enables continuous measurement of financial and non-financial impacts by location, department, business process, application or line of business. It simplifies the risk assessment process using natural language navigators and wizards that guide users step-by-step through the process of evaluating risk and related financial exposures—leveraging the hard work your institution has already done.

Regardless of approach, FIs need to be assessing each of these vendor risks to determine the level risk and amount oversight and monitoring a specific vendor requires. As regulators continue to expand and investigate categories of risk, it's no longer efficient or effective to conduct these risk assessments in silos. Careful risk assessment and monitoring from pre-contract due diligence and throughout the length of the relationship is critical for proper vendor management.

Ncontracts® is a leading provider of risk management software and services to financial institutions. While we started with our industry-leading vendor management platform, our portfolio offerings have evolved to feature enterprise risk management, business continuity risk management, compliance management, findings management, and cybersecurity management. More than 650 financial organizations use Ncontracts to manage risk more efficiently and effectively using our integrated suite of software and services.

(888) 370-5552
info@ncontracts.com
www.ncontracts.com