PAS 201:2018

Supporting fintechs in engaging with financial institutions – Guide

HSBC

BARCLAYS

NatWest

Santander

LLOYDS BANKING GROUP

TECH NATION

Royal Bank of Scotland

bsi.

Publishing and copyright information

Published by BSI Standards Limited 2018.

ISBN 978 0 539 00165 5

ICS 03.060, 35.240.40

Contents

Foreword

This PAS is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 7 November 2018.

This PAS was sponsored by the Fintech Delivery Panel (FDP). Its development was facilitated by BSI Standards Limited and it was published under license from the British Standards Institution.

Acknowledgment is given to Matt James (Royal Bank of Scotland), as the Technical Author of this PAS, and the following organizations that were involved in the development of this PAS as members of the steering group:

- Barclays
- HSBC
- The ID Co.
- Innovate Finance
- IWOCA
- Lloyds Banking Group
- Market Invoice
- NatWest and the Royal Bank of Scotland
- Santander
- Tech Nation

The following funders of this PAS are also acknowledged:

- Barclays
- HSBC
- Lloyds Banking Group
- NatWest and the Royal Bank of Scotland
- Santander

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS, and to the wider FDP who also supported its development.

The PAS process enables a guide to be rapidly developed in order to fulfil an immediate need in industry. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Regulation and compliance

IMPORTANT:

The information contained in this document is for general guidance only. The application and impact of laws can vary widely based on the specific facts involved. Given the changing nature of laws, rules and regulations, there may be delays, omissions or inaccuracies in information contained in this document.

Accordingly, the information in this document is provided with the understanding that the authors and publishers are not herein engaged in rendering legal, accounting, tax, or other professional advice and services. As such, it should not be used as a substitute for consultation with professional accounting, tax, legal or other competent advisers.

Sources of UK regulatory guidance:

- HM Treasury (HMT): www.gov.uk/government/organisations/hm-treasury
- Bank of England (BoE): www.bankofengland.co.uk/prudential-regulation
- Prudential Regulation Authority (PRA): www.prarulebook.co.uk
- Financial Conduct Authority (FCA): www.fca.org.uk
- EU General Data Protection Regulation (GDPR): www.eugdpr.org
- Competition & Markets Authority (CMA): https://www.gov.uk/government/organisations/competition-and-markets-authority
- Ring-fencing: https://www.gov.uk/government/publications/ring-fencing-information/ring-fencing-information
- The Computer Misuse Act (1990): https://www.legislation.gov.uk/ukpga/1990/18/contents

See also Annex B for further support.

NOTE *Some financial institutions will operate in a variety of countries and as such the regulatory requirements of those jurisdictions will also become relevant.*

Introduction

Financial services is in the midst of fundamental change, driven and enabled by technology advances that will transform the industry, place control in the hands of customers, and radically change the nature of the competition the established institutions face.

The business of banking will look completely different, delivered through digital technology that customers, conditioned to expect speed and innovation from all suppliers, regard as a basic hygiene factor. Banking is becoming more connected; with business models that digitally link customers and other providers of products and services.

New competitors, unencumbered with expensive and inflexible legacy architectures are entering the market. Open Banking will reduce barriers to entry. Banking services may simply become a commodity component of wider value chains. The environment is challenging. The changes are significant. The industry is moving from the traditional models to one where small can now compete effectively with larger suppliers.

Most established financial institutions are recognising the need to position themselves to address these threats and embrace the opportunities. The positive approach by established providers demonstrates a widespread awareness of how fintech will benefit all: the start-ups, the financial institutions and, most importantly, the consumers.

The UK has long recognised that embracing innovation is central to ensuring long-term success and the development of new financial technologies is the latest pivotal shift. It is a testament to the UK's competitiveness that its financial services sector, with support from the wider ecosystem, has positioned itself at the forefront of the fintech revolution.

As we move beyond the initial hype it has become clear that the benefits of this high-growth area can best be secured through a collaborative, joined-up approach. The Financial institutions have longer established customer relationships, larger scale, more funding, and developed regulatory and legal knowledge; whilst start-ups often have more innovative ideas, more specialised technological expertise, and the ability to be agile and move fast. The combination of these factors can help the UK continue to grow as a world leading fintech hub.

