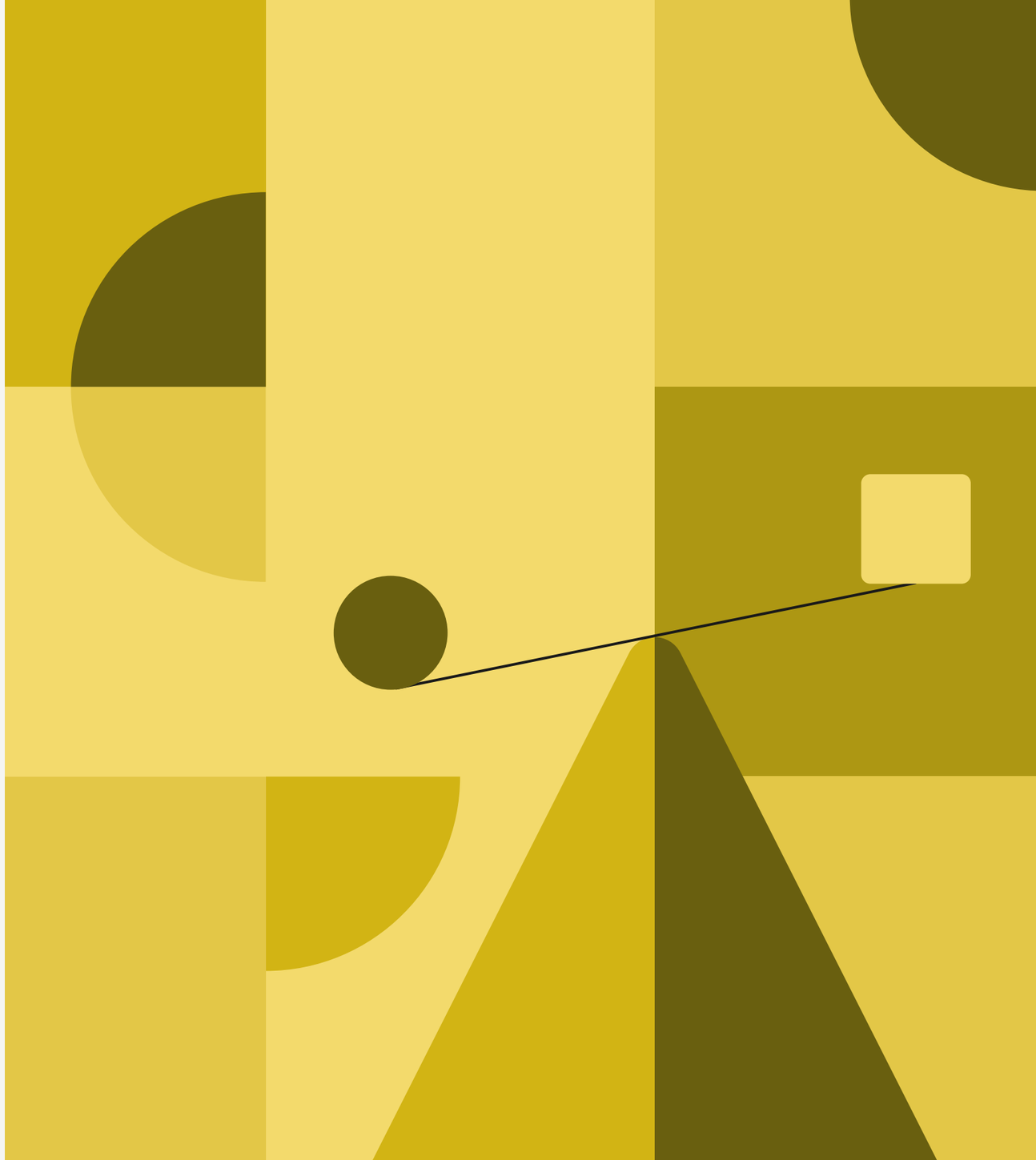
ALLOY

Your guide to building vs. buying an Identity Risk Solution

Understanding the different approaches, challenges, and benefits for banks

Table of contents



Introduction

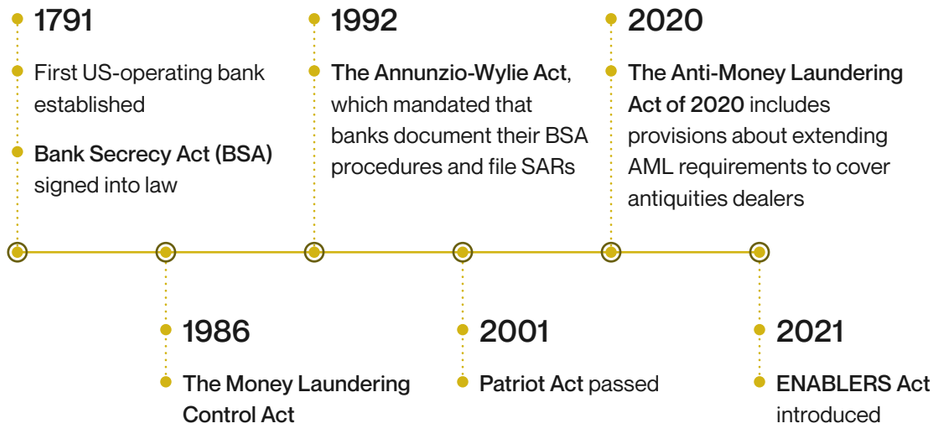
Federal regulations for US-operating financial institutions have been evolving since the creation of the first bank in 1791. These regulations often change in response to political or national incidents. After the 9/11 terrorist attacks in 2001, for example, the Patriot Act was passed. This legislation included provisions that require banks to establish Anti-Money Laundering (AML) programs and conduct customer due diligence to prevent financing of terrorist activities.

