

Banking for startups

A founder's guide



HSBC Innovation Banking

Contents

▼ A partner for growth	3
------------------------	---

Chapter 1

▼ Choosing a bank: Why it matters and what to look for	4
--	---

Chapter 2

▼ Questions to ask	7
--------------------	---

Chapter 3

▼ Navigating your Treasury Policy	11
-----------------------------------	----

Chapter 4

▼ What to expect from onboarding	16
----------------------------------	----

Chapter 5

▼ Managing fraud risk	20
-----------------------	----



A partner for growth

The right bank can help you to manage risk, pursue new opportunities and focus on key milestones – but how do you find the best fit for your startup?

In this guide, we take an in-depth look at how to find a bank that's well-suited to you, what to expect from the relationship and some of the ways your provider can help you succeed.

Chapter 1

Choosing a bank: Why it matters and what to look for

Finding the right banking partner means you can focus on what matters most: building and growing your business. Many startups and scale-ups are naturally drawn to providers with slick UX, but when you're choosing a banking partner it's important to look beyond its digital presence and explore the offering as a whole.

All businesses want a bank who keeps up with them. That means staying ahead of industry advances, giving you solutions that scale with you, and eventually becoming a connected partner you turn to for innovative solutions.

Understanding of the startup ecosystem

A bank that has a dedicated startup team will naturally be more familiar with your unique challenges and opportunities. Tailored support – like industry-specific insights, networking opportunities and connections with venture investors or mentors – can help you gain real traction in the marketplace.

Reliable day-to-day banking

Startups may want a banking partner that provides seamless account, deposit, payment, foreign exchange (FX) and digital solutions, as well as smooth application programming interfaces (API). It's critical to ensure that your bank can not only offer the solutions you need today, but also provide access to a wider set of capabilities as your requirements evolve. This approach helps you scale your business effectively, and minimises your reliance on disparate, single-solution providers.

Flexible financial solutions

Fixed options can be too restrictive for startups. Financial solutions should be as dynamic and adaptable as you are.

Your bank should be able to offer products to suit each stage of your growth journey.

This may involve diverse funding options – such as business loans, lines of credit and venture capital connections – that align with evolving needs. Flexible financing solutions can empower you to seize growth opportunities without facing cashflow constraints.

Scalable global infrastructure and technology

As you grow, your banking needs will change. Scalable financial technology solutions – like global digital banking platforms, apps and data analytics tools – enable you to streamline operations and make data-driven decisions as you evolve. Selecting a bank that has global capabilities and international banking can also allow your company to enter new markets and scale your global footprint.

A strong partner to support long-term growth

From providing access to funding to offering more sophisticated products and solutions, a strong banking relationship can help you build the resilience and adaptability to navigate rough waters. A bank that appreciates your growth trajectory will be able to support you in making financial decisions that align with your long-term strategy.

Opting for a bank with a dedicated relationship team can also enable smoother onboarding and integration with financial platforms, like Xero and NetSuite. Your relationship team can get to grips with your business and current accounting requirements and may be able to offer their experience from integrating platforms with previous clients. This investment in the relationship can help your bank better understand your business.

Now you know what to look for in a strong banking partner, and the benefits the right relationship could bring to your business, it's time to find out whether a prospective bank can deliver on its promises.



In summary

- To compete and succeed globally, you need an active banking partner with shared goals.
- Tools, connections and know-how from your bank should help you adapt and scale at speed.
- Your banking needs will shift as you grow, so tailored, flexible solutions are key.

Chapter 2

Questions to ask

Finding a banking partner may seem like one more item on a long list of things you need to do, meaning it might not get the level of thought it deserves. After all, most banks seem to do the same thing, so investing energy in making a choice could feel like a waste of precious time.

However, the right decision can be a vital component of future business success. So, how do you choose who to trust with your business?

Asking a few key questions, such as the ones below, can help you gauge whether a bank truly understands your unique needs and can support you as your business grows.

