



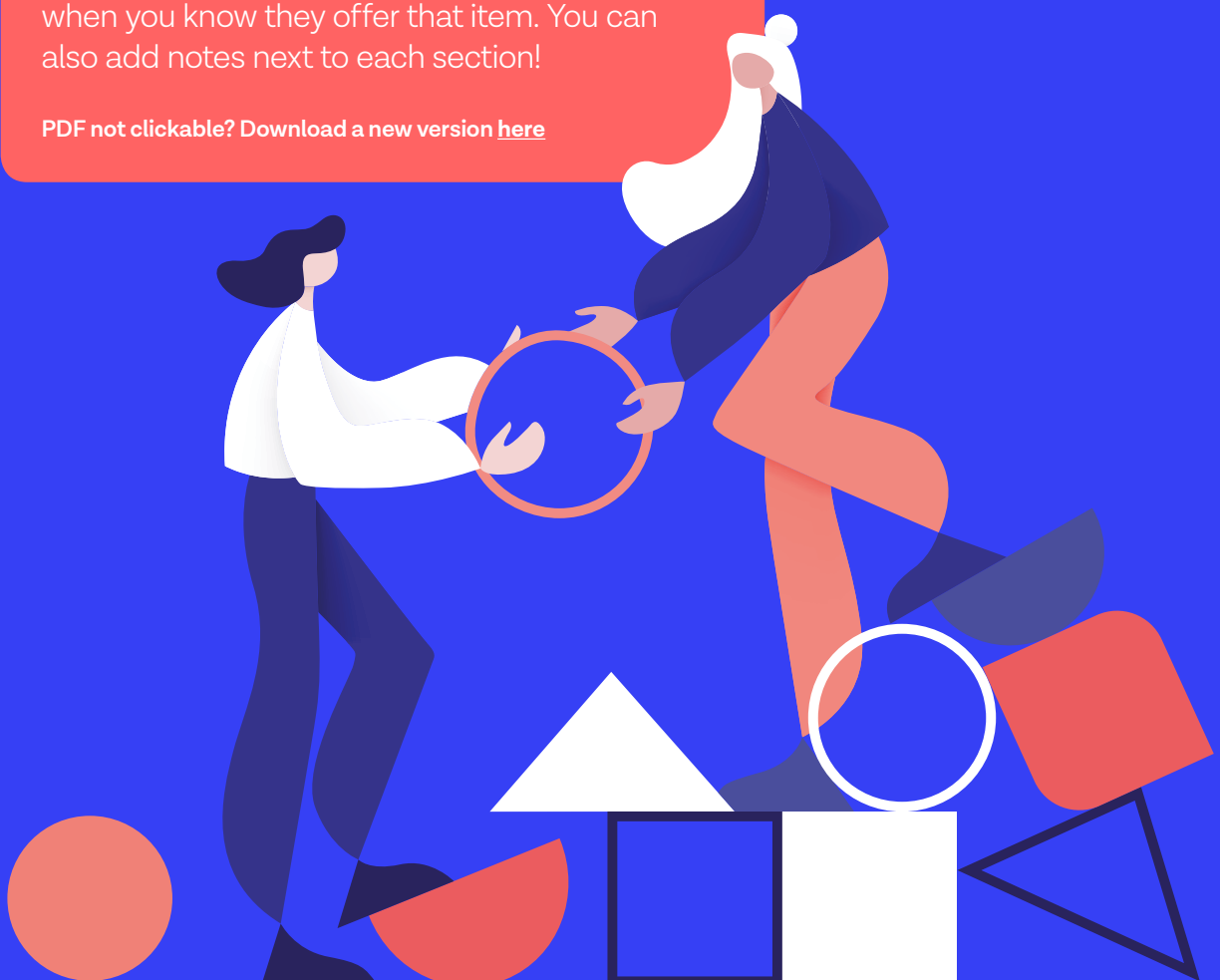
Evaluating identity verification solutions

Document and facial identity verification solutions

Click the check list!

This is an interactive RFP template. To evaluate a supplier, check off each section when you know they offer that item. You can also add notes next to each section!

PDF not clickable? [Download a new version here](#)



Section 1

Quantifiable Measures

Measurable techniques to qualify user experience, fraud accuracy and technical support.