Yet, too many fintechs and financial institutions are still uncomfortable allies. Financial institutions often risk being perceived by start-ups as inflexible and bureaucratic, while fintechs may be perceived as lacking understanding of the regulatory challenges and demands of servicing customers at scale faced by established financial institutions.

Any great engagement is underpinned by open communication and mutual understanding. The purpose of this PAS is to lay out guidance for fintechs that will help them understand, prepare for and more easily navigate the path to forming successful engagement with large financial institutions. In addition it can provide a foundation document around which fintechs, financial institutions and regulators alike can discuss ways to improve and streamline the process to enhance the UK's position and importantly benefit customers.

The FDP was formed in 2017 at the request of HM Treasury to help sustain and accelerate the growth of the fintech sector in the UK. The FDP is facilitated by Tech Nation and brings together the leading fintechs and established financial institutions from across the UK.

This PAS has been produced in response to an FDP commitment to drive collaboration between fintechs and financial institutions. It is believed that introducing voluntary standards is crucial to achieving more collaboration to make piloting products and services easier.

This page is deliberately left blank.

1 Scope

This PAS provides a guide to fintechs on the terms and approach used by many financial institutions for collaboration and commercialisation of new fintech propositions. It forms part of a wider body of work, referred to within the HM Treasury, Fintech Sector Strategy (March 2018), to develop a set of industry standards that will support fintech firms by providing them with a consistent understanding of what financial institutions will need from them before entering into partnership arrangements.

Its intention is to provide a framework that will allow fintechs to better prepare for and confirm that they are ready to engage with a large financial institution. It provides an explanation of both the commercial considerations and the necessary checks and controls that need to be satisfied to meet business and regulatory demands.

NOTE *Many of the processes and policies within this PAS are similar to those used for any supplier engagement and are not unique to engagement with fintechs.*

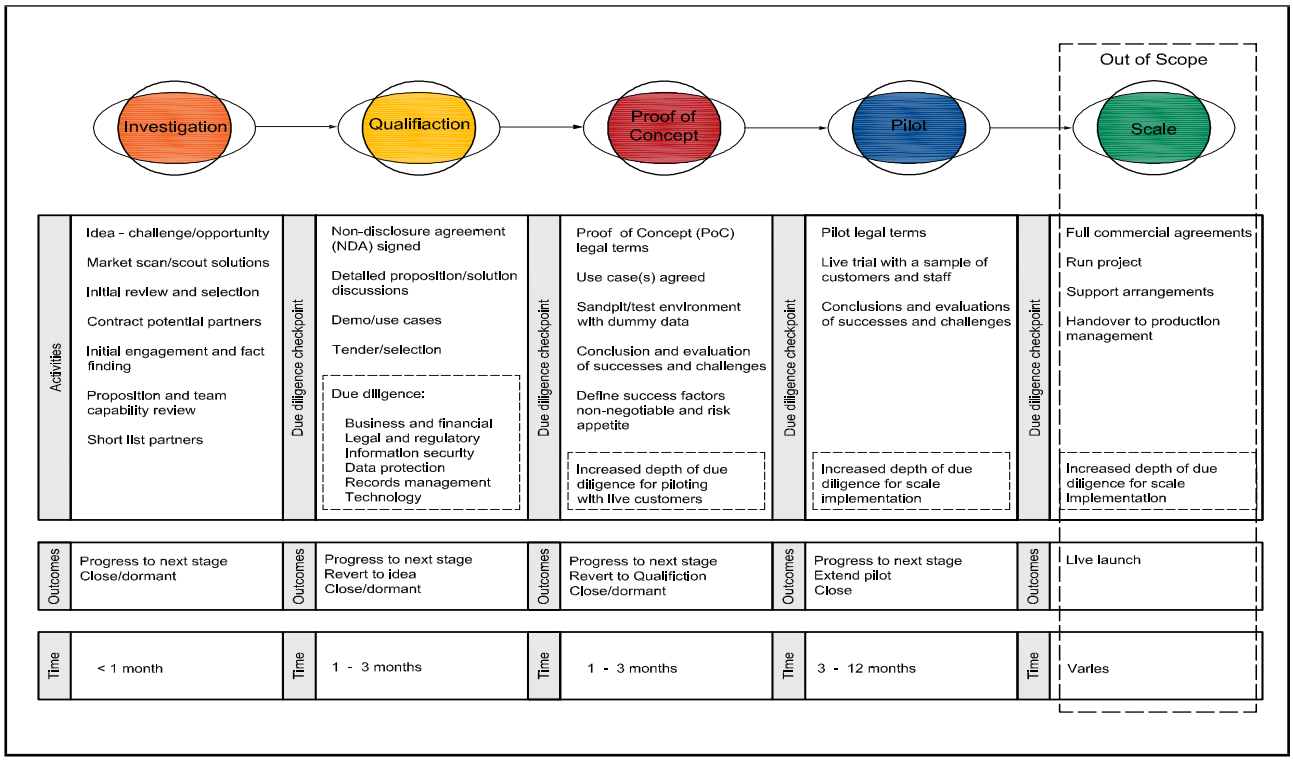
Specifically it provides:

