BizPass

Unlocking Verified Growth

August 2026

STARTUP COALITION

Authors

Charlie Mercer
Policy Director
Startup Coalition

About Startup Coalition

Startup Coalition, formerly the Coalition for a Digital Economy (Coadec), is an independent advocacy group that serves as the policy voice for Britain's technology-led startups and scaleups. Startup Coalition was founded in 2010 by Mike Butcher, former Editor-at-Large of technology news publisher TechCrunch, and Jeff Lynn, Chairman and Co-Founder of online investment platform Seedrs. Startup Coalition works across a broad range of policy areas that matter the most to startups and scaleups: access to talent, access to finance & regulation.

Polling Acknowledgment

On behalf of Startup Coalition, Stack Data Strategy conducted an online survey of 501 senior business leaders in the United Kingdom. Fieldwork was conducted between the 2nd-6th of July 2026. Quotas were used to ensure balanced representation of businesses by region and size. All results are unweighted, and, due to rounding, estimates may not always add up to 100%.

Executive Summary

Britain's businesses spend eleven million hours a year proving they are who they say they are, and almost none of that effort is ever reused.

Startup Coalition commissioned Stack Data Strategy to poll 501 senior business leaders on how they share information, verify themselves, and would respond to a Business Digital Identity. The picture inverts the one we found among consumers in our 2025 report Licence to Share. Consumers share their data because it gets them something: a better deal, a faster service. Businesses share because they have to. The most common reason a business hands over its information is legal or regulatory obligation (55%); getting a better deal trails at 24%. A consumer shares for a reward; a business shares to avoid a penalty.

That obligation is constant. 84% verified their identity or provided registration details to an external organisation in the past year, a quarter of them six times or more, and 43% repeated a check they have effectively already completed at least monthly. At roughly six checks a year and twenty minutes a check, that is more than 11 million hours across Britain's 5.6 million businesses: the equivalent of more than six thousand people working full-time on nothing but proving that businesses are who they say they are.

The state verifies well and remembers nothing. 74% find it easy to prove who they are to any single government service; only 48% find it easy to get one government body to recognise a verification already completed elsewhere. The most widespread consequence is duplication inside government itself: 30% have handed identical information to more than one department separately. Three in five have suffered a concrete harm on top of it, including bank accounts delayed (17%), errors from manual re-entry (15%), suppliers or customers not onboarded (13%) and finance delayed (12%).

Only 37% say their business spends too much time proving who it is. We report that honestly, because it is the key to the problem rather than an exception to it. Each check is quick enough that nobody names it as a grievance; it is the accumulation of six, ten or fifty checks, none of which can see the others, that produces the delayed accounts and the lost contracts.

Businesses want this fixed, and want it built a particular way. 57% support our business digital identity concept against 17% opposed; 68% would use one; 82% say verifying once and reusing that verification would be valuable. Support concentrates where the burden falls: adoption intent runs at 85% among firms with 11-49 employees against 52% among sole traders. This is a growth policy in the strictest sense, because the pain rises as a firm grows. The conditions attached are about control rather than convenience: strong security (51%), clear rules on access (49%), control over what is shared and with whom (45%) and a government-backed trust mark (44%) all outrank any promised benefit such as faster service or less admin (38%).

We call our answer BizPass: one identifier, with two on-ramps for the two halves of the business population.

This is not a personal digital ID, and businesses draw the line themselves: they are three times more likely to say they are more comfortable sharing business data than personal data (25%) than the reverse (8%). There is no privacy case against a company reusing verification of facts already on a public

register. For companies, the Companies House number becomes the authoritative anchor of a BizPass. It is already unique, already public, and once ECCTA's verification programme completes it will be backed by a freshly verified record of the individuals holding statutory roles in that company. What ECCTA does not produce is a record of who may act for a business, in what capacity, and how that permission is granted and withdrawn. That authority layer is the one genuinely new thing this report asks the state to build. It is not a permissions database: the systems furthest ahead, Singapore's Corppass and Australia's Relationship Authorisation Manager, make the root authoritative and let delegation cascade from it under the business's own administration.

For sole traders, partnerships and other unincorporated businesses, BizPass is anchored instead to a GOV.UK One Login-verified personal identity, without a UTR or National Insurance number ever appearing in a business credential. Two on-ramps, one destination: when a business incorporates the BizPass persists rather than resetting at the precise moment a firm is trying to grow.

A credential nobody is required to accept is a filing cabinet, not infrastructure. The government should regulate for its own use so that tax filings, licensing, grants, procurement and regulatory returns run on one credential. No business would be required to hold a BizPass; departments would be required to accept one. Alongside it, a Business Data Smart Data scheme designated under the Data (Use and Access) Act 2025 would let businesses consent to their own state-held records flowing to third parties of their choosing, with an enrichment market built by the accountants, banks and software providers businesses already trust most.

Six to seven million directors and persons with significant control are verifying their identity with Companies House this year, in the largest identity assurance exercise the British state has ever asked of its business population. Committing now that this effort will yield a reusable credential turns a compliance cost into an investment while businesses are still paying it. Committing in 2027 asks them to feel differently about a cost already sunk. The second deadline is not ours. Regulated European acceptance of legal-person wallets begins in December 2027, and 9% of British businesses have already been unable to trade overseas because of verification friction. Business identity is becoming trade infrastructure, and absence from it is a non-tariff barrier of our own making.

Our blueprint runs to ten recommendations across three phases. Four can start now, and none requires new primary legislation:

1. **Declare BizPass:** commit publicly that the ECCTA verifications now under way will yield a reusable credential.
2. **Name the accountable owner:** so the programme has somewhere to live from day one.
3. **Issue the credential to verified companies:** with a lookup that lets a counterparty check a BizPass is live and genuine.
4. **Commence the information gateway and draft it for organisations now.** Section 45 of the Data (Use and Access) Act 2025 awaits approval of its Code of Practice. Approve it, and write both the Code and the trust framework so they anticipate organisational attributes before the power to carry them exists.

Each is a precondition for the authority layer, universal coverage and the Smart Data scheme that follow.

BizPass is the Government's ticket to verified growth.

Introduction: Why we care

Startup Coalition believes that data makes the world go round, and, put to work, drives forward economic growth. To this end, we are deeply involved in the UK's data policy landscape:

- We sit on the Government's Smart Data Council, supporting the Department for Business, Innovation, Science and Trade (DBIST) chart a course to deliver its Smart Data Strategy.[1]
- We co-chair the National Data Library initiative, led by the Department for Digital, Culture, Media and Sport.[2]
- We sit on the FCA's PRISM taskforce.[3]

Most policy work in this space around data access, portability, interoperability and security centres on the consumer. Businesses are an afterthought, if given any thought at all. This is, to an understandable degree, the necessary consequence of policymakers in the UK focusing on the electorate, on the "doorstep" offering. However, neglecting businesses in these policy discussions risks missing the bigger economic opportunities resulting from improving access to and interoperability of data in the UK. An average business that is able to enhance a product and service, function more efficiently, or innovate as a consequence of putting data to work can have a far greater impact on the economy in the short term than an average individual.

Beyond the electoral offer, another core reason that Startup Coalition believes businesses have been neglected in conversations around data access is because of the lack of a clear entry point. The absence of definitive, efficient, and accessible means to verify a business is who it says it is. Consequently, connecting or accessing datasets from providers they interact with has for too long been put in the 'too hard' bucket of policymaking.

As always, when approaching a policy challenge, Startup Coalition begins with the evidence. First and foremost we ask our ecosystem, and many of them frequently regale us with stories of frictionful interactions with the state. Take applying for grants funded by UKRI, for example, a critical part of many startup founders' journey: applications must start from scratch every time. Beyond the anecdotal, however, we wanted to consult a broader range of businesses, and chose to commission polling from Stack to understand the views of 500 British businesses. We took a similar approach when building our agenda to support individuals as part of our Licence to Share report in 2025, yielding fascinating insights that underpin our advocacy today.[4]

Only through asking businesses themselves can we design reliable and resilient policies to support their growth and ambition.

---

[1] https://www.gov.uk/government/publications/smart-data-strategy#:~:text=The%20UK's%20Smart%20Data%202035,including%20artificial%20intelligence%20(AI).

[2] https://www.data.gov.uk/

[3] https://events.fcainnovation.co.uk/PRISM_Taskforce

[4] https://startupcoalition.io/u/2025/12/Startup-Coalition_License-to-Share_FOR-RELEASE.pdf

Groundhog Day: How Businesses Share Data

When we asked consumers about data sharing in Licence to Share last year, the consumer story was one of choice: three-quarters of the public share data at least sometimes, overwhelmingly because doing so gets them something: a better deal, a faster service, a personalised product.

When we asked businesses the same family of questions, the story inverted.

The single most common reason a business shares its information is that it is legally or regulatorily obliged to (55%), followed by to access finance, banking or credit (45%) and then because a service, supplier or customer requires it (43%). Getting better deals, terms or pricing (the consumer's headline motive) trails at 24%. A consumer shares for a better deal; a business shares to avoid a penalty.

84% of businesses verified their identity or provided registration details to an external organisation in the past twelve months; nearly one in four (25%) did so six or more times, and one in nine did so eleven or more times. The organisations demanding it are everywhere: 68% regularly share business information with HMRC or Companies House, 54% with banks or lenders, 52% with accountants, 50% with accounting software providers, 45% with insurers, 30% with regulators, and a long tail runs through energy suppliers (27%), online marketplaces (23%), social media firms (21%) and even AI chatbots (17%).