Both Know Your Customer (KYC) and Know Your Business (KYB) guidelines arose as part of the overall AML regulatory framework that was established to combat financial crimes and promote transparency and accountability in the financial system:

- KYC regulations require banks to verify the identity of their customers during the onboarding process.
- KYB regulations require banks to obtain additional information about their business customers, such as the nature of their business activities, ownership structure, and sources of funding.

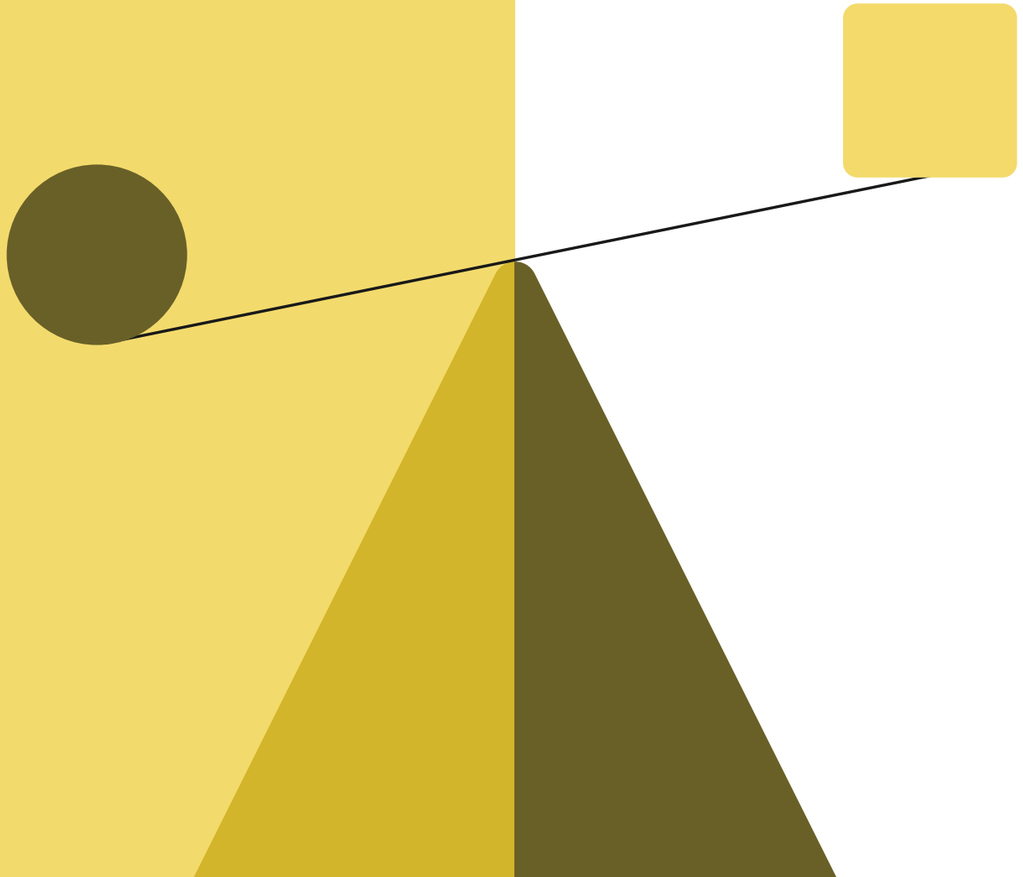
KYC/KYB processes also protect banks from fraud by helping them detect suspicious behavior and identify fraudsters at origination.