1. How will your services accelerate my startup's growth?

Tools and products built for your type of business can be a game-changer as you move from pre-seed to post-IPO (initial public offering).

As your business expands – whether that's through growing your headcount, moving through different funding rounds or venturing into overseas markets – you'll likely need an easily accessible, clear picture of your banking operations.

Online banking platforms may be a given, but even in the early days of your business, real-time access and customisable setup features can put you in control of your organisation's finances wherever you are. Additionally, ensuring that your bank can directly integrate with your accounting platforms will save time and automate financial workflows.

Services like business accounts, credit options, FX and payment processing can be helpful in taking care of your day-to-day banking needs, but they can also do more. These solutions can help to automate and simplify payments, processing, reporting and reconciliation – streamlining your business operations in a cost-effective, secure way that helps you run things more efficiently.

If you have global ambitions, it's helpful to verify that your bank has the capabilities you need sooner rather than later.

A provider with a global network will allow money to be sent internationally through traceable wire transfers, while expertise in FX risk management can help you navigate FX markets and mitigate risk.

2. What's your approach to supporting startups?

Not all banks are set up to support startups. Consider whether your bank can help fulfil your growth ambitions.

Dig deeper with questions like:



- What solutions can the bank offer as my business grows?
- Does it have sector expertise?
- Can it offer networking connections?
- Is it set up to support your international expansion?

Facilitating working capital, providing revolving and flexible lines of credit, offering venture debt and even making venture capital connections can help you move forward at speed. Treasury services and payments infrastructure designed with rapid growth in mind can also enable growing volumes of domestic and international transactions in an efficient, secure way.

It's not always easy to find the best path – particularly if you're doing research on your own. Working with a bank that assigns a dedicated relationship manager can help you create the right solution set for your business.

Relationship managers aren't necessarily just banking experts. Look for a team that has meaningful sector expertise, so they can provide relevant guidance about financial planning and growth strategies. Ideally, find a bank that has a background in building and scaling startups, or experience raising venture funding.

3. What fees and charges should I account for?

Dynamic banking solutions inevitably come with fees. Request a clear, transparent schedule of these charges – when they're payable and whether different fees apply to different levels of accounts – as early as possible. As a startup founder, you'll be all too aware that operating budgets are often tight, so understanding the fee structure upfront is essential for financial planning.

Also consider monthly account fees: some banks may charge them, while other products are free to maintain. Be mindful of what you'll get for your money. Sometimes, fee-paying accounts may be the best option as they offer enhanced features, like global online banking platforms or multi-user access.

It's also important to look at other potential costs linked to specific services and providers.

The risk of unexpected expenses can be overwhelming and, as a founder, you need to be prepared. All banking costs and their timings should be clear so you can factor them into your financial planning.

Consider questions like:



- Will you face additional transaction fees?
- Will there be charges for late payments?
- What are the interest rates for FX transactions or cash savings?
- Are there onboarding fees?
- What are the cost implications of overdraft facilities?

4. Can you provide references or case studies of other startups you've partnered with?

Hearing about the shared experiences of other startups can provide valuable lessons and insights. Other founders can share real-life stories of a bank's onboarding process, reliability, support and overall effectiveness in fostering startup growth.

For example, can the bank's relationship managers empathise with your journey? Do they understand what a startup goes through on a daily basis? And will they offer products and services that are truly relevant?

While client testimonials and case studies are certainly helpful, a bank that also connects you with a community of peers takes this support one step further. Accessing these networks enables founders to listen to one another, share wisdom and learn from each other's mistakes.

5. How quickly can we expect to be onboarded?

The prospect of time-consuming bank onboarding processes can be off-putting, so it's worth looking into this when considering prospective banking partners.

Applications can be as simple as providing details about the business and its owners. This generally requires certain documentation such as proof of business address, Companies House registration and estimated turnover, as well as personal information about the founder alongside any partners or directors.

