Buyers guide:

How to evaluate identity proofing providers: RFP questionnaire template

In this guide, you'll learn how to evaluate identity proofing providers, which criteria to include in your RFP, and get access to a free questionnaire template.

data zoo

RFP questionnaire template

Many organisations continue to find it challenging to differentiate between solutions when choosing their identity proofing vendor. The saturated market requires organisations to undertake a more thorough and nuanced vendor selection approach. Traditionally, a vendor could be evaluated simply by trialling a solution in a proof of concept (POC). These days, organisations must take into consideration a range of factors such as orchestration capabilities, price, ease of implementation, compliance and efficient UX.

When security and risk management leaders are evaluating vendors, they should avoid asking yes or no questions. Instead, open-ended questions will help to uncover the methods and processes that vendors would suggest to address a specific requirement. The questions below can be used as a guide when creating an RFP for an identity proofing solution. Each question includes context to the value and reason for asking each question.

Identity proofing capabilities

Question	Context of question (i.e., why ask the vendor this question?)
Describe what identity proofing capabilities exist to confirm the real-world identity and genuine presence of a user.	*Most vendors will support a variety of identity proofing methods. It's important to understand whether the vendor offers orchestration capabilities, or whether you will need to manage how additional vendors are integrated into your workflow.*
Do you offer any additional capabilities, such as checking an identity with data-centric checks, screening users against global watchlists, and verifying additional risk or trust signals (e.g., phone, email)?	*If such features are offered by the vendor, it may present an opportunity to replace multiple vendor integrations and reduce cost and complexity.*
Can your solution extract identity data from government-issued identity documents?	*The use of OCR data extraction during the onboarding process will reduce friction and improve the UX.*
Do you offer a fully automated solution that does not involve any human analysts in the workflow?	*A fully automated workflow will give the quickest response. It is important to understand that human analysts can offer higher accuracy, although this will increase costs and response times.*
Describe what data you return to the client after a data or document check and after the selfie check.	*Understand whether the vendor simply returns a YES/NO response, or additional insight into the element-level attribute response, or whether they return a more nuanced confidence score.*

Data sources and coverage	
Question	**Context of question (i.e., why ask the vendor this question?)**
Summarise your coverage with respect to countries and document types supported.	*Most vendors will support a variety of identity proofing methods. It's important to understand whether the vendor offers orchestration capabilities, or whether you will need to manage how additional vendors are integrated into your workflow.*
Do you connect to other vendors or data sources in order to perform further checks on the identity data obtained from the user's identity document?	*Vendors should provide transparency on where they access their data and the information security controls in place.*
What steps are you taking to minimise the effects if one of your third-party integrations or data sources is down?	*Some vendors do not have redundancy strategies in place and will still charge you for a check to an offline data source. Seek to understand how the vendor is addressing down-time, or showing too high a degree of latency.*
Data sources and coverage	
Do you offer real-time feedback (e.g., incorrect DOB format, empty field etc) to help prevent the submission of incorrect or inaccurate information?	*Real-time feedback to users on identified input errors will lead to less time spent on re-entering information and higher match rates.*
Can a client define which data sources are invoked for identity data checks, or is this defined by you?	*Understand if the vendor can only offer a pre-configured solution or if they can give the flexibility to tailor your data source selection.*
Can relationships between rules be defined? For example, can the execution of one rule be dependent on the outcome from a previous rule? Can rules be nested together to create conditional logic and decision trees?	*There is a significant difference between having a monolithic group of rules that all execute on every transaction, and having rules that can be targeted more effectively based on other prerequisite rules having triggered.*
If you can create define relationships, does the platform generate alerts (e.g., instant, email or SMS) for exception events?	*Alerts can be useful to ensure there is awareness of exception events. Such features can help to reduce drop-offs and improve match rates.*
Does the vendor suggest new rules or how to optimise existing rules?	*Often, automated rule suggestions are not intuitive, whereas human analysts can add value and provide insights to suggest possible rules.*
Does the vendor offer the capability to make changes in a low-code or no-code manner?	*This reduces development efforts, with obvious implications in terms of cost savings and implementation timelines.*

Data privacy and compliance

Question	Context of question (i.e., why ask the vendor this question?)
Describe in which geographies your processing infrastructure is located and where data is stored.	*Obtain clarity about where users' PII is being processed.*
Is it possible to restrict that users' PII is only ever processed/stored in a given region (e.g., US, EU, AU)?	*Understand whether you can restrict this to meet your business requirements.*
Do you store users' PII (e.g., name, date of birth, image of face from document, selfie image) beyond the lifetime of the verification workflow?	*Some vendors purge PII as soon as checks are complete, others may retain it for various reasons (e.g., for you to view in their portal; for you to retrieve should you need it; for their own modelling purposes).*
If you do store users' PII, is it retrievable by clients? Or do you keep it purely for back-end modelling purposes?	*Obtain clarity about how and why your users' PII is being stored.*
If user PII can be stored by your solution and retrieved by clients, can retention periods and purge regimes be custom-defined?	*Some vendors may allow you to effectively use their system as your PII data repository, to remove the burden of you storing such data. If this is the case, it is important to understand what controls are in place.*

Key performance indicators

What metrics would you volunteer that best describe how effective your solution is?	*Different vendors measure the efficacy of their solutions in different ways. This question gives the vendor an opportunity to position its efficacy as it chooses.*
How do you assess whether the identity proofing decision that you made was correct or not? Do you rely on clients to give you feedback regarding fraud that they may experience? What mechanisms are available for clients to provide this feedback?	*If vendors are providing metrics about the efficacy of their solution, you must understand how they are assessing that efficacy.*

About Data Zoo

Data Zoo is a global identity solution for digital businesses. From Fortune 100 companies to startups, the Data Zoo orchestration helps companies build and scale a reliable solution to mitigate risk and prevent fraud.

See what you can do with Data Zoo

www.datazoo.com

data zoo