However, the state of fraud grows more complex every day. The more transactions and other banking activities move online, the quicker fraudsters move to adapt and exploit vulnerabilities in those systems.



In fact, approximately 18% of open accounts turn out to be fraudulent[1]. So, banks must prepare to future-proof against fraud, even as they navigate an increasing number of fraud attacks.

The complexities don't end there. There's also the issue of compliance requirements varying across markets, which makes the regulatory landscape even more difficult to navigate. Then, there's the fact that customers expect not only a seamless but fast onboarding experience. Beyond onboarding, banks have to consider that both KYC/KYB and fraud processes require ongoing monitoring because the risk associated with a business or consumer can change over time.



Certain factors — such as change in business ownership, frequent transactions with high-risk countries or sanctioned entities, unexpected shifts in financial performance, or other unusual or complex transactions that deviate from typical consumer behavior — can trigger additional verification needs. Flexible, ongoing monitoring helps ensure that the customer remains low-risk and compliant with applicable regulations, regardless of location.

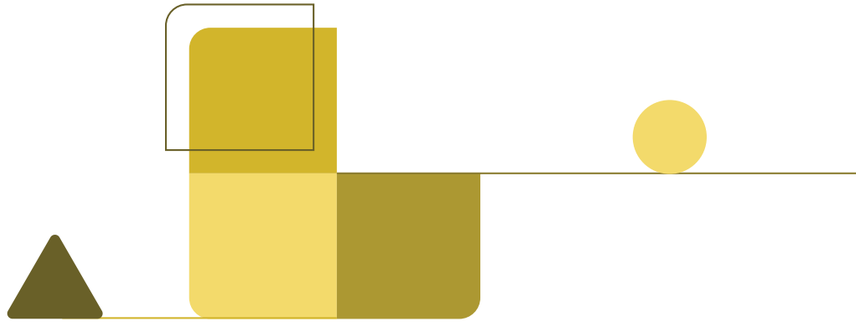
While some banks choose to build solutions in-house to help fight fraud, meet compliance requirements, determine credit risk, and automate KYC/KYB processes, others purchase an Identity Risk Solution. Leveraging a third-party Identity Risk Solution can help banks stay focused on onboarding new customers and speed up the go-to-market timeline of new credit offerings.

In this eBook, we explore:

- The components that make up a robust Identity Risk Solution
- When it makes the most sense to build your own solution in-house
- When it makes more sense to purchase a solution and outsource to a third-party vendor
- A checklist of questions to help banks understand what they need to ask their internal teams and review with potential providers
- Frequently asked questions banks face when they’re making the decision to build vs. buy

What is an Identity Risk Solution?

An Identity Risk Solution helps banks and other financial institutions make more informed decisions about identity verification, credit underwriting, and ongoing financial activity. It offers robust third-party integrations and streamlined access to comprehensive data via a single API to automate workflows and processes.



