From: Sheila Stratton <sstratton@lead.bank>
Sent: Tuesday, September 22, 2020 7:02 PM
To: Comments
Subject: [EXTERNAL MESSAGE] July 24, 2020 - Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services; Comment Request (RIN 3064-ZA18)
Attachments: FDIC fil20071a Document - Initial responses.docx

Please find the attached comments regarding RIN 3064-ZA18.
Thank you!

Sheila Stratton, AAP
Senior Vice President
Director of Digital Strategy

9019 S 7 Highway
Lee's Summit, MO 64064
P.O. Box 6874
Phone: 816.874.4921
Fax: 816.220.8602
sstratton@lead.bank
www.lead.bank

[redacted]

The Federal Deposit Insurance Corporation (FDIC) today announced that it is seeking the public's input on the potential for a public/private standard-setting partnership and voluntary certification program to promote the efficient and effective adoption of innovative technologies at FDIC-supervised financial institutions. Given rapid technological developments and evolving consumer behavior, this public/private partnership model program has the potential to help promote innovation across the banking sector and streamline a costly and often duplicative system for both banks and technology firms.

Released as part of the FDiTech initiative, the Request for Information asks whether the proposed program might reduce the regulatory and operational uncertainty that may prevent financial institutions from deploying new technology or entering into partnerships with technology firms, including "fintechs." For financial institutions that choose to use the system, a voluntary certification program could help standardize due diligence practices and reduce associated costs.

"Fostering innovation in the financial sector is a top priority for the FDIC," said Chairman Jelena McWilliams. "We have to remove unnecessary regulatory impediments that banks must overcome when developing or deploying new technologies."

The FDIC encourages comments from all interested parties by 60 days from publication in the Federal Register.

FDIC: PR-83-2020

Questions from fil20071a attachment

General Questions

Question 1: Are there currently operational, economic, marketplace, technological, regulatory, supervisory, or other factors that inhibit the adoption of technological innovations, or on-boarding of third parties that provide technology and other services, by insured depository institutions (IDIs), particularly by community banks?

Regulatory controls do inhibit certain abilities to move timely for third-party partnerships depending on the risk appetite venture. If the certification does not allow for the replacement of a full due diligence review, there will be limited benefits in having a certification. Should it be performed similar to an ISO 27001 or PCI ROC certification then it would provide a benefit.

Question 2: What are the advantages and disadvantages of establishing standard-setting and voluntary certification processes for either models or third-party providers?

This will depend upon the scope and level of scrutiny applied when verifying controls and regulations to issue a certification. The usefulness of the certification is dependent upon the depth, breadth, and evidence validation of the company issued the certificate.

Some Advantages/Disadvantages may be –
Advantages: Ability to move faster and provide some addition credibility to the company holding the certificate if the certification has set regulations in place to obtain and is not just a purchase with no validity.
Disadvantages: Honesty or completeness of controls and regulatory requirements may not fully identify all the risks.

Question 3: What are the advantages and disadvantages to providers of models of participating in the standard-setting and voluntary certification process? What are the advantages and disadvantages to providers of technology and other services that support the IDI's financial and banking activities of participating in the standard-setting and voluntary certification process?

This will depend upon the scope and level of scrutiny applied when verifying controls and regulations to issue a certification. The usefulness of the certification is dependent upon the depth, breadth, and evidence validation of the company issued the certificate. It is also important that validation is performed by an independent third party, versus self-certification.

Question 4: What are the advantages and disadvantages to an IDI, particularly a community bank, of participating in the standard-setting and voluntary certification process?

This will depend upon the scope and level of scrutiny applied when verifying controls and regulations to issue a certification. The usefulness of the certification is dependent upon the depth, breadth, and evidence validation of the company issued the certificate.

Question 5: Are there specific challenges related to an IDI's relationships with third-party providers of models or providers of technology and other services that could be addressed through standard-setting and voluntary certification processes for such third parties?
(1) Are there specific challenges related to due diligence and ongoing monitoring of such third-party providers?

The main challenge is getting a complete, timely response from a third-party for key due diligence evidence. For example, not all third parties have a SOC or independent audit performed, and others are privately held and will not share financial reports. A certificate may provide some additional credibility depending on the regulations set to obtain the certification. This will depend upon the scope and level of scrutiny applied when verifying controls and regulations to issue a certification. The usefulness of the certification is dependent upon the depth, breadth, and evidence validation of the company issued the certificate.