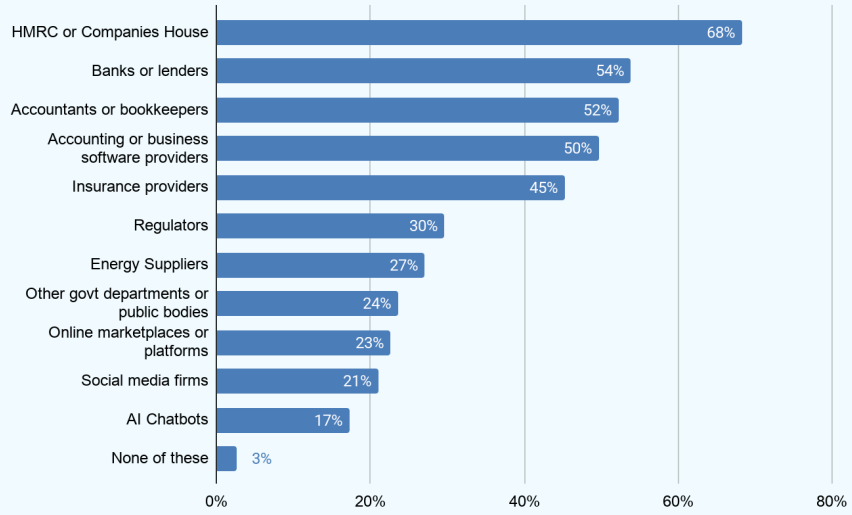


Figure 1, Which of the following does your business regularly provide or share business information with? Please select all that apply

Easy to prove, hard to reuse

Proving a business's identity to any single government service is not the problem: 74% find it easy, and 72% find a single government login easy to use. A decade of digital government has worked, one

interaction at a time. But the numbers fall as soon as reuse enters the picture: only 51% find it easy to avoid re-entering the same details across different government services, and asked about getting one government body to recognise verification they have already completed elsewhere, the number drops to 48%, with 23% finding it outright difficult. The system verifies well but remembers nothing.

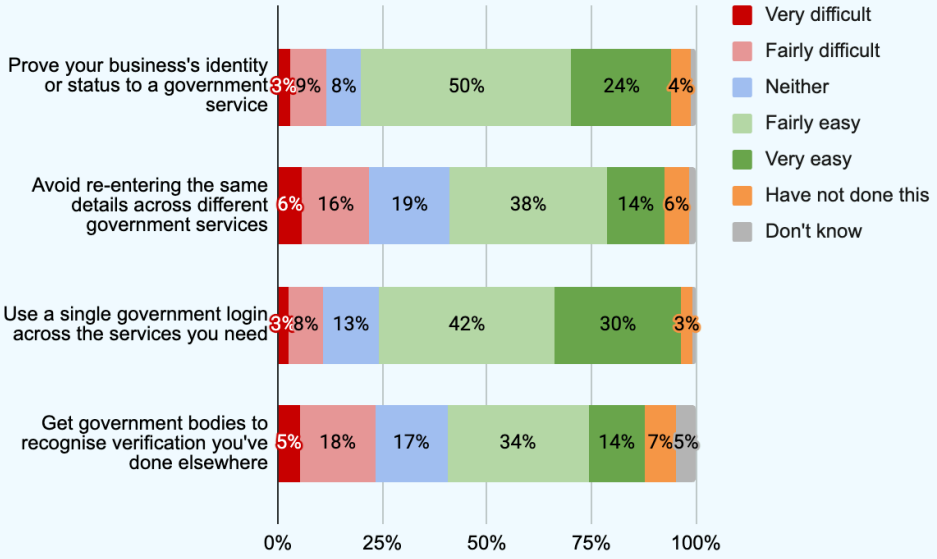


Figure 2, Thinking specifically about dealing with government and public bodies, how easy or difficult is it for your business to do each of the following?

The behavioural data shows what living inside that gap looks like. 43% of businesses repeat an identity check they have effectively already completed at least monthly, including 4% at least daily, 21% at least weekly, whilst 73% repeat a check at least a few times a year. Every one of those repetitions is founder or director time spent re-keying facts that have often already been verified elsewhere: the company number, the registered address, the directors' names, the VAT status.

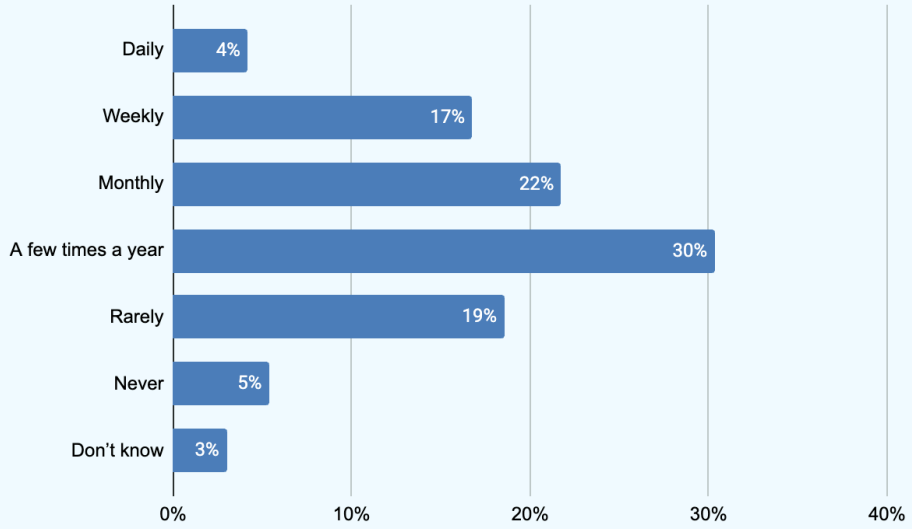


Figure 3, How often does your business have to repeat an identity or verification check it has effectively already completed elsewhere?

Even worse, scratching the surface through our conversations it is clear that reuse is also not often baked in but bolted on by the user in a myriad of insecure ways. In conversations with small business owners that we held in the build up to launching this report, we heard about passwords stuck on office kitchen fridges, shared in whatsapp group chats or posted between colleagues on slack or team channels.

Eleven million hours

The average business verified its identity roughly six times in the past year, and the average check takes roughly twenty minutes: two in five businesses report ten to thirty minutes or longer per check, and one in eight report over half an hour. Multiplied together, that is around two hours per business per year spent purely on identity verification.

Across Britain's 5.6 million businesses, more than 11 million hours a year: the equivalent of more than six thousand people working full-time on nothing but proving that businesses are who they say they are.[5]

One accountant we spoke to said it was “the waiting that killed you”. For example, you might request a HMRC code but then have to wait seven days before receipt delaying the onboarding of a new client from the get go and violating customer service expectations.

The cost of the treadmill

Repetition may be tolerable if it were merely annoying, but it is much worse than that. The most widespread consequence is the plainest: 30% of businesses have handed the same information to more than one government department separately. Three in five have gone further and experienced at least one concrete harm as a result of repeatedly proving who they are.

- 17% have had the opening or switching of a business bank account delayed;
- 15% have made errors through manual re-entry;
- 13% have been unable to onboard a new supplier or customer;
- 12% have had access to finance delayed;
- 10% have been unable to bid for or win a contract;
- 9% have been unable to trade with a business overseas;
- 8% have been unable to sell through an online marketplace.

That duplication is a government-side failure of reuse, squarely within the state's own gift to fix, and it is why this report's first recommendations require no new legislation at all. The finance and banking delays land on precisely the interactions where the UK's scaleup economy is most sensitive: a firm that cannot open an account or draw down finance on time is a firm whose growth is being rationed by paperwork.

[5] We assume every business sits at the very bottom of its reported band on both questions, and assume those who could not recall spent no time at all. The floor is still 5 million hours a year, around 2,800 people working full-time on nothing else. Our full arithmetic, including the band distributions, is set out in the methodology, and every version of this counts only the direct time of the check itself, none of the waiting, chasing or downstream delay the next section describes.

What businesses didn’t (need to) say

We report our data honestly, including where it complicates the story. Asked directly whether their business “spends too much time proving who it is”, only 37% agree, 36% disagree and 26% are neutral. Asked to compare proving their business's identity with proving their own, most businesses say it is about the same (48%) or actually easier for the business (32%). At first sight those findings sit oddly beside the 59% who have suffered concrete harms and the 43% repeating checks monthly. We think the explanation is familiar from every other corner of red-tape research: businesses experience the harms vividly but have normalised the cause.

Each individual check is quick and painless enough that nobody names it as a grievance; it is the accumulation of six, ten or fifty painless checks, none of which talks to the others, that produces the bank-account delays and lost contracts businesses report in such numbers. Nobody complains about a tax they do not know they are paying.

Speaking to those at the sharp-end the impact of the cumulative effect becomes clearer. Business hours wasted on low value work, taking away from higher-value strategic work that could move the needle for the business. This matters when you consider the landscape: the typical accounting firm, serving our startups and the broader business community, is either a micro or small business, employing fewer than 10 people. The vast majority (upwards of 85%) of the 35,500 accountancy practices nationwide sit in this category. Filling the 24 hours in their day with low value, but, as the system operates today, necessary work, strangles their opportunities for growth and development. Not only are they unable to serve businesses in the way they would want, they are able to dedicate less time to growing their businesses.

Insult to injury

Nearly one in ten businesses (9%) say they have been impersonated or had false information filed about them: a fake director added, a fraudulent filing made, an account opened in the business's name. This is a harm in its own right, and it is the bridge to this report's central argument: government's own answer to business identity fraud, the Companies House verification programme under the Economic Crime and Corporate Transparency Act (ECCTA), is exactly the investment that makes a reusable Business Digital Identity possible. The state is building the answer to fraud but it has not yet decided to let businesses use it for anything else.

How businesses feel about data

If the first section of this report establishes that something should be built to fix the problem of verifying business identity, this chapter explores how. Responses to our polling gave us a map, with gradients of comfort and trust that any credible solution must respect.

Comfort is tiered, and the tiers are rational

Asked how comfortable they would be sharing specific categories of business information through a secure digital system, businesses drew a clear line between the public and the private. The registered business address tops the table (75% comfortable), followed by the company registration number and legal status (68%), VAT registration status (68%) and the names of directors or owners (68%). These are the facts that already sit on a public register. Trading history (65%) and even tax compliance status (64%) remain solidly in positive territory. The floor is summary financial accounts, at 44% comfortable and 34% uncomfortable, the one category where discomfort comes close to comfort. The design lesson is that sensitivity tiers are real and rational: businesses are relaxed about the scheme carrying what is already public, cautiously open on compliance status, and guarded about the numbers.