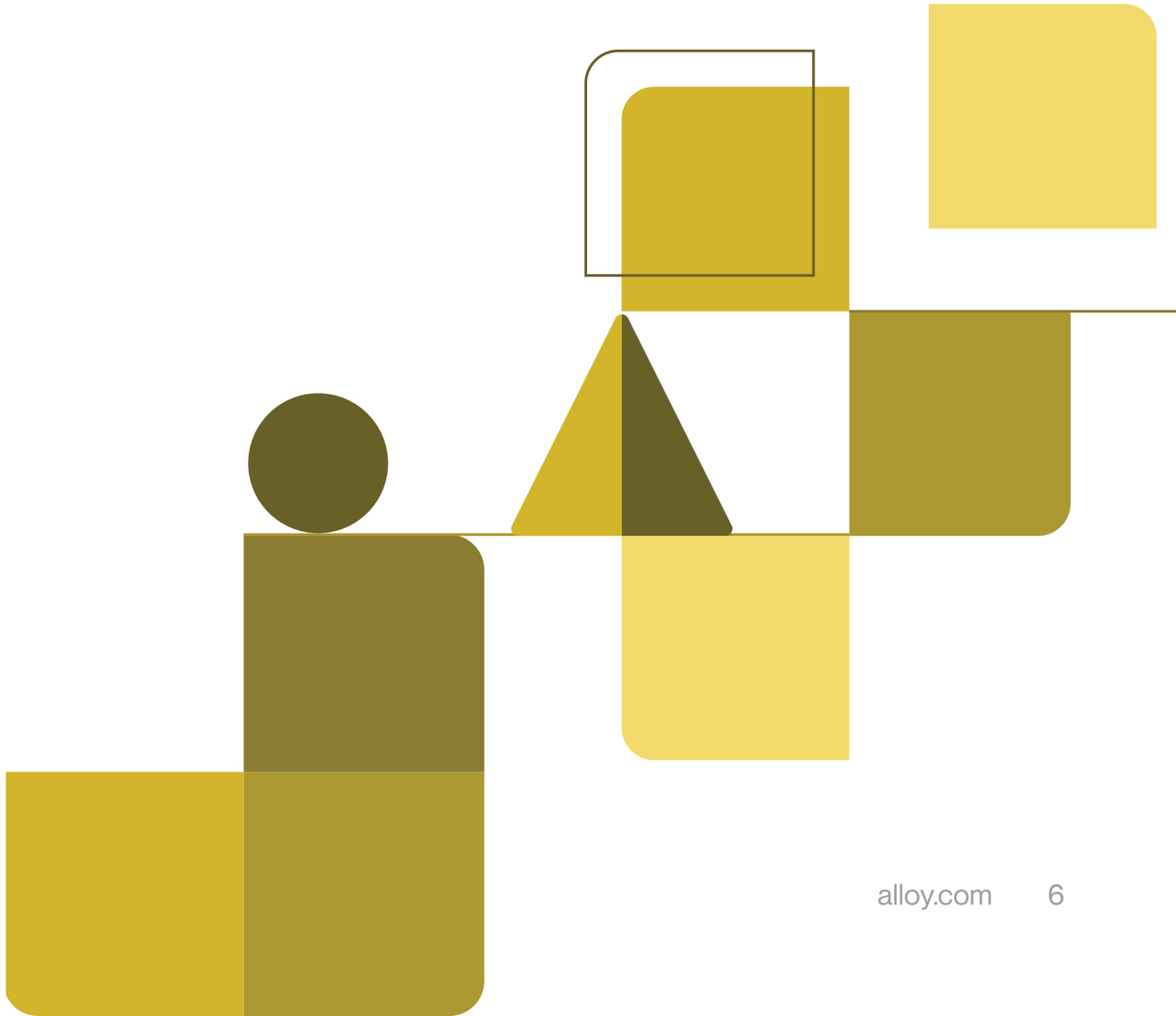
An Identity Risk Solution should offer ease of use, maintenance, and control, and have:

- Pre-established connections to multiple, alternative data sources that allow you to stay ahead of fraud and compliance changes and offer financial products and services to new markets
- A transparent view of the decision-making process with the ability to receive all of the raw data and use it to optimize your strategy and rule set
- The ability to increase your approval rate while mitigating fraud risk
- A seamless integration into your existing fraud and compliance tech stack
- A frictionless user experience
- The ability to add logic and customize workflows to automate decisions, including adding step-up authentication for risky applications or transactions, allowing a client to self-resolve
- A holistic view of your customers' risk, resulting in more automated decisions and fewer manual reviews
- An agnostic approach to multiple data source products to ensure the best outcomes
- The ability to manage multiple channels and products with different strategies
- A robust Software Development Kit (SDK) that makes it easy to add step-up verification into your front-end experiences
- A testing suite that allows you to test new policies or changes to your decisioning logic and see projected outcomes before going live

When banks leverage an Identity Risk Solution to have better control over decisioning and fraud strategies and build dynamic customer risk profiles, they can streamline their onboarding and ongoing monitoring processes, reduce manual workloads, and enhance the accuracy and consistency of their risk assessments.