Banks must then undertake checks to verify these credentials, and the processing time can vary. Mandatory Know Your Customer (KYC) procedures can be time-consuming, but it can also give you peace of mind to know that your bank takes the time to verify the legitimacy of its clients.

Dedicated relationship managers can prove crucial to successful onboarding. They assess the eligibility of each startup on its own merits. A relationship manager can also provide an estimated timeline and a breakdown of all relevant documentation at the start of the process, and keep you informed of progress through each stage.



In summary

- Carefully select your bank that can meet your startup's unique requirements.
- Asking specific and relevant questions narrows your search, helping you find the best fit.
- Being clear on your needs and expectations early on sets the tone for a productive, transparent relationship.

Chapter 3

Navigating your Treasury Policy

As you go through the process of asking questions and evaluating providers, you can also consider the practicalities of how a well-matched bank can help your startup.

A good example of this is supporting the development of your Treasury Policy – a task that might not be near the top of your list of priorities, but certainly should be. Clear policies give you a framework to manage treasury activities and limit risks by defining how cash and financial risk are managed, including assigning ownership, implementing controls and installing a system for regular reporting.

Constructing a robust Treasury Policy framework can improve the financial oversight of your business and promote sustainable growth while helping you avoid common cashflow issues.

What is a Treasury Policy and why may you need one?

A Treasury Policy is a document that outlines how your business manages its money and addresses financial risks. Simply put, it's a plan to help ensure you've got the funds you need to run the business and meet your long-term strategic goals.

In addition to enabling efficient management, a Treasury Policy can help you embed sound treasury risk management processes for your business. It's crucial for mapping out the procedures, policies and operating parameters you'll likely need to safely navigate the changing financial environment.

Managing financial risk in this way is critical for growing your business, as it means there's a plan in place when challenges inevitably arise. It also gives you a compass to guide your financial decision-making, which can either accelerate or slow your overall growth.

A formal, auditable Treasury Policy can cover all the different activities your business undertakes, as well as helping you put operational steps in place to anticipate financial risks.

Developing a Treasury Policy

The four key actions below can provide a solid foundation for your Treasury Policy framework. This fundamental structure can be expanded and built upon, depending on your needs and circumstances.

1. Identify and assess: Set clear objectives and define risks

Your objectives should be clear, concise and relevant. You may want to consider how security, liquidity and yield relate to one another.

Risks you may want to consider:

- Liquidity risk
- Interest rate risk
- FX risk
- Counterparty risk
- Credit risk
- Commodity risk

Key considerations include:



- Risk appetite
- Identifying financial risks arising from operational activities such as technology, processes and fraud
- Regulatory requirements and banking covenants (legally binding conditions in loan agreements)
- The availability of diverse funding and capital sources to support growth
- Ensuring sufficient liquidity and capital are set aside to protect against short-term stresses
- Optimising excess funds for returns

Risk definitions should be clear and unambiguous to ensure general understanding. State the size and sources of risk exposure, as well as the types of products that can be used to mitigate them.

Bear in mind that risk measures tend to be determined by the type of risk. For example, FX exposures could have risk measures based on value-at-risk (VaR), while credit exposure risks might be assessed using the credit ratings, counterparty risk of the banks, or the providers you work with.

A risk management policy can also be a useful internal communication tool to ensure a consistent understanding across the business.

2. Evaluate: Assess your risk exposure and actions

Once you've defined potential risks, it's crucial to review your risk exposure, appetite and triggers, and assign ownership before any risk events occur.

Evaluating and modelling the likelihood and size of potential losses or gains can be helpful when setting a strategy to manage risks.

Your risk response not only defines the limits for each risk, but also takes your business objectives and tolerance into account.

For example, is it best to avoid the risk entirely, or to try and use controls to reduce its impact? Could the risk be transferred by buying insurance or shifting it to your customers or suppliers? Or should you accept that certain risks may fall within your risk appetite? Be aware that your response strategy may create new issues; for example, the use of insurance introduces counterparty risk.