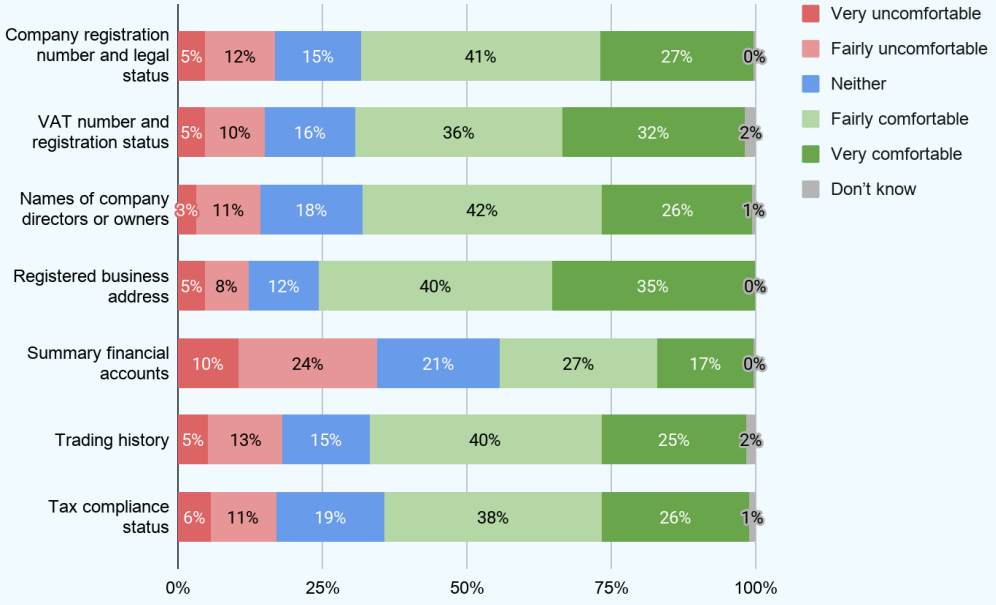


Figure 4, Thinking about your business information (not your personal data), how comfortable would you be sharing each of the following digitally with another organisation?

The trust gradient

Asked how much they trust different organisations to use their business data responsibly, businesses put their professional advisers first, 63% trust accountants and bookkeepers a lot or completely, with HMRC

and Companies House the most trusted institutions at 54%, ahead of accounting software providers (52%), banks and lenders (50%), regulators (47%) and insurers (44%).

Importantly, trust in government is specific, not general: HMRC and Companies House (54%) comfortably outscore “other government departments and public bodies” (41%). Businesses trust the registrar and the tax authority they deal with, not Whitehall in the abstract.

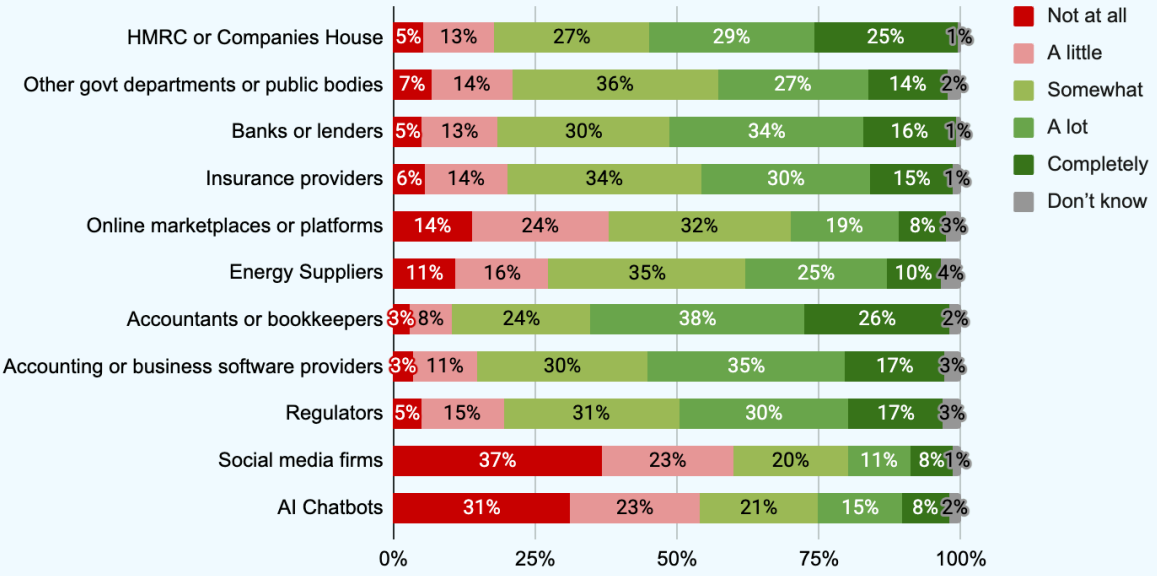


Figure 5, How much do you trust the following types of organisations to use your business data responsibly?

Control, and the absence of it

35% of businesses feel they have little or no control over how their data is used by other organisations once shared. Control is the currency in which Government intervention to support the flow of data in the economy will be judged. Control-related conditions, like clear rules on who can access data (49%) and control over exactly what is shared and with whom (45%), rank among businesses' top preconditions for participating in any data-connection scheme, above any promised convenience benefit.

Business data is not personal data, and businesses know it

Asked which statement comes closest to their view, businesses are three times more likely to say they are more comfortable sharing their business data than their personal data (25%) than the reverse (8%), with 42% equally comfortable with both. This finding matters politically as much as analytically. The UK has just had a bruising national argument about personal digital identity, culminating in Andy Burnham abandoning the policy entirely in one of his first acts as Prime Minister.[6]

A Business Digital Identity is a different object in kind: companies are public, statutorily-disclosed legal entities whose directors, addresses and accounts are already published by the state at Companies House, and businesses' own instincts, on this evidence, already draw the distinction. There is no privacy case against a company being able to reuse verification of facts already on a public register.

[6] https://www.bbc.co.uk/news/articles/c5y08z25q8eo

Businesses demand BizPass

Support and intent

Shown a neutral description of a Business Digital Identity (explicitly a credential for the business, not the individual, and explicitly separate from any personal digital ID) 57% of business leaders support its introduction against 17% opposed: better than three to one, with only 8% strongly opposed. 68% say their business would be likely to use one, with 22% very likely, 46% fairly likely, against 24% unlikely.

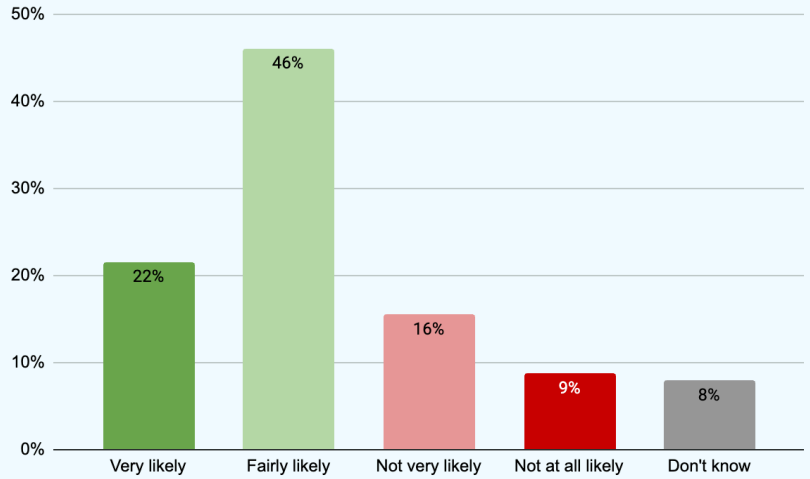


Figure 6, If a Business Digital Identity were available, how likely would your business be to use it?

For a piece of infrastructure that did not exist when respondents opened the survey, that is a remarkable number, and it is reinforced from three directions: 82% say verifying once and reusing that verification across services would be valuable (28% very valuable); 66% believe a single verification system spanning government and the private sector is realistic for the UK to build (only 9% say not at all); and 69% see value in connecting datasets beyond identity itself. Weighing it all in the round, businesses judge that the benefits would outweigh the risks by 41% to 19%, two to one, with 36% calling it even.

In the conversations we had with small business owners to build the picture that sits behind the numbers, it was clear that for many, mandatory business identity would even be tolerated. Those familiar with making tax digital, for example, were aware of how painfully slow and protracted a process could be. Mandation supports faster and higher adoption helping everyone get on to a levelling the playing field, and fast.

Where the appetite lives

The demand concentrates exactly where the burden does. Adoption intent runs at 76% among limited companies against 52% among sole traders, and climbs to 85% among firms with 11-49 employees, holding at 78% for firms of 50-99 and 76% for 101-249. Businesses with no employees beyond the owner sit at 54%. Support follows the same curve: 64% among limited companies and 71% among 11-49 employee firms, against 41% among sole traders. The repeat-verification burden maps onto it precisely: 45% of limited companies repeat checks monthly or more against 23% of sole traders, rising through the employee bands from 55% to 65% to 69%.

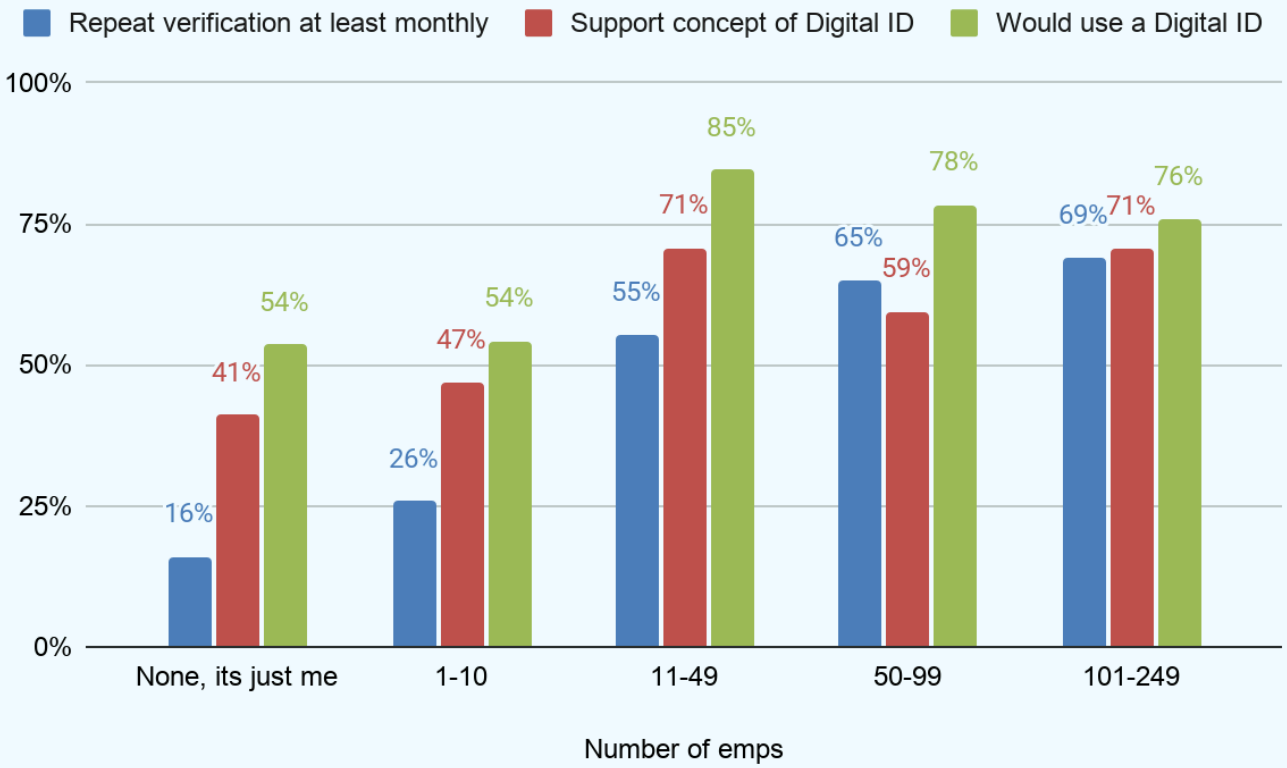


Figure 7, Share of Businesses that Verify ID at least monthly, support Digital ID concept, and would use Digital ID, split by number of employees.

