FEDERAL DEPOSIT INSURANCE CORPORATION

RIN 3064-ZA18

Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services

AGENCY: Federal Deposit Insurance Corporation (FDIC).

ACTION: Notice and request for information.

SUMMARY: The FDIC is issuing this request for information (RFI) as part of its FDiTech initiative to promote the efficient and effective adoption of technology at FDIC-supervised banks and savings associations ("financial institutions"), particularly at community banks, and to facilitate the supervision of technology usage at these institutions without increasing costs or regulatory burden. The FDIC is committed to increasing transparency, improving supervisory and regulatory efficiency, supporting innovation in banking, and providing opportunities for public feedback. This RFI seeks input on whether a standard-setting and voluntary-certification program could be established to support financial institutions' efforts to implement models and manage model risk by certifying or assessing certain aspects of the models themselves, and to conduct due diligence of third-party providers of technology and other services by certifying or assessing certain aspects of the third-party providers' operations or condition. The FDIC is especially interested in information on models and technology services developed and provided by financial technology companies, sometimes referred to as "fintechs."

DATES: Comments must be received by [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by RIN 3064-ZA18, by any of the following methods:

- Agency Website*: https://www.fdic.gov/regulations/laws/federal/*. Follow the instructions for submitting comments on the agency website.
- Email: *Comments@fdic.gov*. Include RIN 3064-ZA18 in the subject line of the message.
- Mail: Robert E. Feldman, Executive Secretary, Attention: Comments, Federal Deposit Insurance Corporation, 550 17th Street NW, Washington, DC 20429.
- Hand Delivery/Courier: Comments may be hand-delivered to the guard station at the rear of the 550 17th Street, N.W., building (located on F Street) on business days between 7:00 a.m. and 5:00 p.m.

All comments received must include the agency name and RIN 3064-ZA18.

Public Inspection: All comments received will be posted without change to *https://www.fdic.gov/regulations/laws/federal/*—including any personal information provided—for public inspection. Paper copies of public comments may be ordered from the FDIC Public Information Center, 3501 North Fairfax Drive, Room E-1002, Arlington, VA 22226 by telephone at (877) 275-3342 or (703) 562-2200.

FOR FURTHER INFORMATION CONTACT: Alexander LePore, Jr., Senior Policy Analyst, telephone (202) 898-7203, email alepore@fdic.gov.

SUPPLEMENTARY INFORMATION:

The FDIC is an independent federal agency with a mission of maintaining stability and public confidence in the nation's financial system, in part by examining and supervising certain financial institutions, including for safety and soundness and consumer protection.[1] The FDIC is

[1] The FDIC also promotes stability and public confidence in the nation's financial system by insuring deposits and resolving failed insured depository institutions, leading sound policy development, evaluating resolution plans of the largest of institutions, and monitoring and mitigating systemic risks in the banking sector and financial system as a whole.

the primary federal banking supervisor for more than 3,000 state-chartered banks and savings associations that are not members of the Federal Reserve System, and it conducts regular examinations of these supervised institutions.[2] Examinations include an assessment of how a financial institution manages the risks presented by its relationships with third parties.

The FDIC reviews a financial institution's management of significant third-party relationships in the context of the normal supervisory process. The FDIC examines the quality and effectiveness of an institution's risk management program as it pertains to the safety and soundness and consumer protection aspects of third-party arrangements. The FDIC also examines a financial institution to ensure that the products, services, and activities supported by a third party are safe and sound and comply with applicable laws and regulations, including those concerning consumer protection and civil rights. Reviews of third-party arrangements are also a critical area included in examinations of the trust and information technology functions.

Financial institutions often establish relationships with third parties to provide certain functions that financial institutions do not perform or to meet short-term needs that they are unable to fulfill. Therefore, financial institutions rely on third-party relationships for many different aspects of their operations, including credit management, operational risk management, valuation, and stress testing. Management is responsible for identifying and controlling risks from activities conducted by or through its financial institution, whether these risks arise from internal business activities or through arrangements with a third party.[3] These risks include those

---

[2] The FDIC also has a back-up supervision and examination role with respect to approximately 2,000 insured depository institutions (pursuant to sections 8 and 10 of the Federal Deposit Insurance Act, 12 U.S.C. 1818, 1820) for which the Office of the Comptroller of the Currency and the Board of Governors of the Federal Reserve System are the primary federal regulators.

[3] Section 39 of the Federal Deposit Insurance Act requires the Federal Deposit Insurance Corporation to establish

that arise from reliance on models, technologies, and other products or services provided by third parties. Model guidelines[4] describe risk management principles relating to financial institutions employing models, which are described as quantitative methods, systems, or approaches that apply statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates.[5] In general, model risk management should be commensurate with the financial institution's overall use of models, the complexity and materiality of its models, and the size and complexity of the financial institution's operations. Financial institutions also should be mindful of consumer protection risks when using third-party models or technologies, to ensure they are developed and operated in compliance with applicable consumer protection laws and regulations, which may include, for example, fair lending laws, privacy laws, and prohibitions against unfair, deceptive, or abusive acts or practices.[6]

As the financial services industry evolves, more financial institutions are using third-party models and technologies for functions that either are new or had been performed in-house in the past. The FDIC recognizes that the use of such models and technologies can assist the financial institution in providing greater benefits to consumers and increasing financial inclusion.

safety and soundness standards. 12 U.S.C. 1831p-1. These standards are set forth in part 364 of the FDIC Rules and Regulations. 12 CFR part 364.

