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

RIN 3064-ZA18

venminder.com | info@venminder.com
400 Ring Road, Suite 131, Elizabethtown, KY
(270) 506-5140

As of September 21, 2020

Background on Venminder

Venminder is a provider of third-party risk management solutions

- Venminder offers a SaaS platform that guides and streamlines third-party risk management. Venminder's platform helps users collaborate on all things vendor-related and guides through critical processes such as oversight management, contract management, risk assessments, due diligence requirements, questionnaires, SLA management, vendor onboarding and more. Robust and configurable reporting can be generated from the tool to give clear visibility into the management and ongoing monitoring of third parties.
- Venminder also offers completed vendor risk assessments which can be found in the Venminder Exchange and include thorough assessments of a vendor's information security, SOC reports, contracts, financials, business continuity/disaster recovery and more.
- Venminder today has over 800 clients of all sizes with the majority being in the highly regulated financial services industry.

Response Led By:

James Hyde, CEO, Venminder. James.hyde@venminder.com
Dana Bowers, Founder and Chief Solution Architect, Venminder. Dana.bowers@venminder.com

Comments to FDIC RIN 3064-ZA18

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

   Often, new FinTech organizations which may offer a community bank technological innovations, are not as mature from a control perspective (for example, relevant audits may not in place or policies and procedures are inadequate). Therefore, they would not meet a bank's regulatory requirements. Many third parties also require a sizeable budget to meet the needs of bank clients (the time spent answering questionnaires, responding to document requests, implementing new processes) and at times, a third party may not be in a position to make those changes.

   For banks, they must each independently spend the money to vet all vendors. Each bank owns the risk; therefore, based on each bank's risk appetite, each bank often has different flavors of questionnaires that they send to vendors. Managing third parties can be costly since a bank may not be able to afford the in-house resources (hiring the relevant and qualified subject-matter expertise for vendor assessments). Reading and analyzing a third-party's 10-K may require a qualified CPA, a third-party SOC Report may require a qualified CISSP. It has also become more difficult to find specific talent in the current COVID-19 environment, just as the workload has increased. Banks have had to bring on new third parties quickly to survive in a remote pandemic world, often with a little less oversight and visibility. Banks have been able to leverage outsourced partners, like Venminder, which offers a technology platform to manage vendors and also a shared library approach to completed assessments (completed by relevant subject-matter expertise), but there is still a cost to the bank. It would be favorable if there was a way to shift some of

that burden of cost to a third party while also empowering the third party with what they need to market to community banks.

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

Today, if you ask five banks how they assess risk, you may get seven answers. While the regulations tell the bank what they're supposed to do, they don't detail the "how". What has therefore evolved is customized methodologies for every financial institution where no two are the same. A third party then gets individualized assessment requests from every client in that client's flavor. The same kinds of questions, trying to get at the same answer, but asked many different ways (and multiplied by each bank prospect/client) – this is incredibly burdensome to third parties. Therefore, if there was a standard set, everyone would then be answering and asking the same questions and receiving the same answers. The overall workload would be reduced and expectations would be clearer for both the third party and the bank.

Advantages:

- Diversifies the cost to support the appropriate oversight for both community banks and third parties to consistently deploy technology in a safe and certified way.
- Banks would have the ability to make sound quick judgements that they know meet regulatory requirements and ultimately feel confident that the appropriate oversight is in place to streamline the purchase decisions.
- Banks could deploy technology faster, possibly allowing them to select innovative technological advancements.
- Third parties can leverage a certification that adheres to the SSO best practices and
    - Use it as a sales enablement tool when marketing to community banks
    - Ensure that they meet industry best practices and have verified the appropriate boxes are checked (infosec, compliance)

Disadvantages:

- We believe that an FDIC model of developing a standard that follows a "pass" or "fail" grade, or "is certified" and "is not certified" will not work. It instead should follow the same model similar to how the FDIC exams are conducted, on a gradient scale. This would be with a score, possibly a 1-4 score, while allowing for indication of level of performance but also acknowledgement of areas available for improvement. For example, if a vendor had an overall score of a "2" and their area of weakness was in financial performance, but information security practices are strong, it would allow a community bank visibility into the areas of strength and into the areas of weakness and evaluate if financial strength is critical to the product/service they are outsourcing so they can make the best decision on whether that area of weakness (or risk) is acceptable to their risk tolerance.

On the topic of voluntary, Venminder has already implemented an exchange network model between third parties and other organizations, namely the Venminder Exchange. Venminder has 800+ clients and thousands of vendors that are already participating in a voluntary assessment process with the process of sharing a library of assessments in place to help reduce the costs for both sides. Our assessments are all completed by qualified and certified experts, and built to ask and assess the areas that need to matter (current regulations and best practices):

- For banks that use Venminder, it reduces their workload and streamlines their processes. They can spend less time chasing third parties and can avoid having to hire costly internal resources to dedicate to reviewing third-party risk.
- For third parties, Venminder provides validation when they have a business that is secure and compliant, they gain visibility into the process (and, therefore, learn where they need to improve), and it can assist them when marketing to clients that require them to meet regulatory expectations.