- key terms and definitions;
- a framework of the categories information, checks and controls necessary to establish a commercial engagement;
- guidance on the preparation, data gathering and steps that a fintech can undertake to facilitate and speed-up the due diligence, commercial and contractual processes; and
- data protection and information security considerations.

It should be noted that each financial institution will have a different risk appetite, dependent upon their business strategy, the customer segments they support, markets they serve and geographies in which they operate. It will also depend on whether the fintech is to be engaged directly with customers or internally within the financial institution. As such it would not be possible to provide a definitive single guide and process.

This PAS is not intended, therefore, to be a definition of the engagement process as this could vary considerably from institution to institution. However, to aid understanding, Figure 1 provides a generic view of the broad stages in taking a new fintech solution from idea to implementation at scale. Whilst many fintechs are experienced in engaging with financial institutions and the on-boarding requirements, this PAS has been written from the perspective of helping early stage fintechs who may have little or no understanding of the process.

Figure 1 – Illustrative innovation process – idea to delivery



***NOTE** Figure 1 depicts a linear process for simplicity, however stages might be skipped or loop-back depending on the solution and findings at each checkpoint.*

The PAS has been produced predominantly from the perspective of large established UK banking institutions. Whilst much of the guidance is applicable to other financial institutions it does not purport to be exhaustive and all encompassing.

The PAS does not therefore cover:

- specific statutory, regulatory or legal requirements which can be obtained elsewhere (e.g. guidance on open banking or GDPR);
- every jurisdictional or geographic, regulatory or market specific requirement;
- in-depth definition of processes which may be applied as part of establishing an engagement;
- specific acceptance standards, as these may differ institution to institution;
- on-boarding the fintech as a banking customer; or
- processes whereby a financial institution may seek to make an investment in the fintech.

The PAS is predominantly for use by fintechs and other industry-related start-ups. It may, however, be of interest to banks and other financial institutions, accelerators, technology incubators and regulators.

2 Terms and definitions

For the purposes of this PAS, the following terms and definitions apply.

2.1 financial institution

company engaged in the business of dealing with financial products and services.

2.2 fintech

new technologies that are disrupting traditional financial services

NOTE *This may be a complete financial services proposition or business model, or a technology used to disrupt existing or create new propositions or approaches. These technologies can be applied to provide service to customers, drive efficiency and cost reduction or enhance security and avoidance of fraud.*

2.3 fintechs

start-up technology companies developing new products, services and approaches in the financial services sector that may or may not be regulated

2.4 innovation

executing new ideas, often enabled by new technologies, that have meaningful impact.

NOTE *Turning insights into new products, services or business models that have the potential to change 'what we do and how we do it' with measurable and material impact on revenue generation, cost reduction and customer satisfaction.*

2.5 minimum viable product (MVP)

new proposition with sufficient features to satisfy early adopters.

NOTE *The final complete set of features are designed and delivered after gathering feedback from these initial customers. Often used as the basis for a proof of concept or pilot.*

2.6 non-disclosure agreement (NDA)

legal contract between parties that defines and protects how intellectual property, proprietary or confidential material and information can be used and shared.