[4] *See, e.g.*, Supervisory Guidance on Model Risk Management, FIL-22-2017 (June 7, 2017), Guidance for Managing Third-Party Risk, FIL-44-2008 (June 6, 2008), Interagency Guidelines Establishing Standards for Safety and Soundness, 12 CFR part 364, Appendix A, and Interagency Guidelines Establishing Information Security Standards, 12 CFR part 364, Appendix B.

[5] For example, financial institutions entering into a relationship with a third party to employ these models would also need to comply with section 5 of the Federal Trade Commission Act (15 U.S.C. 45) and ensure that lending practices that are not discriminatory in violation of the Equal Credit Opportunity Act (15 U.S.C. 1691-1691f).

[6] *See, e.g.*, Equal Credit Opportunity Act, 15 U.S.C. 1691-1691f; Fair Credit Reporting Act, 15 U.S.C. 1681-1681x; Interagency Statement on the Use of Alternative Data in Credit Underwriting, FIL-82-2019 (Dec. 13, 2019); Interagency Fair Lending Examination Procedures (Aug. 2009); Policy Statement on Discrimination in Lending, FR Doc. No. 94-9214 (Apr. 15, 1994); Dodd-Frank Act, Title X, Subtitle C, Sec. 1036; PL 111-203 (July 21, 2010)

The use of third-party models and technologies may also give the financial institution access to greater expertise or efficiency in providing a particular product or service at lower cost.

Many financial institutions, particularly community banks, have indicated to the FDIC that sometimes the costs and other resources associated with deploying models or technologies from third parties can be prohibitive. Vendors offer increasingly complex models with a range of features, and as a result, institutions may find it challenging to validate and assess such models. For example, an institution might conclude that it must hire new internal staff, retain consultants, or impose contractual obligations on the third party in order to conduct the model validation. In addition, for third-party outsourcing arrangements that support models, institutions conduct risk reviews on third-party providers. These risk reviews involve financial, operations, contract, and insurance assessments, along with assessment of other aspects of the outsourcing arrangements. Representatives of financial institutions have expressed concerns to the FDIC that the costs associated with the financial institutions' review of both models and third-party providers of models can create barriers to entry, particularly in the community banking market, by limiting the institutions' ability to effectively and timely on-board third parties and deploy new and innovative models.

The FDIC recognizes the important role that technological innovations can play in transforming the business of banking and enabling regulators to supervise more efficiently, thereby reducing regulatory burden while maintaining consumer protection and safety and soundness standards. Therefore, the FDIC is exploring opportunities to assist financial institutions in effectively complying with laws and regulations regarding management of third-party risks concerning the use of models, such as credit underwriting models. Among other things, the FDIC is considering the value of standards for assessing models. The development of

relevant standards, along with the development and application of a voluntary certification process to ensure that models conform to those standards, could potentially allow for more financial institutions—particularly community banks—to engage with third parties, including fintechs; permit FDIC supervision resources to be used more efficiently and effectively; and reduce costs of doing business for financial institutions and providers of models.

The FDIC also is considering whether a voluntary certification or assessment program could support financial institutions' due diligence of third-party providers of a range of technology and other services by certifying or assessing certain aspects of the third-party providers' operations or condition. The FDIC is interested in whether there are unique elements and challenges associated with financial institutions' due diligence of third-party providers of technology and other services that would benefit from a voluntary certification or assessment program applicable to such providers. The FDIC is primarily interested in due diligence elements associated with third-party providers of technology and other services that support a financial institution's financial and banking activities, such as deposit, lending, and payment functions. The FDIC also is interested in comments regarding due diligence for other types of third-party providers, such as those providers that support the financial institution's corporate activities, including payroll and human resources. The FDIC also requests comments on what alternative steps the FDIC could pursue, other than a voluntary certification or assessment program, to support financial institutions' efforts to assess risk efficiently and effectively when contemplating new or monitoring existing relationships with third-party providers.

As part of this Request for Information, the FDIC is not considering substantive revisions to its existing supervisory guidance with respect to model risk management or third-party provider risk management. However, the FDIC seeks comment on the possible changes to its

supervisory guidance that would be appropriate to facilitate financial institutions' use of a voluntary certification or assessment program for conducting due diligence and ongoing monitoring of third-party providers of technology and other services, or for reviewing models or other technologies.

Standard-Setting and Certification Programs

Government and the private sector have worked together for more than a century to develop standards for use in private industry. The Federal government has encouraged using standards developed by voluntary, consensus standard-setting bodies.[7] The typical standard-setting process involves a standard-setting organization (SSO) working with stakeholders, including government agencies, to develop a standard for a particular industry or sector of the economy. The standard is established on a voluntary, consensus-driven basis and provides guidelines for engaging in a particular process or for offering a particular service or product. Categories of common standards include product-based standards, performance-based standards, management system standards, personnel certification standards, and construction standards.