An Identity Risk Solution can also be customized to meet specific regulatory requirements and risk tolerance thresholds, which helps banks comply with AML and KYC/KYB regulatory requirements, prevent fraud, while improving the overall customer experience.

In short, an Identity Risk Solution is a hub for a broad range of capabilities that manage risk throughout the entire relationship and customer lifecycle to increase the number of good customers banks can onboard, help them make better lending decisions, and stay on top of any changes in customer-risk levels.



What’s at stake for banks

For banks, the stakes couldn’t be higher. When today’s fraudsters are well-funded, tech savvy, and nimble, banks need to make fast, accurate identity decisions that catch fraud throughout the customer lifecycle. When it comes to fraud and compliance, skipping steps or overlooking details doesn’t only cost time, resources, and money — it could result in incalculable reputational damage and loss. Since customer trust and confidence are the cornerstone of financial services, it goes without saying that banks need to care deeply about which solution they adopt to mitigate risk and manage their fraud and KYC/KYB processes.

However, it isn’t uncommon for most banks to grapple with whether to build or buy this important piece of their tech stack. The decision is complex and requires careful consideration of factors such as cost, expertise, time to market, and compliance. Banks need to balance not only speed and accuracy, but also compliance and legitimate business needs like the prioritization of good customer experiences.

Ultimately, the success of a bank’s fraud and compliance programs can have a major impact on its overall financial performance and long-term viability.

Let’s explore further and discover the right solution for your organization.

Why your bank might prefer to build

You may choose to build an in-house Identity Risk Solution for two key reasons:

1. Familiarity

When you have direct oversight and ownership of the technology and data used for decision-making, leveraging existing engineering resources to build an in-house solution could provide more familiarity with not only the development process, but also the aligning decision and fraud strategies. You also may feel that an in-house solution is the only one that can be tailored to meet your specific, specialized needs and requirements.

2. Cost

Depending on the size of your organization and its resources, building an in-house solution could be viewed as more cost-effective than purchasing a solution from a third-party provider. If an established system is already in place, you may think you only need an upgrade or it's too complicated to integrate new solutions into your existing technology. In that case, your immediate expenses could be lower compared to the cost of buying a whole new system.

Also, if you employ a team of seasoned fraud experts and have the ability to expand your engineering resources, a build approach could make sense. You'd get to leverage their existing expertise and knowledge, and continue to build on it as well.

However, building an in-house Identity Risk Solution can also be challenging when you consider time to market, regulatory compliance, and the operational costs of ongoing maintenance and support.

Why your bank might prefer to buy

Buying an Identity Risk Solution might make more sense for several reasons:

1. Access to advanced technology

Whether it's a higher volume of applicants or the need to support a growing number of product lines, you need technology that can accelerate the transformation of the digital customer experience while staying one step ahead of the increasingly challenging fraud landscape. Your solutions need to continuously iterate decisioning algorithms and add step-up verifications on an as-needed basis. As a result, you want to be able to easily test changes to your strategies and add new tools into both your front-end and back-end. In contrast, hardcoded legacy software might be too inflexible to keep up with the necessary changes.

2. Use of data orchestration vs. a linear approach

A third-party Identity Risk Solution often partners with multiple technology and data providers to automate and aggregate a seamless flow of data across systems and sources into a single dashboard — a process known as data orchestration. In contrast, the linear approach of most in-house solutions or legacy systems involves manual data movement and limited integration, resulting in inefficient data silos and decision-making. Data orchestration enables real-time insights, consistency, and accessibility. The best third-party solutions also provide global data coverage to help you onboard customers who are increasingly interested in doing cross-border business as well as existing customers who want to expand to new markets.

3. Speed and scalability

Purchasing from a third-party vendor actually can be faster than building an in-house solution. When the third-party Identity Risk Solution is already developed, tested, and specifically designed to meet regulatory compliance requirements and adapt to ever-changing fraud risks, you can quickly implement it, minimize disruption to operations, and reduce time to market for new products and customer segments. In contrast, an in-house solution might need to be built from scratch, limiting flexibility and causing substantial delays to your product timelines.

Also, third-party Identity Risk Solutions are often designed to integrate with your existing systems and processes, making it easier to scale solutions and meet growing customer demands — no need to rip and replace!