3. Respond and control: Define your risk response and implement prevention strategies

The next step is to define how your business will respond if a risk materialises and what controls could help to prevent risk events from happening in the first place.

The goal is to ensure treasury activities are undertaken in a controlled manner to minimise undue operational risk. Day-to-day risk controls should include a mixture of preventative, detective and corrective tools.

For example, you may opt for policies such as:



- Having a clear distinction between staff who initiate payments and those who account for transactions
- Implementing a system of confirmation for all counterparty transactions
- Requiring payment instructions/confirmations to be authorised

4. Monitor: Measuring, testing and reporting

Treasury management reporting is crucial to ensuring your policy's effectiveness. It provides oversight of your cash position, including transactions against your treasury objectives. You can choose to produce daily reports on the movement of cash, borrowing and lending, alongside more in-depth monthly reports. These monthly views could include analysis of cash and borrowing, as well as forecasts, a focus on liquidity and the security of funding, and even a review of your bank relationships and services.

Measurement of risk exposures, triggers and appetite can be delivered using key risk indicators (KRIs). Establish a system for reporting KRIs and the performance of the associated controls so that your key company risks can be monitored.

A performance management framework can help track the overall effectiveness of

your Treasury Policy and ensure that it's implemented correctly. Many startups choose to have a regular, independent review of their policy, how it's designed and its operating effectiveness.

Designing and implementing a Treasury Policy can help you plan for financial risks in a systematic, structured way.

To provide a starting point for drafting a Treasury Policy, we've created this example checklist, based on our four key components. This is not exhaustive and you may want to add or remove elements depending on your needs.



Treasury Policy checklist

1. Identify & assess

Policy name

What is your document going to be named?
e.g. [Company name] treasury policy, liquidity policy etc?

Policy objective

What is your treasury policy trying to achieve?
Objectives: security, liquidity and yield

Risk description

What are your risks and how do they arise?
Define your risks

2. Evaluate

Risk exposure

What is your exposure before and after existing risk mitigation?

Express as the likelihood and size of potential loss or gain. The measure could vary by type of risk e.g. counterparty credit exposures based on credit ratings. Additionally, are there any natural hedges (offsetting risks) in your company that reduce the exposure?

Risk appetite

What is the amount of this risk that your company is willing to take to meet your objectives?

The risk exposure typically should not exceed your pre-agreed risk appetite.

Risk owner

Which individual/department is responsible for managing the risk? Include when the treasurer should report back to anyone e.g. The board/fd in the company, and list authority limits (if not specified elsewhere).

Risk triggers

What are the risk triggers, have they been determined and approved and is an action plan in place?

These triggers are usually warning signs that the exposure is approaching its risk appetite and action may be needed. You may want to create reports to escalate to senior management with recommendations on how to manage the risk exposure, such as reducing the underlying risk or mitigating the exposure.

3. Respond & control

Risk response avoid, transfer, reduce, accept

What is your risk response?

This should typically align with the policy objective, for example, eliminate fx transaction risk due to foreign currency receivables. Some options for the risk response: i) avoid (e.g. Don't enter a market) ii) transfer (e.g. By insurance or to 3rd party) iii) reduce (e.g. Using controls); and iv) accept (e.g. If not material)

Key risk controls

What are your key risk controls?

A mixture of risk controls can be described here: preventative, detective and corrective. List authorised instruments and, if necessary, hedging strategies. List authorised counterparties with risk limits.

4. Report & monitor

Key risk indicators

Have you selected KRIs that measure the risk exposure, related hedges (if relevant), risk triggers and risk appetite?

Reporting

Have you established a system for reporting KRIs and the performance of the associated controls so that senior management can monitor and control the key risks within the company?

Assurance

Have you developed a system for ensuring that treasury policies are implemented as agreed?