Fixing digital verification of business identity is a growth policy in the strictest sense: the pain rises exactly as a firm grows and a business digital identity would remove friction at precisely the margin where expansion happens. Meanwhile, the sole trader numbers are the softest in the dataset, and we do not hide it: sole traders are less burdened (their business is, legally, themselves, so personal identity infrastructure already part-serves them) and correspondingly more lukewarm to the concept of business digital identity. That is not an argument for excluding them, however, because our polling shows that this is a pain point waiting on their growth horizon. This finding validates what CFIT also found in their work on business digital identity.[7]

Benefits sought, concerns held

The perceived benefits of a business digital identity selected by respondents to our polling were strikingly practical. Easier compliance with government reporting requirements (34%) and reduced fraud and financial crime risk (34%) narrowly lead time saved on paperwork (33%), with protection against impersonation (27%), fewer re-entry errors (24%), faster access to finance (22%) and easier proof of track record when bidding for work (21%) behind. Businesses see this as compliance-and-security infrastructure at least as much as convenience, which is exactly how it should be built and sold.

[7] https://cfit.org.uk/wp-content/uploads/2026/02/CFIT-Blueprint-Report-March-2025-Revised2026.pdf

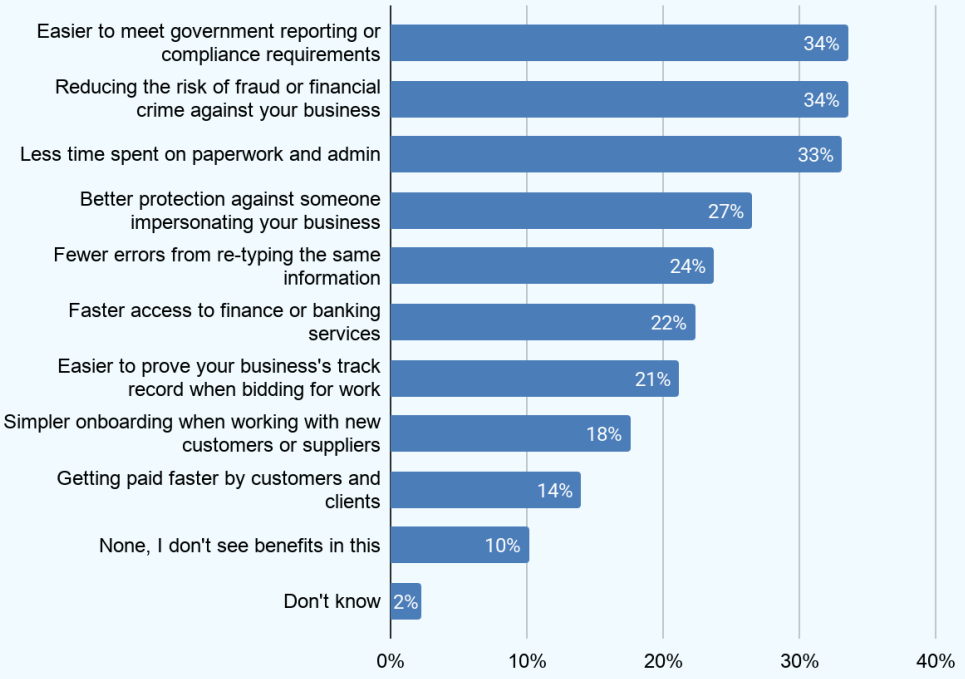


Figure 8, What would you see as the main benefits of a system that lets your business share verified information digitally, rather than re-submitting it each time? Please select up to three

The concerns were just as instructive: data breaches and cyber attacks (46%), information shared without consent (35%), losing control over who sees business information (30%), government using the system to monitor business activity (29%), the cost of adopting new systems (24%), distrust of whoever runs it (24%), smaller businesses being disadvantaged (23%) and doubts about data accuracy (21%). Only 7% of businesses reported no concerns at all. These concerns will be critical to mitigate in the design of the solution.

What have others proposed

Nobody arriving at business identity in 2026 is starting with a blank slate. In the past eighteen months, three serious pieces of work have converged on a version of the same conclusion: that Britain's businesses need a single, reusable way to prove who they are. We agree with that conclusion. Where we differ, and it is a practical difference, not a rhetorical one, is on the one question none of the three has actually answered: how do you mint an identifier that covers every business in the country, including the millions that aren't companies at all?

The Master Key: Xero, Enterprise Nation and The Entrepreneurs Network[8]

Master Key is the most ambitious of the three and the closest in spirit to this report, and it deserves specific credit for one contribution above the rest. Before Master Key, the UK debate on business identity was a debate about entities: how to know that a company exists and that its filings are accurate. Master Key correctly diagnoses the core problem: a business today is not one thing to the government, but many. There is a Companies House number here, a VAT number there, a Unique Taxpayer Reference somewhere else, and nothing joins them up. Its proposed fix is a Unique Business Identifier: not a new number, but a federated index that links a business's existing identifiers together behind a single reference, held in a digital wallet and built on GOV.UK One Login.

Master Key was also the first to state plainly, and in language a founder could act on, that the harder and more valuable question is authority, including who may act for a business, in what capacity, and how that permission is granted and withdrawn. Everything this report says about a role-and-delegation layer descends from that framing. Master Key proposes “Guest Passes”, time-limited, role-specific delegation, so an owner can let an accountant file a return or a bookkeeper view transactions without handing over a password. Master Key deserves real credit for putting a delegation model on the table in plain language, and for anchoring its case to two live legislative hooks, mandatory eInvoicing from 2029 and the Electronic Trade Documents Act, that give the proposal a practical, near-term reason to exist.

Where federation reaches its limit is the unincorporated economy, and the difficulty arrives in two stages. The first is confidentiality. Some of the identifiers Master Key proposes to link are confidential by design: a Unique Taxpayer Reference exists precisely so that it is not shared casually, because it can be used to impersonate a taxpayer. Federating such an identifier into a business credential either strips it out, removing the very link that makes the federation work, or carries it, and creates a new fraud surface the moment the credential is presented. The Master Key report leaves open how confidential identifiers are protected once federated, and we think that question has to be answered before a federated index can safely reach the whole business population.

The second is coverage. A sole trader has no Companies House number to federate around, because legally their business is themselves: their business identifiers are their personal ones, a UTR or a National Insurance number. Linking existing identifiers together works well for a company that has several to link. It has nothing to work with for the more than 3.5 million sole traders and other

8 https://a.storyblok.com/f/102007/x/2e6f1cd5a7/the-master-key-xero-enterprise-nation-the-entrepreneurs-network.pdf

unincorporated businesses in the country. Master Key set the destination and rightly insisted that sole traders must be included; this report proposes the mechanism for reaching them.

CFIT's Digital Company ID[9]

The Centre for Finance, Innovation and Technology's (CFIT) blueprint is the most architecturally developed of the three, and it is honest about its own scope: this is a company ID, not a business one. Its design has three layers: verified attributes drawn from the register, the personal identity of the people involved, and a "mandate" layer recording who is authorised to act for the company. This is, in essence, the right shape for a credential. The gap is in how that third layer, the mandate, gets established: CFIT left it to self-attestation by the company itself, rather than an authoritative record anchored to something the government already verifies, as the coalition convened before the ECCTA's work. Importantly, the advent of Companies House Director ID verification gives the business owner the opportunity to re-use their verified credentials.

The City of London Corporation's Digital Verification Orchestrator initiative[10]

The DVO is a different kind of document altogether, not a credential proposal but a piece of plumbing. It sets out a neutral routing layer that lets verified information move between organisations on a business's instruction: not a data store, not an assessor of whether an attribute is accurate, and explicitly not a regulator. Its own blueprint states that it complements CFIT's work by handling the exchange of verified attributes, and gives the exchange of Digital Company IDs as its example of what flows through the pipe. The City of London Corporation is already treating a business identity credential as existing cargo to be routed, without itself creating one. The DVO answers a real question: how do verified facts move between counterparties safely? But it presupposes the very credential this report, Master Key and CFIT are all, in different ways, trying to build.

What the three share, and what none of them has settled

Read together, these three documents describe a field that has already converged on the destination without agreeing the route. All three assume, explicitly or implicitly, that businesses need a single verified identity they can reuse rather than re-proving from scratch with every counterparty. None of the three has specified a workable mechanism for minting that identity for the whole business population: Master Key's federation model does not extend to confidential identifiers or sole traders; CFIT's mandate layer rests on self-attestation rather than an authoritative source; and the DVO assumes the credential is already solved elsewhere. This report exists to close exactly that gap.

[9] https://cfit.org.uk/wp-content/uploads/2026/02/CFIT-Blueprint-Report-March-2025-Revised2026.pdf
[10] https://www.theglobalcity.uk/PositiveWebsite/media/Research-reports/DVO-Blueprint.pdf

Our position

A universal identifier, minted rather than federated

We share Master Key's ambition without reservation: this has to work for every business in the country, sole traders included, or it is not a national identity system at all, it is a company registry with a new name. Where we differ is the mechanism. A federated index of existing identifiers cannot cover sole traders and creates a privacy exposure wherever it touches confidential ones. The alternative, proven in every international comparator from Australia's ABN to New Zealand's NZBN, is to mint a single new identifier and anchor everything else to it, rather than trying to stitch old ones together after the fact. We propose two routes into that single identifier, one for each half of the business population that currently has no route at all.