4. Operational efficiency

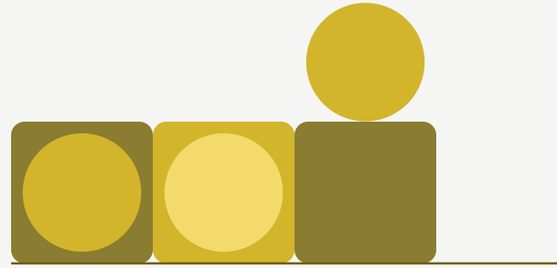
65% of banks say that their employees spend too much time on manual identity verification, and 61% say their lack of agility in managing fraud and identity processes is limiting their growth and leading to lost revenue opportunities. The long-term value of streamlining this work to a third-party Identity Risk Solution is the amount of time it can save and the bandwidth it can add to your internal resources.

Would you rather your engineers work on building out new product lines for your customers, or would you rather them work on building and maintaining your identity risk management systems? If the third-party solution is a simple API and user interface, you can design workflows that enable automatic action on high-risk or suspicious activities — all without having to code. By the same token, when you want to add new data sources or make changes to your workflows, you can do so without pulling in your engineering team. As a result, they stay focused on your core product roadmap and aren't distracted by additional or ongoing API maintenance.

Ultimately, the decision to buy an Identity Risk Solution from a third-party vendor should be based on a careful assessment of your needs, resources, and strategic objectives, as well as the capabilities and reputation of the vendor.

A build vs. buy checklist

To get a better sense of the right approach for your organization, we've created a checklist for you to review with your internal teams, plus additional questions to ask potential vendors if you're preparing to buy.



Internal review

- [ ] What do your current identity decisioning and fraud solutions look like?
- [ ] What's working?
- [ ] What isn't?
- [ ] What internal pain points are most important for your organization to solve?
- [ ] Can your in-house engineering team design the decisioning process, build the necessary third-party integrations, and easily handle ongoing maintenance?
- [ ] Do you want your teams to focus on risk management or growth?
- [ ] How much risk are you willing to manage on your own?
- [ ] Are your AML and KYC/KYB processes scalable?
- [ ] Are your fraud processes scalable?
- [ ] Can they accommodate future growth?
- [ ] Do you have the resources and bandwidth to continuously evaluate and improve fraud, AML, and KYC/KYB processes to ensure they remain effective and efficient?
- [ ] Do you have the resources and bandwidth to streamline your fraud, AML, and KYC/KYB processes and reduce manual effort?
- [ ] Does your solution improve operational efficiencies?
- [ ] Does your solution provide the ability to view all of the data in one place?
- [ ] Can you easily add new customer segments to your workflows?
- [ ] Can you easily test new data sources? Can you easily add new data sources into your tech stack?
- [ ] Can you easily add additional step-up verifications to your workflows on an as-needed basis?

Vendor review

- [ ] What are the vendor's core product offerings?
- [ ] Who are the founders?
- [ ] How long ago was the company founded?
- [ ] How much funding does the company have?
- [ ] Who are their current clients?
- [ ] Does their strategic roadmap show significant investments and advancements to align with market need?
- [ ] What data source integrations does the vendor offer? Are these integrations pre-built?
- [ ] Are there specific features that meet your business needs and goals?
- [ ] Can the solution be customized to meet additional needs?
- [ ] Is it a "no-code" or light development solution with a user interface (UI) that's designed for business users?
- [ ] How does the vendor stay up to date with evolving regulations and best practices?
- [ ] How does their solution handle data privacy and security?
- [ ] How much funding does the company have?
- [ ] Does the vendor solution integrate with the bank's existing systems and workflows?
- [ ] Can the vendor solution complement your existing software?
- [ ] What level of customer support and training is provided?
- [ ] What is the pricing model?
- [ ] Can you anticipate any hidden costs?
- [ ] What is the track record and reputation of the vendor?

FAQ

Our business is complex. Could an Identity Risk Solution cover all of our use cases?

The key to an Identity Risk Solution's flexibility is the multiple data sources it connects to, which result in more robust AML, KYC/KYB, and fraud processes that cover most of, if not all, of your use cases.