For example, independent regular review of the policy, and design and operating effectiveness of controls.

Update of policy

Have you defined the process for updating this policy, including the frequency of update and approval process?



In summary

- A holistic approach to treasury can help you manage liquidity and cashflow.
- Clear action points provide a structure for a Treasury Policy framework, allowing future financial decisions to be made effectively.
- Practical considerations like support with corporate treasury can help you assess banks and find the best partner for you.

Chapter 4

What to expect from onboarding

When you feel confident that you've found a good fit for your startup, you can focus on what's involved in kicking off the relationship.

For the most part, banks aim to make onboarding as smooth, seamless and secure as possible. The process will include, but is not limited to, the following:

- Verifying your identity
- Collecting necessary documents and data
- Opening the account
- Registering devices for digital banking
- Setting up authentication procedures

It's important to note that onboarding is unique to every bank, and the various checks, questions and procedures involved differ between providers. The documentation you'll likely need to provide and the exact process involved could also vary depending on your business.



Starting onboarding: General documentation and questions

As you begin your onboarding journey, you could be asked upfront to provide basic documentation validating your business. Details such as your Companies House registration and proof of address may have been provided while you were assessing potential partners, but it's a good idea to have these to hand in case you need them again.

It's also important to be well-informed and prepared for the KYC process, which typically consists of five steps:

1. Customer identification:

This involves collecting customer information, such as name, address, date of birth and government-issued ID.

2. Customer due diligence:

This step focuses on verifying the accuracy of the collected information, often using documents like passports, utility bills and bank statements.

3. Enhanced due diligence:

This is a more in-depth review for clients that work in higher-risk industries or geographies, including those from countries with weak anti-money laundering enforcement.

4. Continuous monitoring:

This involves monitoring customer accounts and transactions for suspicious activity and potential risks.

5. Reporting and compliance:

If any questionable activity is uncovered during the KYC procedures, the bank will need to report this to the Financial Conduct Authority (FCA).

Another useful step when preparing for onboarding is to anticipate potential questions about your business and be ready to answer

them. If your bank offers a dedicated representative for this early phase of the relationship, they might ask you about:

Potential questions



- What your business does
- How many people you employ
- Your key business goals
- Any specific concerns or challenges you're experiencing
- Expected growth



What to expect from a smooth onboarding process

Communication and speed

Clear communication and timeliness are the foundations for a user-friendly onboarding journey.

You shouldn't feel confused or uncertain about what happens next or what details or documentation you need to provide. You also shouldn't be waiting too long for

information about the next step; the bank should be proactive and keen to complete your onboarding. If you feel like you're not getting the clarity you need, contact the onboarding team for updates.

Help from a specialist

Some onboarding processes may seem lengthy, but usually this is important to capture necessary information from you and your business. To alleviate this, some financial institutions will assign a dedicated onboarding specialist to assist in the process. This specialist may have sector expertise and will get to know your business and its needs. A one-on-one relationship with the bank should mean you feel more supported throughout the onboarding journey.

Post-onboarding support

Onboarding doesn't end once you've become a client. You may have further questions, particularly around the product set you've just integrated. Post-onboarding support should be provided by the bank to help you in the short term. As a business banking customer, you may have a dedicated relationship manager, but it's worth asking whether the high-touch service continues beyond the official onboarding process.

Clear roles and responsibilities

Although this might be the first time you've opened a business bank account, your provider has done this many times before. That means they should be clear in defining the tasks you need to complete and what sits with the bank itself. If at any stage you're unsure or feel inclined to ask, the onboarding team should respond quickly.

Transparency on timings

Every business is different and usually onboarding teams accommodate for this. Some banks will provide an estimated turnaround time for the full process. While this is helpful, setting out a timeline before getting to know your business could prove to be a false promise. You should be able to get a better indication of onboarding timings once your bank has established a strong understanding of your business.