We call this identifier BizPass.

Route one: evolve the Companies House number into BizPass

For the companies on the Companies House register, the anchor already exists and does not need inventing. The Companies House number is already unique and already public. The practical proposal is to evolve this number in place: the same identifier, the same register, now expressed as a verifiable credential, a BizPass, that the company can present and reuse rather than re-prove. This is deliberately the smallest possible design decision. Nothing is replaced and nothing new is invented. The number a company has always had becomes something it can finally use. Our polling suggests businesses will meet it where it starts: comfort is highest for exactly the attributes this credential would carry: registered address (75%), registration number and legal status (68%), directors' names (67%).

Route two: sole traders, verified through One Login into a BizPass of their own

The harder half of the population is the more than three million sole traders and unincorporated businesses who have no Companies House number to evolve, because they are not required to have one: legally, a sole trader's business is, simply, them. This is precisely where Master Key's federation model runs out of road, because there is no register entry to federate around. Our proposal is to solve it from the personal side rather than the corporate one.

GOV.UK One Login already exists as the government's personal identity service. A sole trader who verifies their personal identity through One Login, to the same evidential standard already required of company directors under ECCTA, should be able to register a trading identity against that verified personal record and be issued a BizPass of their own: a business-facing credential, distinct from and never exposing their personal identifiers, but anchored to a One Login verification that government already trusts.

This gives sole traders exactly what companies get from Companies House: a minted, authoritative anchor, without a UTR or National Insurance number ever appearing in a business credential. It is, in effect, a Companies-House-equivalent for the unincorporated economy. The privacy logic runs with the grain of business instinct: businesses are three times more comfortable sharing business data than

personal data (25% versus 8%), and the sole trader route is designed to ensure they can distinguish between the two.

Put the two routes together and the coverage question Master Key rightly asks is answered without weakening either the confidentiality or the authority case: every company gets a BizPass by evolving a number it already holds; every sole trader gets one by verifying an identity the government already has the means to check. Two on-ramps, one destination, one minted identifier, for all 5.6 million British businesses.

Partnerships complicate the picture, because no single person is obviously the anchor, and they are the case CFIT's design excludes by name. Our answer follows from the authority layer rather than requiring anything new. One partner verifies through One Login and registers the partnership's trading identity, and the BizPass is issued to the partnership rather than to that individual. The remaining partners are bound to it through the authority layer (see below), each verified to the same standard, each holding visible permissions, and any of them capable of holding the right to revoke another's. The anchoring partner is the route in, not the owner: their departure changes the authority record, not the identifier.

This is the same structure that governs a company, where directors are bound to an entity that outlives any of them, and it is why the authority layer has to be built for the unincorporated economy at the same time as the incorporated one rather than extended to it afterwards. Limited liability partnerships and Scottish limited partnerships are already on the Companies House register and take Route One unchanged.

Crossing the lanes

Two on-ramps do not mean two destinations. A sole trader issued a BizPass who later incorporates should not be issued a second one. The BizPass should persist; what changes is the record beneath it. On incorporation, the new Companies House number should be bound to the existing BizPass as its authoritative anchor. The credential must make the change of legal personality explicit: a counterparty needs to see that they are now contracting with a limited company, and from when. But the identifier (and everything that hangs off it if it evolves as we predict…) should not have to be rebuilt.

This is where the cost of the current system bites hardest. Incorporation is the moment a founder is most likely to be raising, hiring and onboarding new counterparties, and it is precisely the moment the state currently makes them start their verification history from zero.

Who may act

Minting an identifier answers the first question a counterparty asks: does this entity exist, and is it what it claims to be? It does not answer the second, which is the one that actually holds up bank onboarding, procurement and grant applications: is the person in front of me entitled to act for it, and for what? Master Key was the first to put this question in language a founder could act on, and we adopt that framing whole. What the UK lacks is not a way to describe delegation but an authoritative place to record it.

We propose that the record sits at the register: which verified individuals may act for which entity, and in what capacity, with defined, revocable, role-based permissions. A director may hold full authority; a finance manager authority to open accounts but not to file; an accountant authority to submit returns and

nothing else. The delegation model here is Master Key's Guest Passes, and we adopt the concept whole. Our addition is a claim about provenance rather than design.

It is worth being precise about what ECCTA does and does not deliver, because that distinction is the whole of our ask. ECCTA verifies the identity of natural persons and binds them to a company record in statutory roles: director, person with significant control, authorised filer. That is a substantial achievement and it is the foundation everything here depends on. What it does not create is a mandate. Nothing in the ECCTA record says that a bookkeeper may submit a VAT return but not change the registered office, or that an authority granted in March expires in September.

That gap is why CFIT's blueprint leaves the mandate layer to self-attestation. It is not a flaw in their design so much as a consequence of there being no authoritative source to point at. A company can say who its authorised signatories are; nothing today confirms that assertion against a record the state constitutes.

And authority over a registered company is a fact the state constitutes. It is created by incorporation, changed by filing, and extinguished by dissolution. The record of who holds it can therefore only be made authoritative by the body that constitutes it. This is the layer only the state can constitute, and it is the one genuinely new thing this report asks it to build.

The UK is not starting from nothing. HMRC's agent authorisation regime already binds accountants to their clients with defined scopes, at very considerable scale, and ECCTA has just created a verified class of authorised corporate service providers entitled to file on a company's behalf. What the UK has is several partial authority records, each stopping at the boundary of the department that built it, none of them portable to a bank, a marketplace, or another department.

What the systems furthest ahead have is one. Singapore's Corppass and Australia's Relationship Authorisation Manager work the same way: the state establishes the root, an individual verified against registry data as entitled to act for the entity, and delegation cascades from that verified root under the entity's own administration. Neither government records every permission, and neither should. Both make the root authoritative, which is precisely what self-attestation cannot do, and precisely why a mandate layer a company asserts for itself will not carry the weight a bank or a procurement team needs to put on it.

The stack

It is worth being explicit about the architecture, because most confusion in this debate comes from collapsing distinct layers into a single "digital ID".

1. The authority layer is the record of which verified individuals may act for which entity, and in what capacity. This is the layer only the state can constitute, and the one this report asks it to build.
2. The credential layer is BizPass itself: the entity's verified attributes and its role-and-delegation record, expressed as a presentable, revocable credential.
3. The orchestration layer routes verified information between holders and relying parties on the business's instruction. It is neutral: not a data store, not an assessor of whether an attribute is true, not a regulator. The City of London Corporation's Digital Verification Orchestrator is an example of this.

4. The market layer is everything businesses actually touch: the accountants, banks, software providers and corporate identity services that consume authoritative credentials, enrich them, and build propositions on top.

This report is a proposal about the first two layers. It is deliberately not a proposal about the third and fourth, though below we discuss what the role of the Government *could* be in bringing BizPass to life, alongside the critical role of the private sector.

What we are not asking for yet

Master Key pointed towards a public directory, holding up Australia's ABN Lookup as a model, and the destination is right: an identity a counterparty can look up is worth more than one its holder can only present. We endorse the outcome but believe that it represents an evolution of the product rather than part of the MVP. A public directory of sole traders is, unavoidably, a directory of people, as their business is legally themselves, and this report's case rests on this distinction holding firm. Publishing that index before the privacy design is settled would put the strongest argument for BizPass at risk to deliver a benefit we can get most of another way first.

The staging post is a verification lookup rather than a browsable register: a counterparty presented with a BizPass can check that it is live, genuine and currently held through reference back to the BizPass issuer, without an index of names and trading addresses existing to be scraped.

How to make it happen, and what to do with it: the second half of this report

A universal identifier that exists only as a handful of attributes, and that nobody is required to use, is a filing cabinet, not infrastructure. This is, in the end, the quiet failure mode shared by every proposal reviewed in this chapter. The second half of this report is therefore not about how BizPass is minted but about what makes it matter.

Firstly, this means minting the core identity, as set out above.

Secondly, this involves setting out, from the start, how BizPass will be experienced in the market, and, critically, the role of the private sector in delivering the real value that infrastructure makes possible.

Thirdly, this involves setting out the means through which these core attributes minted on conception at Companies House or with GOV.UK One Login can be enriched, eventually to include every interaction that a business has with the state through a Smart Data scheme.

And fourth, this involves a regulated requirement that interactions between businesses and the state, tax filings, licensing, grants, procurement, regulatory returns, run through BizPass as the standard means of verifying who is dealing with the government, rather than as one option among several. This is what turns a credential into a rail, and it targets the single largest harm in our polling directly: the 30% of businesses handing identical information to multiple government departments separately.

How to do it

What businesses told us to build

The demand for the core function is close to unanimous by polling standards: 82% say it would be valuable to verify once and reuse that verification across services. 69% see value in going further and connecting other datasets to a verified identity, and businesses ranked what they would connect: HMRC and Companies House records lead at 61%, followed by banks (48%), accountants (42%), accounting software providers (41%), regulators (40%) and insurers (39%), with marketplaces (13%), social media (11%) and AI tools (10%) far behind.

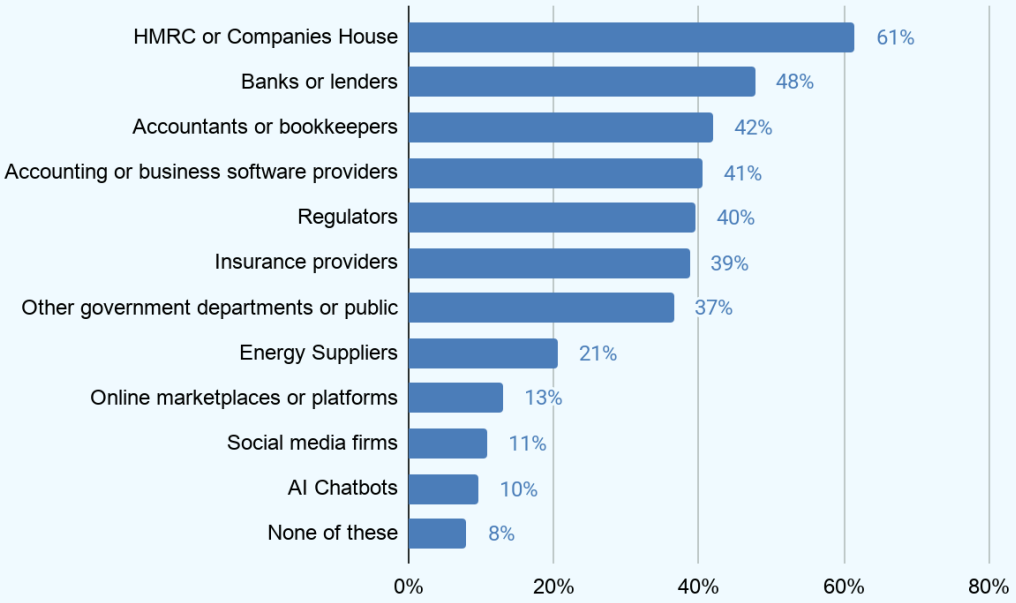


Figure 9, Of the following providers who hold data on you, which would be valuable to be able to connect to your Business Digital Identity? Please select all that apply

The conditions for trust are the design brief, and their ordering is the single most important finding for implementation: strong security and encryption (51%), clear rules on who can access data and why (49%), control over exactly what is shared and with whom (45%), and a government-backed trust mark (44%) all outrank a clear benefit such as faster services or less admin (38%), with independent oversight close behind (37%).