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?**

   Demonstrated by the Venminder Exchange, it allows a model provider to leverage work already completed for one, to be distributed to many.

   For the provider of the model, such as Venminder, it requires having adequate staff and subject matter expertise on a wide variety of topics to ensure the certification assessments are done in a qualified manner and meet regulatory expectations. Whether it's a tabletop exercise via documentation or onsite assessment, it always requires the right subject matter expertise, much like a SOC audit which requires a qualified CPA firm to perform the audit.

   Some disadvantages may include the cost and time investment. It's the cost and the waiting period for assessment results that could result in it being more difficult for a third party to do business with a financial institution if the results in any assessment are less than satisfactory.

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

   From an advantage standpoint, it provides confidence of an independent third-party assessor evaluation. It also allows the bank to share the cost across a broader base of users and shift some, if not all, of the cost of assessments to the third parties.

   A disadvantage to a certification program, is that if a bank required a unique process, it cannot be customized since it is a standard setting.

5. **Are there specific challenges related to a bank's relationship with a model provider or the third parties that could be addressed through standard-setting and voluntary certification processes for such third parties?**

Yes, it would set expectations for both sides of the relationship and educate and provide understanding to the third party community on what is required to do business with a bank, which in turn validates the request for information and documentation to demonstrate compliance.

(a) Are there specific challenges related to due diligence and ongoing monitoring of such third-party providers? Yes, many vendors either don't have, won't release, won't respond, won't answer a questionnaire, or won't provide adequate documentation, to demonstrate adequate controls on topics such as financial health or information security. A standardization would make it clear, for third parties of all sizes, on what is required to do business with a bank.

(b) Are there specific challenges related to the review and validation of models provided by such third parties? Adequate subject matter experts would be required to review the many different areas that need to be assessed. For example, a CISSP to assess the third party's SOC reports for weaknesses, a CPA to review the vendor's long-term financial viability.

(c) Are there specific challenges related to information sharing or data protection? A provider of a model would have to demonstrate that it has its own adequate information security practices to protect the data provided by both third parties and/or community banks and has the experience to build and support the relationship between both parties.

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?**

   Yes, for all three use cases. The certified third-party may find a drastically reduced influx of questionnaires and other requests from banks. A bank may then be able to make decisions more efficiently and faster.

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)?**

   A certification fee should be owned by the third party. A financial institution may pay an association or membership fee for access.

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?**

   Yes - it would limit a particular third party's ability to ever meet a banks requirements if the certification was built as a "pass" or "fail" certification. But, if it was set as a gradient scale with strengths and weaknesses, then no.

   A bank must ultimately own their risk appetite. There is always going to be a cost of selling to the financial institution market that third parties should expect and be willing to meet the additional controls that need to be satisfied when providing services/product, especially if the third party would be a high risk or critical third party to that bank.

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?**

   Reassurance that banks can look for that "stamp" of approval on the level of due diligence required, that the certification program does not require them to look deeper and that they can meet regulator/examiner expectations with the level that the certification has set. It should then to faster exam processes. Without this FDIC backing, banks will remain under pressure to continually figure out how to meet expectations.

   Are there alternative approaches that would encourage or facilitate IDIs to use such programs?
   Venminder's current approach that assess specific control areas of third parties enables collaboration and visibility to both banks and third parties to help address the appropriate oversight around third-party risk.

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 provider**

    We recommend that the FDIC would encourage both banks and third parties to participate.

    The FDIC could also leverage the FFIEC exams of significant fintech providers as a source for information and way to encourage third parties to take part in the approach.

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?

    It is our opinion that this is about assessing risk, not compliance. Assessments should be done based on FDIC guidance and should be driven by criticality, PII access, probability vs. impact etc.

12. **Which technical and operational aspects of a model would be most appropriate for evaluation in a voluntary certification program?**
    Financials, SOC, Business Continuity and Disaster Recovery, Physical Security, Cybersecurity, Resiliency, Privacy, Reputation

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?**

    These models can certainly have a place in managing third-party risks but availability of relevant data is limited as you're only getting information generally available to the public. However, machine learning could be very helpful in establishing trends and predicting likelihood of future events.

We are of the opinion that due to the nature of an assessment process, it must involve the human element of experience.

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 follow the FDIC guidance in place today. The regulations today are solid, the only challenge is that it doesn't provide instructor guidance on the "how" nor a standardized process for completing it.