Once a standard is developed, application of a conformity assessment process provides assurance that processes, products, or services meet the requirements identified in the standard. This step is vital because creating a standard alone cannot promote (for voluntary standards) or guarantee (for mandatory standards) adherence to the standard. The conformity assessment can verify that processes, products, or services meet the specified level of quality, safety, or performance. Depending on the risks of nonconformance and the confidence level necessary, there are several ways to assess whether processes, products, or services meet a standard, from

[7] *See, e.g.*, National Technology Transfer and Advancement Act of 1995, Pub. L. 104-113, section 12(d) (Mar. 7, 1996); OMB Circular No. A-119 Revised, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities" (Feb. 10, 1998).

an entity's self-declaration to third-party certification, validation, verification or auditing. Accreditation by an independent body of organizations that perform conformity assessment activities provides formal recognition that the organization is competent, capable and impartial. In many ways, the assessment process is as important as setting the standard itself.

The standard-setting system in the United States is based on globally accepted principles for standards development including transparency, openness, impartiality, effectiveness, and consensus. The standard-setting process assures that:

- information regarding standardization activities is accessible to all interested parties;
- participation is open to all stakeholders;
- all interests are balanced;
- standards respond to regulatory and market needs; and
- decisions are reached through consensus among those affected.

SSOs also strive to make standards as flexible as possible, allowing for the use of different methodologies to meet the needs of different stakeholders. Good faith efforts are made to eliminate, or at least minimize, conflict with other existing standards or rules.

SSOs often partner with government entities, academia, and industry to identify proposed solutions and work together toward a common goal. SSOs also involve consumers in the process so their needs are considered and addressed. This process results in standards that often balance regulatory and market needs, facilitate innovation, promote consumer protection, and strengthen competition.

In applying this standard-setting framework to models and third-party providers of technology and other services, financial institutions would have the ability to rely on

certifications related to the third-party provider or certified models or other technology products and services. Financial institutions would not be required to use only certified third parties, models, or technologies. Instead, financial institutions would retain the flexibility to require certified third parties to meet different requirements that the financial institutions viewed as appropriate. For example, financial institutions would retain the right to request that certified third parties submit additional information for purposes of on-boarding at that financial institution consistent with the financial institution's unique use of the model or service, and consistent with applicable law and regulation.

Request for Comment

Given rapid technological developments and evolving consumer behaviors in banking, the FDIC seeks to learn more regarding the benefits and challenges of collaborating with an SSO and other stakeholders to create a standard-setting and a voluntary certification process. This certification process would potentially assist financial institutions in completing assessments or due diligence of: (1) certain models, such as credit underwriting models, by certifying or assessing certain aspects of the models; and (2) third-party providers of technology and other services, by certifying or assessing certain aspects of the providers' operations or condition. The FDIC is interested in comments regarding initial due diligence and ongoing monitoring elements associated with third-party providers of technology and other services that support the financial institution's financial and banking activities, such as deposit, lending, and payment functions. The FDIC also is interested in comments regarding due diligence for other types of providers, such as third-party providers that support the financial institution's corporate activities, such as payroll and human resources.

Consistent with the collaborative approach to standard setting that government and the private sector have long taken, the FDIC envisions a collaboration among an SSO, the FDIC, and other stakeholders to set standards under an SSO, along with a voluntary conformity assessment process through accredited, independent certification organizations. The certification organizations would conduct conformity assessments of third-party providers that voluntarily submit required information regarding their products, services, models, or organization, with the task of determining conformance with the established standards. The FDIC is issuing this RFI to seek public input regarding all aspects of establishing an SSO, qualifying certification organizations, and implementing a voluntary conformity assessment process.

The FDIC also is considering, and seeking comment on, whether and how the FDIC's supervisory and examination efforts would need to be modified to facilitate a financial institution's use of a certified model or a certified third party of outsourced technology services.

The FDIC encourages comments from all interested parties, including but not limited to insured banks and savings associations, technology companies and fintechs, other third-party vendors and service providers, other financial institutions or companies, depositors and consumers, consumer groups, researchers, innovators, technologists, trade associations, and other members of the financial services industry. The FDIC also encourages comments from standard-setters and participants in other industries using standardization and certification processes, whether voluntary or mandatory.

The FDIC invites public comment on all aspects of the RFI, including the following questions.

General

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?

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

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?

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?

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?

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

(3) Are there specific challenges related to information sharing or data protection?

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?

(2) the certified technology?

(3) potential IDI technology users, particularly community banks?

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)?

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?

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?

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?

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

(3) customer service models?

(4) business development models?

(5) underwriting models?

(6) fraud models?

(7) other models?

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

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?

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?

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?

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?

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?

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?

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?

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?

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?

(2) What notification requirements should COs have for financial institutions that have relied on a certification that was subsequently withdrawn?

(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?

Federal Deposit Insurance Corporation
Dated at Washington, D.C., on [date], 2020.
James P. Sheesley,
Acting Assistant Executive Secretary

BILLING CODE 6714-01-P