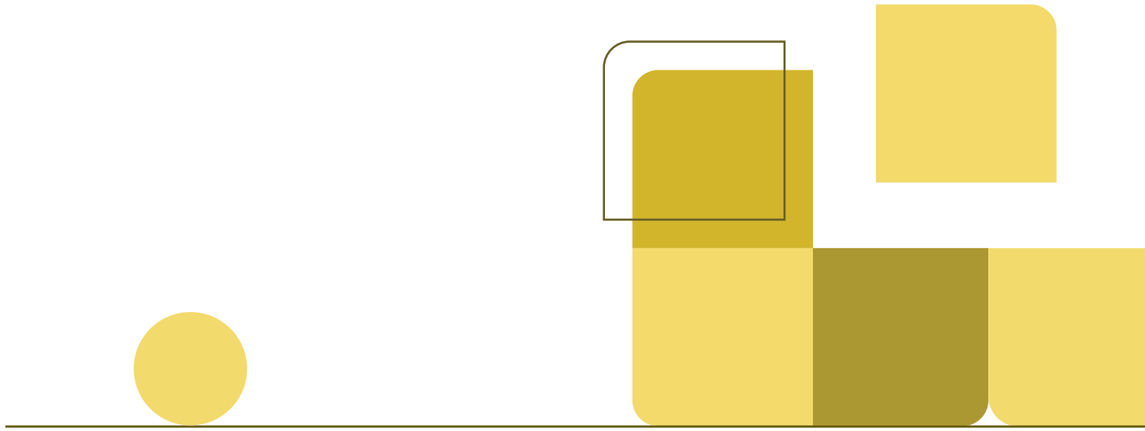
Multiple data sources enable:

- Cross-referencing of information, allowing for validation and verification of the data provided
- Access to a wider range of information about an entity or an individual, including data from public records, credit bureaus, government agencies, and other third-party sources
- An additional layer of backup, so processes can continue and won't be delayed or disrupted if one data source has been compromised

Different sources of data can be used for different use cases, depending on the specific business and compliance requirements. This allows for process customization that can be tailored to meet your unique needs.

Our organization already has existing contracts with third-party data providers. Shouldn't we just manage those costs directly?

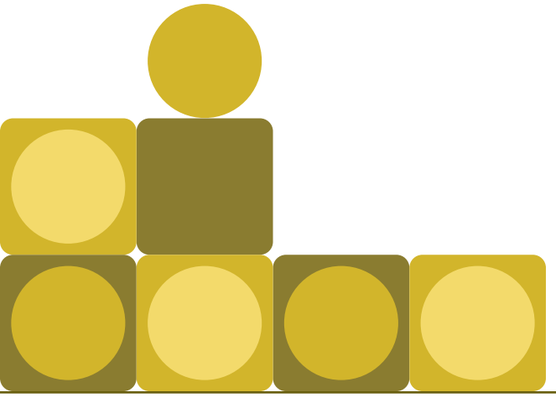
You could, but an identity risk management vendor may be able to get you the same data for less, without being locked into longer-term contracts. If this is important to you, look for an Identity Risk Solution that still allows you to maintain your own contracts with data providers or leverage the Identity Risk Solution's relationships with data vendors.



If we have our own team of engineers, why wouldn't we build?

Let's rephrase that question a bit to get to the heart of the matter. How do you *want* your in-house engineers to spend their time? If you choose to purchase an Identity Risk Solution, then your engineering experts can focus on the bank's core products and services. You avoid dedicating time to building and maintaining an in-house solution, which can be complex and resource-intensive.

With a third-party Identity Risk Solution, your organization should have increased productivity, improved efficiency, and, ultimately, better business outcomes.



But what if we've already spent a lot of time, resources, and money building our own solution?

An Identity Risk Solution doesn't have to be a "rip and replace" experience.

You can use it alongside your existing software to cater to new customer segments — like Small and Medium Enterprise (SME) banking, equipment leasing and finance, non-profits, professional service firms, government agencies, and international customers — that your legacy tech might not be able to easily support.

Or, you can use it to add better step-up verifications to your existing process on an as-needed basis when your legacy platform isn't able to integrate those additional precautions quickly enough. Then, an Identity Risk Solution becomes a component of the decision process and unlocks a lot of different options around step-ups — like device or behavioral biometrics or one-time passcodes — without having to replace your current solution.

How will our in-house fraud and compliance teams maintain their involvement in decisioning and fraud prevention processes if we choose to outsource?

First and foremost, your teams should always be involved to ensure effective decisioning, fraud prevention, and process refinement.