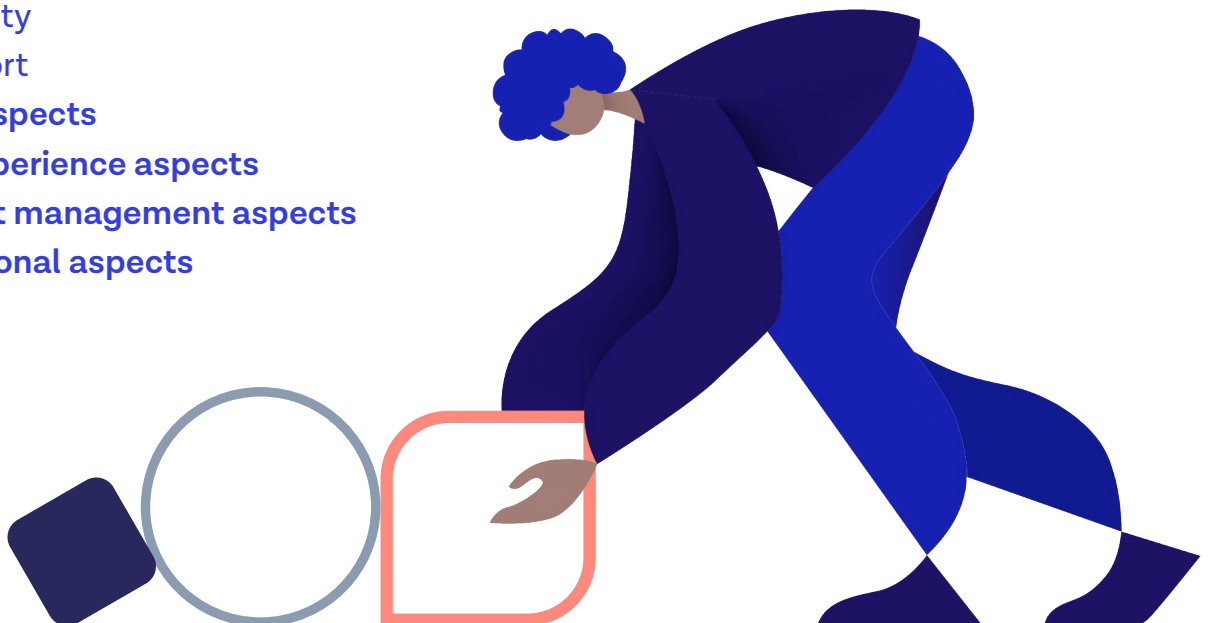
1. Key client metrics
2. Key vendor metrics
 - a. General
 - b. Technical

Section 2

Qualitative Factors

Those things you can't exactly measure, but which make a big difference.

1. Technical aspects
 - a. General
 - b. Security
 - c. Support
2. Fraud aspects
3. User experience aspects
4. Account management aspects
5. Operational aspects



Your key metrics

You should aim for an overview of your entire system. So calculate results here based on both internal teams and external vendors, as well as any additional factors those two introduce.

Provided	Description	Notes
	First time acceptance rate What percentage of documents are accepted on the first attempt? (i.e when users upload all of the required information for the first time)	
	Acceptance rate What percentage of all documents are accepted (overlooking number of attempts), when users have uploaded all of the required information?	
	Identified fraud accuracy Percentage of correctly identified frauds, percentage of incorrectly identified frauds, percentage of fraudulent documents missed.	
	Average time to resolution The average time it takes you to resolve identity verification cases.	
	Drop off rate & drop off funnel rates The rate of users dropping out of your signup, onboarding, and verification process. If possible, split your results by each different stage, and by each vendor involved (if external vendors are part of your system)	
	Rejection rate The rate of users you have to reject for reasons other than drop off (e.g they need to be a US Citizen to complete.)	

Pass Rates

How likely is it that a user will successfully complete the verification process?

Provided	Description	Notes
	Pass rate What percentage of total requests can be passed—with a clear result?	
	Rejection rate Percentage of total documents that the vendor can't process. This could be down to poor quality data, or the vendor being unable to process that type of data.	
	Input quality failures Percentage of input quality failures is a marker of how effectively the vendor can process documents.	
	Unsupported data failures Percentage of unsupported data failures helps you measure the vendor's ability to accept different data types (documents supported).	