Trust outranks convenience. Notably, only 18% need proof that similar systems work in other countries. Businesses do not care about Estonia; they care about control. A scheme marketed on time saved will underperform a scheme guaranteed on security and consent. Deliverability scepticism, meanwhile, is lower than the state's IT record deserves: 66% think a single UK-wide system is realistic against 9% who think it outright unrealistic.

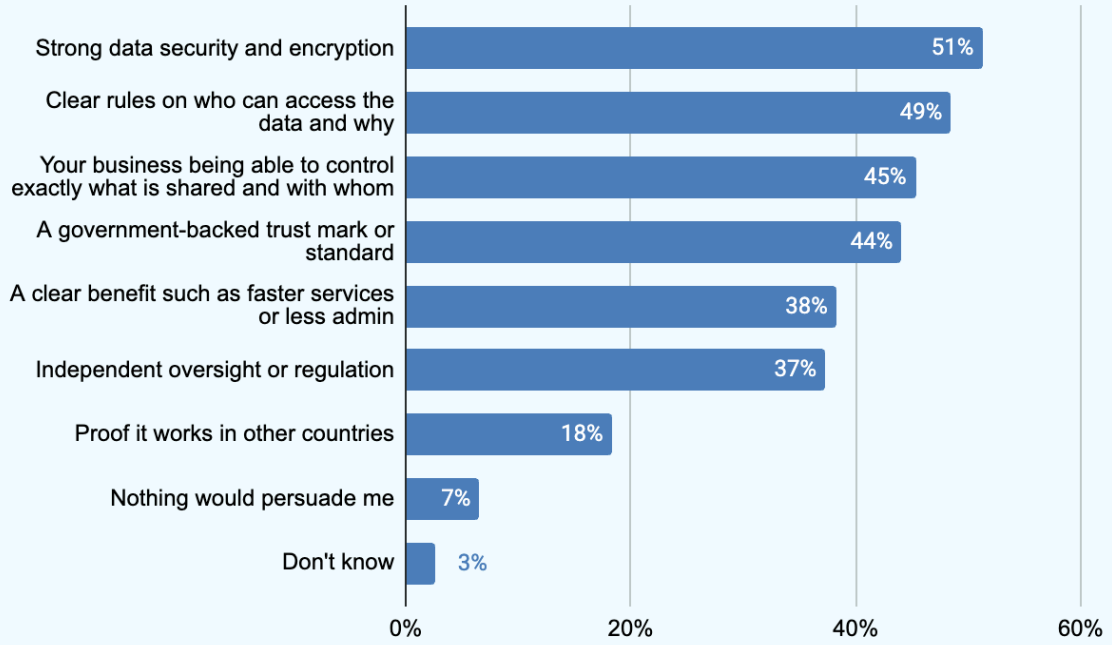


Figure 10, What would your business need to see before being willing to connect data about your business to your Business Digital Identity? Please select all that apply

Part One: the BizPass credential

The core is the universal identifier set out earlier in this report, expressed as a verifiable credential. For companies, BizPass is anchored to the Companies House record and carries the verified attributes the state already holds: registered number, legal status, registered address, filing standing. For sole traders, it is anchored to a One Login-verified personal identity, carrying trading details without exposing personal identifiers.

In both cases it also carries the role and delegation record set out in "Who may act" above, which is what turns a statement about an entity into one a counterparty can act on.

For every use of BizPass, we agree with CFIT in the principle of data minimisation, whereby the minimal amount of data should be shared to achieve the use case, though it is fundamentally up to the business themselves to determine which datasets they consent to share with a third party. The trust gradient supports the anchoring: HMRC and Companies House are the most trusted institutions in our polling (54%), well ahead of Whitehall in general (41%), and the most trusted actors overall, accountants (63%) and accounting software providers (52%), are precisely the regulated market this design hands the delegation and product layer to.

The delivery route is deliberately unglamorous, but it is not free. Section 45 of the Data (Use and Access) Act 2025 creates an information gateway allowing public authorities to disclose information to certified providers at the subject's request. It is a good piece of machinery and it is the right route for BizPass, with one obstacle: Part 2 of the Act is scoped, as a matter of statutory definition, to verifying

facts about individuals. The gateway cannot carry organisational attributes without the definition being extended, and that extension is primary legislation rather than a regulation.

It is, however, a single clause amending a definition Parliament passed last year, not a new statutory regime. It is the only primary legislation anything in this report requires. The gateway is also not yet in force: section 45 commences once the Code of Practice under section 49 is approved by both Houses. That sequencing is an opportunity rather than a delay, because the Code and the trust framework are being drafted now, and both can be written to anticipate organisational attributes before the power that carries them exists.

Part Two: the Enrichment Market

For Startup Coalition, the foundational BizPass is just the start. Where meaningful value comes in is what the business itself chooses to do with it, and this starts with enabling the private sector to utilise the BizPass.

The core credential answers one question: is this business who it says it is, and may this person act for it? That question sits at the front of almost every commercial interaction a business has. A bank onboarding a new customer, a marketplace admitting a new seller, an insurer writing a policy, a procurement team assessing a supplier, a lender assessing risk: each currently reconstructs the answer from scratch, from documents, and slowly. Each could instead check a credential in seconds and spend its effort on the judgement that actually differentiates it.

That is the immediate prize, and it requires nothing of the private sector except the ability to accept the credential. But acceptance is the floor, not the ceiling. Once an authoritative core exists, providers can build on top of it: corporate identity services that combine the state-verified core with trade references, payment history, sanctions and adverse media screening, sector accreditations, or ESG and supply chain attestations. A credential that says "this company exists, is in good standing, and this person may act for it" becomes the spine to which a market of enriched, differentiated propositions attaches. None of that enrichment needs to be built by the state, and none of it should be.

This is the division of labour the report has argued for throughout and identified by others, including, notably, CFIT. The state constitutes authority, because only it can. Everything a business actually touches, the interface, the wallet, the dashboard, the enriched profile, the integration into accounting software or a banking app, is built by a competitive market, and businesses choose between providers rather than being handed a single government product. Our polling supports the split: the actors businesses trust most are their accountants (63%) and their accounting software providers (52%), ahead of the institutions that would issue the credential. The people businesses want to deal with are not the people who should be minting the identity.

For that market to form, three things have to be true.

1. The credential must be portable. We take no position on where a BizPass is held in the first place. A government wallet, a certified private provider, or the accounting software a business already uses should all be able to hold and present it. A credential that works in only one wallet is a product, not infrastructure.
2. Checking must be free at the core. The credential costs nothing to hold, and verification of the state-held attributes should be free at the point of use. A per-check fee on the foundational layer

would price out precisely the smaller relying parties whose adoption determines whether this becomes universal. The market charges for enrichment and for the propositions built on top, not for asking whether a business is real.

3. Interoperability needs a neutral layer. A market of many issuers, many holders and many relying parties needs something between them, and it should not be a single dominant identity product. Orchestration is already a defined, certifiable role under the UK digital verification services trust framework, and the framework now prohibits an orchestrator from also being certified as an identity, attribute or holder service provider: the neutrality of the pipe is a regulatory requirement, not a design aspiration. The City of London Corporation's Digital Verification Orchestrator is an example of that layer.

Part Three: use Smart Data to bring all state interactions to the BizPass

The private market can only enrich what it can reach. Today, the information the state holds about a business is locked inside the department that holds it. A Business Data Smart Data scheme, designated under the powers in the Data (Use and Access) Act 2025, would unlock it, making BizPass the means by which every interaction a business has with the state can be brought into one place, on the business's instruction.[11]

A Smart Data scheme could mandate every part of the state apparatus that interacts with a business to build an API that enables the information they have about the firm to be shared, with the explicit consent of the business, verified through their BizPass, to a third party of the business's choosing. In practice, this would require a one-off investment of time from the business owner to associate their accounts, connecting each of their existing relationships with the state to their BizPass. Once connected, these federated attributes would be available through the Smart Data scheme to aggregate with an authorised third party (ATP).

Accreditation for ATPs can be provided for within the Smart Data scheme's own regulations under Part 1, which covers business data directly and needs nothing from Part 2 to operate. But the standards should not diverge. Any ATP handling verified business attributes should be held to the requirements of the UK digital verification services trust framework, overseen by the Office for Digital Identities and Attributes, and should become certifiable and listed on the DVS register once Part 2 is extended to legal persons. This matters for sequencing as much as for trust: the accreditation regime for a business data market does not need building from scratch, and it does not need to wait for the primary legislation either. Such a scheme should start with HMRC and the insolvency register, and then extend out to *every touchpoint with state bodies.* This should include Government departments and procurement directories, as well as arms-length bodies like UKRI and the British Business Bank.

ATPs would then be able to connect the data, with Business's consent, to build enriched, reusable business profiles on top. Consent should be scoped, time-limited, purpose-bound, logged, granted by role rather than by person, and revocable. Selective disclosure should be designed in from the start: a business should be able to prove "turnover above £X" without disclosing the figure, or "VAT-registered and current" without opening its tax affairs, a design principle aimed squarely at the one data category where discomfort nears comfort, summary financials (44% comfortable, 34% not). And this should be made possible through an orchestration layer.