(2) Are there specific challenges related to the review and validation of models provided by such third parties?

There could be several depending on the business relationship. The same challenge as listed in 1 above obtaining due diligence key evidence, validating current status of the business, etc. is applicable.

(3) Are there specific challenges related to information sharing or data protection?
Typically, there is an NDA agreement in place for information sharing.

Questions 6: Would a voluntary certification process for certain model technologies or third-party providers of technology and other services meaningfully reduce the cost of due diligence and on-boarding for:
(1) the certified third-party provider?

Yes, provided that the FDIC and regulatory requirements have controls in place to accept the due diligence requirements are in place with certification. This would greatly help with time and effort of validation. This depends upon the scope and level of scrutiny applied when verifying controls and regulations to issue a certification. The usefulness of the certification is dependent upon the depth, breadth, and evidence validation of the company issued the certificate and certifying organization.

(2) the certified technology? Yes, for example third parties with a complete overarching ISO 27001 Certification demonstrate their security and technology controls are adequate.

(3) potential IDI technology users, particularly community banks?
Insured Depository Institution (US department of the Treasury) IDI. This would be a benefit for users to know that the bank is taking steps to partner with verified reputable third parties to do business. Yet this will depend upon the scope and level of scrutiny applied when verifying controls and regulations to issue a certification. The usefulness of the certification is dependent upon the depth, breadth, and evidence validation of the company issued the certificate.

Question 7: What are the challenges, costs, and benefits of a voluntary certification program or other standardized approach to due diligence for third-party providers of technology and other services? How should the costs of operating the SSO and any associated COs be allocated (e.g., member fees for SSO participation, certification fees)?

Annual time and cost to complete evidential documentation to certify and potentially a third party cost to perform. The benefit would be processing time of new partnerships and effort at the time of on-boarding should the certification be accepted in place of other due diligence reviews. Again, this will depend upon the scope and level of scrutiny applied when verifying controls and regulations to issue a certification. The usefulness of the certification is dependent upon the depth, breadth, and evidence validation of the company issued the certificate and the certifying organization.

Question 8: Would a voluntary certification process undermine innovation by effectively limiting an IDI's discretion regarding models or third-party providers of technology and other services, even if the use of certified third parties or models was not required? Would IDIs feel constrained to enter into relationships for the provision of models or services with only those third parties that are certified, even if the IDIs retained the flexibility to use third parties or models that were not certified?

It would depend upon the scope and level of scrutiny applied when verifying controls and regulations to issue a certification. The usefulness of the certification is dependent upon the depth, breadth, and evidence validation of the company issued the certificate and the certifying organization. If the certification is done well and could be used in place of some due diligence, then it might restrict those that choose not to obtain it, implying that they would not pass or another company could more quickly get through the overall process.

Question 9: What supervisory changes in the process of examining IDIs for safety and soundness or consumer protection would be necessary to encourage or facilitate the development of a certification program for models or third-party providers and an IDI's use of such a program? Are there alternative approaches that would encourage or facilitate IDIs to use such programs?

Question 10: What other supervisory, regulatory, or outreach efforts could the FDIC undertake to support the financial services industry's development and usage of a standardized approach to the assessment of models or the due diligence of third-party providers of technology and other services?

Set up a certification that would allow for companies to undergo an annual review like ISO 27001 so that it could be used in place of a full due diligence review individually for each company it does business with.

Scope

Question 11: For which types of models, if any, should standards be established and a voluntary certification process be developed? For example, is the greatest interest or need with respect to:
(1) traditional quantitative models? Yes

(2) anti-money laundering (AML) transaction monitoring models? Yes

(3) customer service models?

(4) business development models?

(5) underwriting models? Yes

(6) fraud models? Yes

(7) other models?

Question 12: Which technical and operational aspects of a model would be most appropriate for evaluation in a voluntary certification program?

The same as those for SOC 2 Type II, ISO 27001, NIST 171, or PCI ROC.

Question 13: What are the potential challenges or benefits to a voluntary certification program with respect to models that rely on artificial intelligence, machine learning, or big data processing?

The same as those for SOC 2 Type II, ISO 27001, NIST 171, or PCI ROC.