Pass Rates & Fraud

Provided	Description	Notes
	Identified fraud accuracy Percentage of correctly identified frauds, percentage of incorrectly identified frauds, percentage of fraudulent documents missed by the vendor.	
	First time acceptance rate (if possible) How often can the vendor give a 'pass' result on a user's data the first time it is uploaded?	

Technical

Provided	Description	Notes
	API uptime %	
	Major outage incidents count	
	API response time & latency	
	Any additional services provided uptime % (dashboard, online portal etc)	

Turnaround Times

When you're looking at turnaround times, don't just look at the numbers. Take into account whether the vendor has an expert review process as part of the verification. This increases fraud accuracy, but can slow down timings. So weight this tradeoff accordingly.

Provided	Description	Notes
	Turnaround time The average time it takes the vendor to provide a result.	
	SLA adherence rate Percentage of requests which return a result within adherence of the stated Service Level Agreement.	

Document Review

Provided	Description	Notes
	<p>Internal intervention rate</p> <p>This percentage tells you how often the vendor provides a result that then needs extra client internal resources to resolve it.</p>	
	<p>Average internal intervention time to solution per request</p> <p>The average time your internal team or agent might need to spend on a single instance to reach a resolution.</p>	
	<p>Average cost of internal intervention to solution</p> <p>The average cost for your internal team or agent to reach a resolution in a single instance.</p>	

General

Provided	Description	Notes
	Is the vendor's documentation clear, understandable, publicly available, and easily accessible?	
	Are the vendor's API, SDKs, and other technical components easy to integrate?	
	Are the vendor's API libraries updated regularly?	
	Is the vendor transparent about service status e.g. status.vendor.com?	
	Does the vendor stand behind their technology e.g. tech blogs, outside speaking etc?	
	What is the breadth of supported platforms e.g. coding languages, supported devices, and supported libraries?	

Security

Provided	Description	Notes
	Does the vendor have a documented identity and access management system in place?	
	Does the vendor's solution support multi-factor authentication for any user/client dashboards/web interfaces?	
	Is the vendor's organization, and all aspects of the service delivery and product/software development, in scope of any industry standard certifications? (e.g. ISO 27001, NIST Standards,)	
	Are the vendor's employees and contractors vetted (and if so, how) before they're onboarded to your business?	

Support

Provided	Description	Notes
	Does the vendor offer customer and technical integration support throughout? And post integration?	
	How does the vendor offer support (email, chat, etc)?	
	How does the vendor communicate product updates, SDK changes, new features etc?	

Support

Provided	Description	Notes
	Does the vendor have a detailed internal QC process?	
	Does the vendor have an internal database of fraudulent data (faces and documents) and devices? And other ways of identifying repeat fraud?	
	Does the vendor dedicate internal resources to expanding its fraud knowledge, and maintaining those learnings?	
	Does the vendor have a mechanism for client feedback on fraudulent activity, to learn and improve their fraud prevention in future?	

User experience aspects

Look at the vendor's UI/UX. Assess the following questions as though you were one of your users, interacting with the product.

Provided	Description	Notes
	Can the user clearly understand what they are supposed to do?	
	Is the vendor prompting the user to provide better quality data whenever possible?	
	Is the user going to walk away from the experience with a positive or negative feeling?	

Account management aspects

Account management aspects

Provided	Description	Notes
	Does the vendor give you a dedicated account manager?	
	Does the vendor offer a comprehensive onboarding checklist?	
	Does the vendor have monthly business reviews?	
	Does the vendor have quarterly product workshops?	

Operational aspects

The key operational questions center around one thing: once you've gone through implementation with your vendor, what kind of internal team would you need to put in place to support with verification data?

Provided	Description	Notes
	How large is the internal team you'd need after implementation?	
	What would be the internal team's purpose? Would they process failed documents, escalate user issues, monitor to make sure key metrics are being maintained?	
	Let's say your internal team are looking into results returned, to resolve an issue. How does the vendor make it easy for them to decide what action they should take?	



Talk to us today onfido.com/signup

Or consider this your invitation to our product demo
info.onfido.com/product-demo