[11] https://www.legislation.gov.uk/ukpga/2025/18/contents

The City of London Corporation's Digital Verification Orchestrator is one such developed UK proposal for that layer, and it is deliberately scoped to routing rather than credentialing: not a data store, not an assessor of whether an attribute is accurate, and explicitly not a regulator. BizPass should be designed to be routable through such a layer from the outset rather than retrofitted to it later. The business never sees the orchestrator, and that is the point, it should be invisible plumbing between the provider asking and the ATP answering.

Whilst the Government could itself build a business facing interface, acting itself as an ATP, we envisage that most, if not all ATPs, would be delivered by the private sector. A lively, competitive market of business identities. One constraint follows from the framework itself, and it is a useful discipline: because orchestration cannot be certified alongside other roles, no participant can be both the neutral routing layer and a competitor in the market it routes. Whoever operates orchestration, including the state, cannot also run an ATP. The separation of the layers is enforced rather than trusted.

Part Four: Make it Mandatory

Once BizPass exists, the government should regulate for its use across the state's own perimeter: departments and public bodies accept BizPass as the standard means of business verification, and, through the Smart Data scheme's action initiation provisions, recognise a verified change made once as made everywhere. Tax registrations, licence applications, grant claims, procurement bids and regulatory returns stop each demanding their own proof and start drawing on the same credential. The sequencing logic is deliberate: government is the counterparty businesses already share with most (68% share with HMRC or Companies House), the source of the single largest polled harm (30% handing identical information to multiple departments), and the most trusted institutional data holder in the study. The state is not being asked to build the market. It is being asked to become the anchor tenant of a rail it already owns, and everything businesses actually touch is built by the regulated market on top.

To be clear, the mandate falls on the state. The business takes on no new obligation. Instead of building a new account and identifier with each arm of the state that they interact with, they will always use their BizPass. BizPass is a credential, not a central database, and business owners will always have authority to revoke access.

What this unlocks

A world of opportunity awaits if the Government gets this right: bank onboarding in minutes rather than weeks, addressing the 17% who have had accounts delayed. Lending decisions on live verified data rather than stale filings, for the 12% delayed on finance. Supplier and procurement onboarding that replaces questionnaire sprawl with a credential, answering the 10% who have been unable to bid for or win a contract and the 21% who name easier proof of track record as a benefit. Tell Us Once for business, extinguishing the largest polled harm outright. Grant applications pre-filled from verified records. Export credentials a counterparty in Rotterdam can check as easily as one in Reading, for the 9% shut out of overseas trade.

Brought to Life

Illustration One: An MVP User Journey of BizPass

Phase 1 capability. No new primary legislation. Companies only.

A founder bids for a place on a public procurement framework. Today the entity section of the supplier questionnaire means re-entering the company number, registered address and legal status, uploading a certificate of incorporation, and attaching evidence that the person signing is entitled to bind the company. The same pack is assembled again for the next framework, and again for a UKRI grant application three months later.

With BizPass, she reaches the identity section and chooses to verify with her credential. The buying authority checks with Companies House that the credential is live and genuine, that the company is in good standing, and that she is a director whose identity has been verified under ECCTA. The entity and signatory sections come back populated and locked, and she starts the bid at the part that actually differentiates it.

The buying authority still runs its own financial standing, capability and due diligence assessment. BizPass removes the identity step in front of that, not the evaluation itself.

This journey needs nothing that does not already exist. The register is public, so no information gateway is required to release it; ECCTA supplies the verified individual; One Login supplies the authentication. What it cannot yet do is carry HMRC data (e.g. VAT status, tax compliance, filing history beyond the register) or let her delegate the submission to her bid writer. The first arrives with the Smart Data scheme, the second with the authority layer.

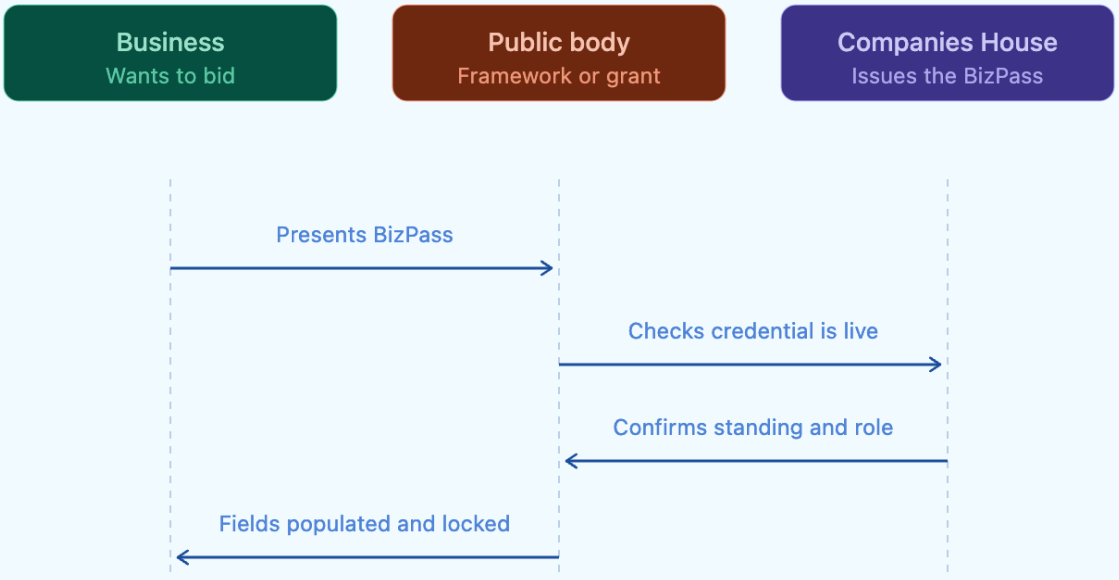


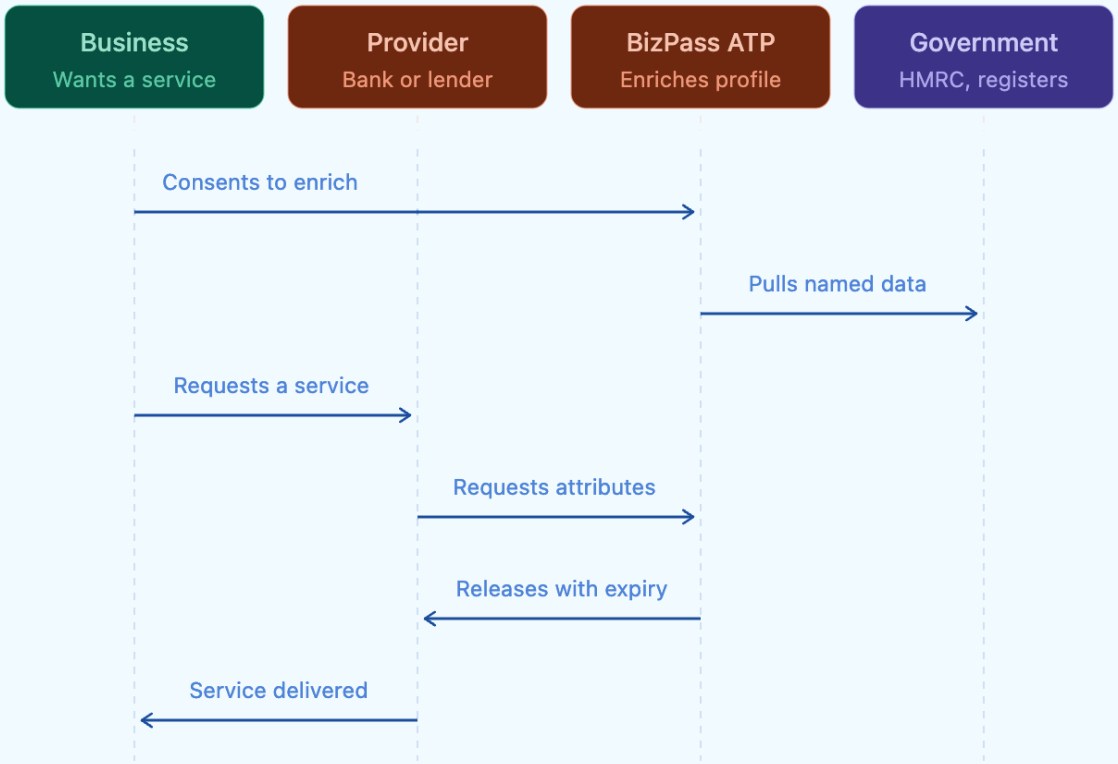
Illustration Two: A User Journey for BizPass 2.0

Phase 2 capability. Sole trader route live, Business Data Smart Data scheme designated.

A four-year-old manufacturing business wants working capital. Today its lender assesses risk from filed accounts that may be eighteen months old, a bank statement export, and a questionnaire.

With a Smart Data scheme live, the founder grants a scoped, time-limited, revocable consent from her accounting software, which is offering an enriched BizPass: for the next twelve months, this lender may see her VAT filing history, PAYE record and register standing. The credential proves who is instructing the release; the scheme provides the API the release runs through.

An enrichment provider, her accounting software, a corporate identity service, or the lender's own platform, combines the state-verified core with trade references, payment behaviour and sector data to build a live business profile. The lender decides on current evidence rather than stale filings, and the founder can revoke the connection the day the facility closes. The state built none of that enriched profile. It made it possible by minting the identity and opening the pipe.



The business authorises enrichment once; the provider asks the ATP, never the state.
Every release names its attributes, carries an expiry, and can be revoked early.

Illustration Three: The State Transformed by BizPass

Phase 3 capability. BizPass as the standard route into government.

The British Industrial Competitiveness Scheme will cut electricity costs for over 10,000 manufacturers.[12] Eligibility turns on three tests:

1. Operating in a designated sector,
2. Manufacturing an eligible product,
3. Using enough electricity in eligible activity

Applications run to a two-month window, and firms must assemble meter-level evidence for the proportion of electricity used in qualifying activity. The predictable result is that a scheme aimed at competitiveness begins with a paperwork exercise that rests on outdated static industry classifications.

With an enriched BizPass, the sequence inverts, with policymakers better placed to target policy interventions. The government can run eligibility rules against verified attributes it already possesses, such as sector, registered activity, filing standing, site records, tax filings, state procurement, even UKRI grant recipients. It could put the BizPass Smart Data scheme to work to ensure the right firms receive support. Additionally, it may be possible to better size a target sector in advance, thus better forecasting costs and impact of interventions.

Support reaches the firms it was designed for rather than the firms best equipped to apply. Take-up is measurable, and non-take-up is visible, which today it is not.