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?**

    - When choosing an SSO, demonstrated experience with both banks and third parties is a must.
    - The SSO must be willing to support bringing value to both sides of the network.
    - They should have the right subject matter expertise on staff.
    - Ensure that their environment is secure/info security protocols. That the provider is certifiable themselves.

    As long as the FDIC sets the standards, there is no reason why there should be one SSO.

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?**

    An independent SSO would be in a better position to rapidly adapt to new technology, for example, cloud providers. An SSO should be able to identify trends with new types of providers requesting certification so that new standards could be developed as adoption grows.

17. **What current or draft industry standards or frameworks could serve as a basis for a standard-setting and voluntary certification program?**

    NIST CSF or Shared Assessments (SIG) or CSA cadence. These are all limited in scope, technology focused and don't include requirements around reputation. On financial health, there is no shared standard today.

    What are the advantages and disadvantages of such standards or frameworks?
    Disadvantages can mean looking at well over 1,000 items in controls. They should be consumable, and it does need to be adaptable to the type of product or service being provided, such as criticality and PII access.

Much like at Venminder, the level of assessment is determined by the criticality and inherent risk level, including PII and inherent, so the level of assessment has to be appropriate.

A startup vs. mature third party providing a critical or high-risk product needs to be assessed at the same level. But, the level of inherent risk, should determine the level of assessments for third parties that is provided.

Today, the SIG has grown large and for many, it has grown so large that they don't know what to do with it, or don't have the internal personnel to understand and assess, "did it get filled out well?". A summary overview of rating based on deep dive analysis by an expert provides a digestible amount for both parties.

Do standards and voluntary certifications already exist for use as described herein?

As mentioned previously, Venminder takes an assessment certification approach. Third parties do not "pass" or "fail", but are assessed on individual controls, such as their financial viability – a third party is rated on individual controls with ratings of low, medium, high or severe risk, and given ratings of satisfactory, confident, vulnerable.

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?**

    It is our opinion that the likelihood is high as long as it ensures the long-term reduction in workload it implies.

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?**

    Venminder is a trusted provider and recognized leader of third party risk management with over 800 clients, the majority of whom are struggling to meet industry regulations in the financial services sector. Venminder already has internal expertise CPA, CISSP, paralegals and more in place. There is a difference between only collecting questionnaire information and actually assessing it with expertise in order to issue some type of certification. Just saying "yes I do it" and providing an answer without someone actually reading the document is dangerous. It is this assessment part that is burdensome to the banks as they know someone with the appropriate qualifications needs to read and assess them.

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 has already provided the guidance on what needs to be done. The FDIC should consider a role that is similar to the AICPA, which is who set the format and standard for CPAs to perform a SOC audit and the qualifications required to perform the audit. Then, any SSO can do it as long as they meet those qualifications. We are not suggesting an SSO should be a CPA firm as there are so many different

disciplines that are required to assess a third party for risk. The approach to standardization is valid. For example, an assessor of information security controls should require certifications such as CISA, CISSP, etc. Any third party that wants to get certified has to ensure that the SSO meets the standardized qualifications.

21. **What benefits and risks would COs provide to IDIs, third parties, and consumers?**

    COs should be an organization that meets the standards and meets the expertise. One that can provide a consistent control set for third parties to be assessed against.

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?**

    We recommend an annual recertification or reassessment process which is less costly and allows for the assessing of what has changed since the last assessment.

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?**

    In some cases, it would depend on the criticality and risk level of the third party as the level of assessment depends on all of those things. For those that require an onsite, leveraging the onsite examinations for those.

    Or would the COs need to test the model and generate their own test results?
    No, as long as the test or audit was performed by a qualified provider.

    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?
    A CO would have to be certifiable too.

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?**

    Yes, for reassessing**.**

    (1) If so, what appeal rights should be available to the affected third party?
    Visibility into the reason why their certification why it's no longer valid and for the third party to be able to receive clear guidance and steps on what it would take to recertify.

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

    May include email notification, manually verifying and system platform notifications. Today, Venminder notifies third parties if their scores changes and notifies banks if the score has changed (if it is within the period of their contract with Venminder).

    (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?
    Yes. Any additional information the regulators have about the third party via onsite audits (exams) should be shared with the CO's.

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?**

    The liability remains on the bank in how they are using the information provided. Only the bank can have a true understanding of this. For example, a provider like Venminder cannot tell if they have a backup provider or if the bank outsources the function but not the risk.

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?**

    Venminder today applies the standards and acts as the SSO and CO. Venminder uses feedback from auditor, clients, and builds assessments to meet all regulations including FDIC, OCC, NCUA, FFIEC. Based on this model, we receive great feedback from bank clients who have been able to reduce the workload. Many of the third parties that Venminder works with, highly value the collaborative approach where we provide them visibility and understanding into how they can achieve better scores.