Regular contact

As you're going through the onboarding process, you should feel like a valued customer receiving a personalised service from your bank. At a basic level, that means the bank being responsive to your questions and fully engaging with the goal of making your onboarding as efficient and seamless as possible.

Personalisation

Banks shouldn't be taking a one-size-fits-all approach when it comes to onboarding. Your partner should have an eye on the future of your business and how to continually provide a product set that best suits your needs as they evolve. Look for customised solutions, not generic offerings.

Human touch

Sometimes, the quickest way to solve an issue or ask a question is by picking up the phone and going directly to a customer service representative. Automated replies or chatbots can feel like a hurdle rather than an efficient way to solve an issue, particularly if it's a nuanced problem. Banking providers should give you the option of speaking to a human if that's what you prefer.



Post-onboarding: What comes next?

Once onboarding is complete, your bank should inform you of when you will have full access to the products and accounts you've set up.

However, post-onboarding should be about more than product access. A committed banking partner will continue to provide the level of hands-on, specialist service you've received in the onboarding phase throughout your relationship.

That includes offering the practical solutions and expertise you need as your startup grows and your banking needs evolve. We'll look at another specific example of how your bank can deliver crucial support for your business in the next chapter, focusing on fraud risk.



In summary

- Sometimes described as 'the last hurdle', onboarding shouldn't really be a hurdle at all.
- Your bank should be committed to keeping the process running smoothly and updating you at every stage.
- Be inquisitive, ask lots of questions and expect a comprehensive service.

Chapter 5

Managing fraud risk

Even the most digitally savvy startups and founders can fall victim to fraud. With so many jobs to do and so much responsibility on your shoulders, it's all too easy to overlook tasks like fraud protection until it's too late.

For small and growing businesses, fraud can be fatal: it not only damages your finances, but can also harm your reputation.

Thankfully, even first-time business leaders with limited resources and a seemingly endless to-do list can mitigate this threat through careful planning. The key is to be aware and know what to look out for.



The most common types of business fraud

Becoming familiar with the various tactics used by fraudsters can help you anticipate the warning signs and implement preventative measures.

Phishing, vishing and SMShing

These are all types of cyberattacks where fraudsters contact their victims via text (SMShing), email (phishing) or phone (vishing). They pose as someone from a legitimate organisation, sometimes even your own, in an attempt to obtain sensitive data such as banking details, passwords or employee personal data, which they then use to infiltrate your business systems.

Malware

This form of cybercrime involves software designed to compromise or cause damage to computers, systems and other software. There are various types, all with the same intention – to allow criminals to extract data or force companies into a position where they're unable to conduct their business. One of the most prevalent malware threats is ransomware, which attackers use to lock owners out of their systems before demanding payment to restore access.

Baiting

This type of cybercrime involves fraudsters using enticing ads, music or promotions that contain malware. The 'bait' can also be in a physical form, such as media storage or external drives that, when used by individuals, infect their computer with malware.

Scareware

Another type of cyber fraud, scareware involves victims being bombarded with false alarms and fictitious threats, often appearing as pop-ups. Users consequently believe their systems have been infected with malware, prompting them to install software which is itself malware. This enables fraudsters to access sensitive data.

Invoice fraud

This is where a criminal poses as a regular supplier and sends an email asking for their bank account details to be changed. The aim is to trick the victim into sending money to the fraudster's account rather than the genuine supplier. These criminals take time to build up knowledge about their targets, including scanning websites for details of authentic suppliers that they use to make their approach more credible.

Card fraud

Card fraud involves the compromise of any personal information from credit, debit or store cards, as well as the physical theft of a card. Fraudsters use this information to purchase goods in your name or obtain unauthorised funds from an account. Cards can also be abused internally by employees purchasing personal goods using a company card; this is known as internal fraud. Another example is 'card-not-present' fraud, where the perpetrator poses as a known contact to take card payment details over the phone.