Although an Identity Risk Solution helps automate parts of the process, there will always be a need for your in-house teams to work alongside these tools. But, just like your in-house engineers, purchasing a solution allows these teams to work at an even higher level where their focus is on core services and building core products.

Imagine, your analysts and subject matter experts will no longer need to pull data manually and instead can focus on optimization and reporting metrics.

Won’t onboarding a new system take time?

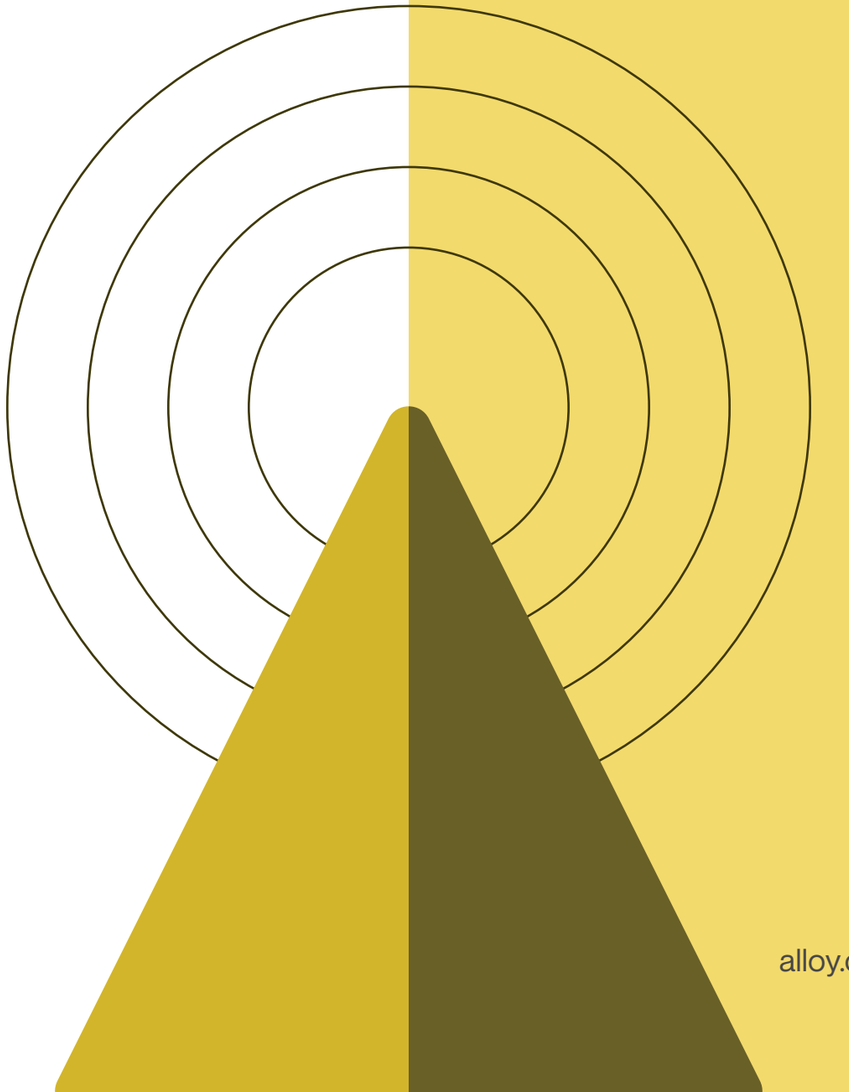
The short answer is yes. Any new system comes with some switching costs and onboarding time.

However, a vendor should be able to tell you exactly how long onboarding will take and what it will entail, so you can set reasonable expectations and train your teams on the new software.

Look for onboarding times of **8-12 weeks**, and read through the vendor review questions in our checklist below.

Making the final call

What matters most is that you feel confident and comfortable in the route your organization takes to handle its decisioning and fraud prevention processes. Whether it's purchasing a solution and working with a third-party vendor or building the internal infrastructure for your own platform, adhering to regulatory compliance and mitigating risks — while providing the best customer experience you possibly can — is of paramount importance.



Alloy solves the identity risk problem for companies that offer financial products. Over 500 banks and fintechs turn to Alloy's end-to-end identity risk management platform to take control of fraud, credit, and compliance risks, and grow with confidence. Founded in 2015, Alloy is powering the delivery of great financial products to more customers around the world. Learn more at alloy.com.

References

1. FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY ALLOY | JANUARY 2022