NOTE *sometimes also referred to as a confidentiality agreement.*

2.7 pilot

approach to test a new proposition, often in the form of a minimum viable product, with a controlled subset of live customers to gain insight and feedback on functionality and satisfaction.

2.8 proof of concept (PoC)

approach to test a new proposition, often in the form of a minimum viable product, in a sandbox environment to gain insight and feedback on feasibility and functionality.

2.9 RESTful (Representational State Transfer)

set of architectural principles by which data can be transmitted over a standardized interface

NOTE *An example of this would be HTTP*

2.10 risk appetite

the level and type of risk a firm is able and willing to assume in its exposures and business activities, given its business objectives and obligations to stakeholders.

NOTE *Risk appetite is generally expressed through both quantitative and qualitative means and considers extreme conditions, events, and outcomes. In addition, risk appetite reflects potential impact on earnings, capital, and funding/liquidity.*

2.11 sandbox

dedicated environment designed for testing of new applications, technologies or processes

NOTE *This "safe" environment is representative of a production environment but often uses synthetic or dummy data.*

2.12 scale engagement

moving a solution from a test or pilot state into a fully productionised and supported solution.

NOTE *Solutions could be deployed to support business critical process or tens of millions of customers, requiring significant support, control and resiliency arrangements to be put into place.*

2.13 start-up

entrepreneurial venture often applying newly emerging technologies or business models to deliver an innovative new proposition or service with the intention of disrupting or materially enhancing established solutions.

3 Qualification process

Whilst it is recognised that working with fintechs requires a different approach to engaging with more established parties, financial institutions still need to undertake suitable due diligence to ascertain the appropriateness of the potential fintech. When entering into contracts, the financial institution will want to know that the relationship will be beneficial to itself and its customers, and to the fintech whilst at the same time identifying and managing any associated risks.

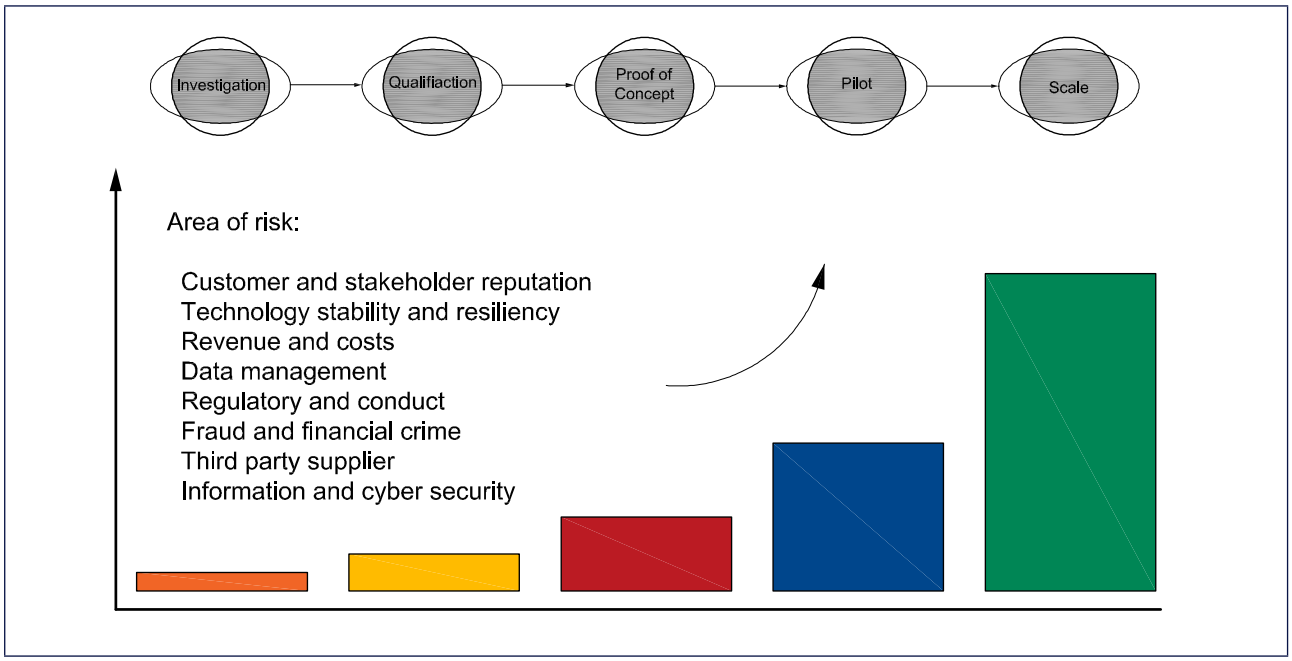
The breadth and depth of due diligence will vary dependent on whether the institution:

- is using the technologies internally to drive efficiency and cost saving;
- is seeking to undertake a research and development study, or proof of concept, in a sandbox environment to learn and experiment around a new technology;
- is seeking to pilot the solution, limiting the scope, scale or duration, but with live customers or transactions; or
- has the objective and intention to deliver and deploy a live solution to market at scale.

The fintech should consider this a two-way process and take the opportunity to understand the aims and objectives of the financial institution.

In addition, as an innovation initiative progresses through the process from investigation to scale, the level of due diligence required by the financial institution will broaden and deepen across the various aspects of risk that have to be considered as illustrated in Figure 2.

Figure 2 – Qualification process



IMPORTANT:

Wherever the term 'fintech' is used within this PAS this encompasses any third party supplier or service the fintech utilises in delivering its proposition, product or service. The fintech has overall responsibility to ensure all third parties that it uses meets the standards and control requirements; and is able to evidence this.

4 Qualification requirements overview

The area of due diligence that the financial institution will be interested in is summarised in Table 1 and expanded in the clauses that follow.

Table 1 – Qualification requirements overview

Section	Criteria	Description
5.	**Proposition and market positioning**	
5.1	Proposition overview	A short summary pitch deck that explains what your proposition is by answering: What is the problem (for customer or financial institution) that you are solving and What is your solution and how does it help to solve the problem.
5.2	Customer pain points addressed and example use cases	A clear articulation of the customer pain points being addressed and for which segments ideally bringing this to life with specific use cases.
5.3	Market insights	Explain your view of the market and assessment of the opportunity. Setting the market context can help align thinking between the parties involved.
5.4	Competitive positioning	Articulate your competitive space; when comparing to competitors, make clear on what dimensions you are better or worse.
6.	**Business and team**	
6.1	General	The people involved in the collaboration are as important as the technology itself. Provide a team make-up, key individuals and insight and the intellectual capital within the start-up.
6.2	Team make-up	Who holds key roles, the team size and organisational structure, what resources would be assigned to the engagement, where are people located geographically, who are the key people and brief resumes, illustration the depth of insight and specialist knowledge of individuals with key skills.
6.3	Development model	An overview of the mid-term business plan of the company and how much of the development of the service will be handled in house, compared to outsourcing.
6.4	Branding	Options around whether the final product will be branded by the fintech itself, co-branded with the financial institution, or distributed as a white-label product.
6.5	Advisers and investors	Information on the existence of an advisory board and its members. This will also be of interest from the perspective of identifying any potential conflicts of interest. Any investors in the start-up will similarly be of interest, including the stake held and any special terms that may apply.