Purchase fraud

In this instance, criminals create websites that appear legitimate to trick buyers into purchasing products and services that don't really exist. These websites even have contact details listed to answer queries you may have about your potential order, helping them appear as if they're a legitimate supplier.

CEO fraud

Here, a fraudster impersonates a senior person in the company, instructing a staff member to either make an urgent payment or change payment details for an employee, contract or supplier. These attacks often involve sophisticated techniques such as hacking or spoofing software to access emails and internal systems and steal data. This helps to make the email request appear genuine to the recipient.

Authorised Push Payment (APP) scams

This scam tactic sees criminals attempting to trick the victim into sending them money by posing as a genuine payee. A common warning sign of APP fraud is the perpetrator trying to persuade you to take action quickly.

Protecting your business against fraud

There's no single solution to prevent business fraud, but there are ways you can mitigate these risks and help keep your startup safe. Implementing strong internal controls and procedures is a good starting point, irrespective of the size of your business. Identify areas where you may be vulnerable to fraud and implement clear and transparent policies that align with your business activities, rather than inhibit them. This could include robust background checks of all associates and implementing AI-enhanced cybersecurity measures. Your systems should be monitored and updated regularly to ensure they're effective and reflect emerging threats.

It's also wise to look beyond your organisation and think about your key stakeholders. Consider discussing challenges with trusted peers in your network. This can increase your knowledge of the threats impacting your industry and help others to do the same.

The buck shouldn't stop with you as the founder. Make sure your entire team is aware of these risks and the different types of fraud, instil good avoidance practices and give everyone the tools to respond to risks should they occur.

Your bank can also provide tools to help protect your business from fraud. For example, using dual transaction authorisation in your online banking platforms provides an opportunity to think about the authenticity of the payment request. It reduces the risk of internal fraud, the potential for human error and the threat posed by cybercriminals, who may target your IT equipment to make transactions.

The most important thing to remember is that in the fight against fraud, awareness, coherent policies and strong security practices are some of the strongest weapons in your arsenal.

Fraud protection: A best practice checklist



- Establish and enforce strict data security policies
- Create employee training schemes, particularly to identify fraud warning signs across communications and transaction activity
- Implement multi-factor authentication for transactions and remote working
- Invest in strong cybersecurity measures and keep them updated
- Conduct regular audits of processes to minimise risk where you can
- Implement strong reporting mechanisms, including an internal employee whistleblowing process
- Conduct due diligence on third parties, including background checks, data verification and contract reviews



In summary

- Fraud is a major business threat, but it can be easy to overlook amid the many pressures of running a startup.
- Risk awareness, internal controls and employee education are essential.
- Your bank can help provide safeguards to boost payment security and reduce the risk of fraud or error.

Find out more about

HSBC Innovation Banking



Disclaimer

Any opinions expressed are merely opinions and not facts. All information in this document is for general informational purposes and not to be construed as professional advice or to create a professional relationship and the information is not intended as a substitute for professional advice. Nothing in this document takes into account your company's individual circumstances. HSBC Innovation Banking does not make any representations or warranties with respect to the accuracy, applicability, fitness or completeness of this document and the material may not reflect the most current legal or regulatory developments. HSBC Innovation Banking disclaims all liability in respect to actions taken or not taken based on any or all of the contents in this document to the fullest extent permitted by law. Nothing relating to this material should be construed as a solicitation or offer, or recommendation, to acquire or dispose of any investment or to engage in any other transaction.

© 2025 HSBC Innovation Bank Limited. All rights reserved. HSBC Innovation Bank Limited (trading as HSBC Innovation Banking) is registered in England and Wales at Alphabeta, 14-18 Finsbury Square, London EC2A 1BR, UK (Company Number 12546585). HSBC Innovation Bank Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority (Firm Reference Number 543146). HSBC Innovation Bank Limited is part of the HSBC Group. HSBC Innovation Bank Limited is committed to making its website and related documents accessible to everyone. Learn more on www.hsbcinnovationbanking.com/accessibility