12 https://www.gov.uk/government/news/government-cuts-electricity-bill-for-10000-manufacturers-in-boost-for-uk-competitiveness

How others do it

THE EU: eIDAS 2.0, and a deadline that is also a threat

Under eIDAS 2.0, legal-person digital identity wallets are being made available to businesses across the EU by the end of 2026, and regulated sectors, banks first among them, must accept them from December 2027. From that date, a French SME proves itself to any European bank in one tap; a British SME couriers certified documents. In our polling, 9% of businesses have already been unable to trade with a business overseas because of verification friction. Business identity is becoming trade infrastructure, and the UK's absence from it is a non-tariff barrier of our own making.

SINGAPORE: Corppass and Myinfo Business: the closest analogue

Singapore is the nearest working model to what this report proposes: Corppass provides the government-issued authorisation layer binding individuals to entities with defined roles, and Myinfo Business lets a company consent to government-verified data flowing to private relying parties, banks pre-fill onboarding directly from verified state records. This represents an example of our two tier proposal: core plus consented enrichment, state anchor plus market delivery.

AUSTRALIA & NEW ZEALAND: minted numbers, universal coverage

Australia's ABN and New Zealand's NZBN are the proof that minting works and federation is unnecessary: single business numbers issued to every business form, sole traders included, that became the default key for dealing with government and, increasingly, with the private sector. Australia then added the layers the UK now needs: Director IDs (where ECCTA is now taking the UK), myID for authentication, and the Relationship Authorisation Manager binding verified people to businesses with delegated permissions. Australia is, in effect, a picture of the UK's own roadmap: ECCTA is completing step one, but the authorisation layer is the step not yet started.

ESTONIA: the register as live infrastructure

Estonia's register is the operating system of its business environment rather than a filing cabinet: who may act for which company is native to the system rather than re-established at every counterparty. The lesson is not "be Estonia"; it is that the authority layer, solved once at the register, dissolves downstream friction everywhere.

GLEIF vLEI: the standards answer

The Global Legal Entity Identifier Foundation's verifiable LEI wraps the twenty-year-old LEI code in modern verifiable-credential cryptography, including role credentials binding named individuals to entities. Its penetration among small businesses is negligible, but as a standards target it matters: a UK credential aligned with vLEI and W3C verifiable credentials is interoperable by design rather than by later retrofit.

The taxonomy across these models, registry-centric (Estonia), portal-and-delegation (Singapore, Australia), wallet-credential (the EU), shows the UK has genuine architectural choice. What it does not have is a choice about the success factor the systems furthest ahead share: they have solved authority, by which we mean the binding of people to entities, and not merely entity existence. None of them records every permission centrally. What each has established is an authoritative root, from which delegation flows under the entity's own administration. That root is what the UK is missing, and it is the one genuinely new thing this report asks the state to build.

Our blueprint

Enabling businesses to verify who they are quickly, repeatedly and securely is unglamorous work, and it is exactly the kind of foundational plumbing a government serious about growth should want to own. It is deliverable inside this Parliament, it starts with a decision that costs nothing, and it would compound for a decade. The state's role throughout is the one only it can play: minting the authoritative core and constituting the record of who may act for whom. Everything a business actually touches is built by the market on top.

The blueprint splits on a real fault line. Phase 1 is decisions: things a minister can announce and officials can begin without any legislation at all. Phase 2 is where the legislation sits, alongside the two things that have to be built. Phase 3 is the rail.

The sequencing is driven by a date. Between November 2025 and 18 November 2026, Companies House expects six to seven million directors and persons with significant control to verify their identity. Declaring today that this effort will yield a reusable credential converts a compliance programme into an asset businesses get back. Declaring it afterwards asks them to feel differently about a cost already sunk. Everything in Phase 1 is therefore worth more before that date than after it, and none of it needs new primary legislation.

Phase 1: Decisions (0–12 months)

1. **Declare BizPass.** A public commitment from the Business Secretary that the six to seven million ECCTA identity verifications to be completed by 18 November 2026 will yield a reusable credential: the Companies House number, established as the authoritative anchor of a BizPass carrying the company's verified attributes. It costs nothing, sets the direction for everything that follows, and converts a compliance programme into an asset.
2. **Name the accountable owner.** DBIST must assign a single body responsible for issuance, with the Office for Digital Identities and Attributes retaining oversight of the trust framework the credential is certified against. Business identity currently sits between Companies House, HMRC and DSIT and is owned by none of them. No programme this cross-cutting survives without a named owner, and naming one is a decision, not a spending commitment.
3. **Issue the credential to verified companies.** Express the Companies House record as a presentable, revocable verifiable credential carrying registered number, legal status, registered address and filing standing. Alongside it, provide a verification lookup so a counterparty presented with a BizPass can confirm it is live, genuine and currently held, without a browsable public index of businesses existing to be scraped.
4. **Commence the information gateway, and draft it for organisations.** Bring the section 49 Code of Practice before both Houses so section 45 commences, and instruct OfDIA to write the Code and the next revision of the trust framework so that organisational attributes and an organisational supplementary code are ready the day the statutory scope allows them. None of this requires legislation. All of it removes months from Phase 2.

Phase 2: Mint universally, designate the scheme (12–24 months)

5. **Extend digital verification services to legal persons.** A single amendment to Part 2 of the Data (Use and Access) Act 2025, extending the definition of digital verification services beyond individuals so that the information gateway, the trust framework and the DVS register can carry organisational attributes. This is the only primary legislation in this report. It amends a definition rather than creating a regime, and it is small enough to ride any suitable vehicle.
6. **Build the authority layer.** Establish, at the register, the record of which verified individuals may act for which entity and in what capacity, with defined, revocable, role-based delegation. A director may hold full authority; a finance manager authority to open accounts but not to file; an accountant authority to submit returns and nothing else. The state establishes the root and holds the record of who may act; it does not administer every permission, and it should not. This is the pattern Singapore and Australia have established and the UK has not, and it is the one genuinely new thing this report asks the state to build.
7. **Complete coverage: build the unincorporated route.** A One Login-verified individual may register a trading identity and be issued a BizPass, a business-facing credential that never exposes personal identifiers. Partnerships anchor to one verified partner, with the others bound through the authority layer at 6. This completes coverage across all 5.6 million UK businesses rather than the 2 million on the companies register.
8. **Designate a Business Data Smart Data scheme under the Data (Use and Access) Act 2025, with a phased data catalogue.** Start with HMRC and the insolvency register, then extend iteratively to every part of the state that holds information about a business, including departments, procurement directories and arms-length bodies such as UKRI and the British Business Bank. Consent should be scoped, time-limited, purpose-bound, logged, granted by role rather than by person, and revocable, with selective disclosure designed in from the start.
9. **Align UK credential standards with the eIDAS Architecture Reference Framework and W3C verifiable credentials.** Regulated European acceptance of legal-person wallets begins in December 2027. Aligning now means British businesses interoperate from that day rather than by later retrofit, and it is the difference between a domestic convenience and trade infrastructure.

Phase 3: Regulate the rail (24 months and beyond)

10. **Make BizPass the default door into government.** A regulated requirement, phased department by department, that interactions between businesses and the state, including tax, licensing, grants, procurement and regulatory returns, accept and run on BizPass as the standard means of business verification, with the Smart Data scheme's action initiation powers carrying a verified change made once as made everywhere. The obligation falls on departments to accept the credential, not on businesses to hold one. Public procurement frameworks should be first, replacing supplier questionnaire sprawl with a single credential. Because much licensing and regulatory interaction is devolved, rollout needs a parallel conversation with the devolved administrations from the outset rather than as an afterthought.
11. **Pursue mutual recognition with the EU wallet ecosystem and the vLEI, so a UK business credential is trade infrastructure, not a domestic convenience.**

What we ask of industry

The state's job ends at the authority layer and the credential. Everything else, including wallets, dashboards, enriched profiles, integration into accounting software and banking apps, is the market's, and the market has to show up. Banks, marketplaces, insurers and procurement teams should commit to accepting a BizPass at the identity step as soon as one exists, before any regulatory requirement obliges them to. Accounting software providers, the actors businesses trust most after their own accountants, should commit to holding and presenting the credential on their customers' behalf. Neither commitment requires the credential to be finished. Both would materially shorten the time between BizPass existing and BizPass mattering.

Methodology

Estimating the verification burden

Our headline estimate multiplies three quantities: the number of identity or verification checks the average business completes in a year, the average time each check takes, and the number of businesses in the UK.

Respondents were asked how many times in the past twelve months their business had verified its identity or provided business registration details to an external organisation. Responses (n=501) were:

Checks in past 12 months	Share
Never	14%
1-2	31%
3-5	28%
6-10	13%
11-20	5%
21-50	4%
50+	2%
Don’t know	2%

Taking the midpoint of each band, rebasing to the 97% who gave an answer, and valuing the open-ended top band at its minimum of 51, the mean is 6.02 checks a year. Valuing the top band at 60 gives 6.21 and at 75 gives 6.52; we use six throughout. The distribution is skewed: the median business sits in the 3-5 band, while the 6% reporting twenty-one or more checks a year account for a disproportionate share of the total. Both facts matter, and the estimate is built on the mean because the aggregate burden, not the typical experience, is what we are measuring.

On duration, 15% reported under five minutes, 40% five to fifteen, 28% ten to thirty, 8% thirty minutes to an hour, 3% one to two hours and 1% more than four hours, with 6% unsure. Midpoints on the same basis give 19.7 minutes; we use twenty. Two limitations should be noted: the five-to-fifteen and ten-to-thirty bands overlap, and no band was offered between two and four hours. Neither materially affects the estimate.

Six checks at twenty minutes is 2.0 hours per business per year. Across 5.6 million UK businesses that is 11.2 million hours, or approximately 6,200 people working a full-time year. We convert at 1,800 hours to a full-time year, above the roughly 1,700 a UK employee works after holiday entitlement, because the higher denominator produces the more conservative headcount.

We also publish a floor. Assign every respondent the lowest value in their band, on both questions, and assume those answering "don't know" spent no time at all: 4.47 checks at 12 minutes is 0.89 hours per business, 5.0 million hours across the population, or approximately 2,800 full-time equivalents. This is below any realistic reading of the data and is offered as a hard minimum.

All figures exclude waiting time, chasing, and any downstream delay to bank accounts, finance, contracts or trade. They measure only the direct time spent completing checks. Full data tables are available on request.

STARTUP
C*ALITION