Question 14: How can the FDIC identify those types of technology or other services, or those aspects of the third-party provider's condition, that are best suited for a voluntary certification program or other standardized approach to due diligence? For example, should such a certification program include an assessment of financial condition, cyber security, operational resilience, or some other aspect of a third-party provider?

Yes, It should consider all the current expectations of FFIEC Due Diligence and those controls expected by a SOC 2 Type II, ISO 27001, NIST 171, or PCI ROC.

SSO

Question 15: If the FDIC partnered with an SSO to set standards for due diligence and assessments of models or third-party providers of technology and other services, what considerations should be made in choosing the SSO? What benefits or challenges would the introduction of an SSO into the standard-setting process provide to IDIs, third-party providers, or consumers?
It should have the same qualities as expected of independent auditors. Examples include those performing SOC reviews, ISO reviews, PCI reviews, or Fraud Examiners.

Question 16: To what extent would a standards-based approach for models or third-party providers of technology and other services be effective in an environment with rapidly developing technology systems, products, and platforms, especially given the potential need to reassess and reevaluate such systems, products, and platforms as technologies or circumstances change?

If done adequately, the certification should maintain and update requirements like PCI Certification.

Question 17: What current or draft industry standards or frameworks could serve as a basis for a standard-setting and voluntary certification program? What are the advantages and disadvantages of such standards or frameworks? Do standards and voluntary certifications already exist for use as described herein?

The same as those for SOC 2 Type II, ISO 27001, NIST 171, or PCI ROC.

Question 18: Given that adherence to SSO standards would be voluntary for third parties and for IDIs, what is the likelihood that third-party providers of models or services would acknowledge, support, and cooperate with an SSO in developing the standards necessary for the program? What challenges would hinder participation in that process? What method or approaches could be used to address those challenges?

Question 19: What is the best way to structure an SSO (e.g., board, management, membership)? Alternatively, are there currently established SSOs with the expertise to set standards for models and third parties as described herein?

Question 20: To what extent should the FDIC and other federal/state regulators play a role, if any, in an SSO? Should the FDIC and other federal/state regulators provide recommendations to an SSO? Should the FDIC and other federal/state regulators provide oversight of an SSO, or should another entity provide such oversight?

The FDIC should play a role if it where to be used in place of due diligence items and robust to withstand scrutiny. Another government entity reference would be the NIST 800-53/171.

Certification Organizations (COs)

Question 21: What benefits and risks would COs provide to IDIs, third parties, and consumers?

Question 22: To what extent would COs be effective in assessing compliance with applicable standards in an environment with rapidly developing technology systems, products, and platforms, especially given the potential need to reassess and reevaluate such systems, products, and platforms as technologies or circumstances change?

If done adequately, the certification should maintain and update requirements like PCI Certification.

Question 23: For model validation and testing, would COs evaluate a model based solely on reports, testing results, and other data provided by the third-party provider of the model? Or would the COs need to test the model and generate their own test results? What steps would the COs need to take to

protect the intellectual property or other sensitive business data of the third party that has submitted its model to the validation process?

Independent verification like SOC, PCI, or ISO.

Question 24: If COs receives derogatory information indicating that a certified third party or certified model or technology no longer meets applicable standards, should the COs develop a process for withdrawing a certification or reassessing the certification?
(1) If so, what appeal rights should be available to the affected third party?
There could be considerations depending on offence and timing. If this is an annual certification then certain stipulations could be determined of how and when it should be addressed.

(2) What notification requirements should COs have for financial institutions that have relied on a certification that was subsequently withdrawn?
Reference data base that allows for current certification validation, similar to those of PCI or for an individuals professional certification like CISA.

(3) Should the FDIC or federal/state regulators enter information sharing agreements with COs to ensure that any derogatory information related to a certified third party or certified model or technology is appropriately shared with the COs?

Question 25: Are there legal impediments, including issues related to liability or indemnification, to the implementation of a voluntary certification program that the FDIC, other federal/state regulators, third-party providers, and IDIs should consider?

Question 26: To what extent should the FDIC and other federal/state regulators play a role, if any, in the identification and oversight of COs, including assessments of ongoing operations? Should the FDIC and other federal/state regulators provide oversight of COs, or should another entity, such as an SSO, provide such oversight?