Table 1 – Qualification requirements overview *(continued)*

Section	Criteria	Description
7.	**Legal regulatory and commercial**	
7.1	General	It's paramount for fintechs to understand the structure of the agreements they are entering into. At the same time, the financial institutions should only engage with fit and proper partners as they have various regulatory obligations to be satisfied.
7.2	Non-disclosure, PoC and pilot agreements	There are usually requirements to draw up appropriate legal agreements between the two parties. Often these agreements are 'mutual', meaning there are restrictions and protections afforded to both the financial institution and the fintech.
7.3	Company legal structure and conduct	An explanation of the legal structure and set up of the fintech including identification of holding companies, subsidiaries and other related companies. There will be a requirement to demonstrate that there are no aspects relating to the fintech which disregard appropriate controls, activities or processes relating to: anti-bribery and corruption laws and regulations; anti-money laundering, tax avoidance or terrorist financing laws and regulations; sanctions relating to restricted countries or individuals; and regulatory rules and requirements.
7.4	Conflicts of interest	Any engagement will need to operate on the principle that they identify and manage conflicts of interest fairly and effectively. There needs to be an understanding of any relationship between the financial institution and the fintech, including key personnel on both sides, to ensure any engagement has been introduced, selected and contracted with integrity and transparency to avoid the perception of, or actual: bribery, corruption, questionable conduct, seeking to obtain any improper influence; advantage obtained as a result of the giving or receiving or gifts, hospitality and entertainment by any of its employees or third parties; and breach of any law, regulation, code or policy.
7.5	Company financials	Evidence of financial performance and ongoing viability in terms of: capital availability, funding stage and sources; existing revenues and debts; profit and loss account, and balance sheet; cash flow; existing engagement commitments; resourcing levels; and financial forecasts and growth/scaling plans.
7.6	Commercial model	An explanation of the commercial terms including the proposed use, by either party, of brand marks or marketing collateral associating the organisations. Include aspects such as: proposed pricing model e.g. per transaction, user or enterprise level; revenue share; license fees to be charged; services levels and cost tiers, if costs change by volume or other factor; support arrangements and service level agreements, third parties used, including associated costs; guarantees and/or indemnities expected or given; responsibility for any liabilities; and penalties relating to non-performance.
7.7	Intellectual property agreements	An understanding of how the two businesses will work together, and to provide clarity about: what intellectual property already exists; who owns the existing intellectual property; how existing intellectual property might be used by each party, and on what terms; who will own any new intellectual property created as a result of working together; and how intellectual property might be combined, where necessary.

Table 1 – Qualification requirements overview *(continued)*

Section	Criteria	Description
7.8	Fraud prevention	Explanation of scenarios/responsibilities which relate to fraud risk, particularly with relation to introduction of customers, processing money transactions and handling classified (including customer) data.
7.9	Business resilience	Details of business resilience plans in place in case their premises/staff fail to enable them to continue to operate and supply the contracted service or product within an acceptable recovery time.
7.10	Regulatory compliance	Demonstration of regulatory compliance and required approvals, along with disclosure of any information that may give rise to regulatory concern.
7.11	Other ethical policies	Explanation of your sustainability policy including economic, ethical (social) and environmental considerations. As a minimum requirement, demonstration of adherence to all relevant human rights, labour, health & safety and environmental laws.
8.	**Information security and data protection**	
8.1	General	There is a need to ensure that both customer data and the financial institutions data are safe and adequately protected through appropriate physical, procedural and technological protection and controls.
8.2	Information security, back-up and archiving	An explanation of the activities and responsibilities relating to: capturing, storing or disposing of records, customer transactions, data or assets; supporting or maintaining facilities or infrastructure containing or processing any information whether on-site or off-site; and having remote access or connectivity or access to their data or premises.
8.3	Payment security	A description of the activities and responsibilities of the fintech where they undertake any aspect of the end to end payment process. Evidence where required of registration with the respective card schemes and demonstration of compliance with the Payment Card Industry Data Security Standard.
8.4	Physical security	Explanation of the activities and responsibilities where you have access to, manage, processes or store the Institution's assets; or unescorted access rights to the Institution's premises.
8.5	Access rights and controls	Explanation of the activities and responsibilities in terms of technical and support personnel having administrator or special access rights to systems and data relating to the financial institution's deployment of a solution; and how the rights and privileges are appropriately monitored, controlled and audited.
8.6	Data protection	Description of the activities, protections, controls and responsibilities relating to compliance with GDPR regulations including an details of access to any data, however stored, (including electronic data, systems and printed records and confidential waste) relating to: customers/clients, staff (including contractors, job applicants, pensioners etc.) and shareholders; and protection of company confidential and secret information.
8.7	Records management	Description of the activities and responsibilities of the fintech which cover creating, using or storing and deleting the institution's records.

Table 1 – Qualification requirements overview *(continued)*

Section	Criteria	Description
9.	**Technology**	
9.1	General	An understanding of the technologies being applied, how they can be scaled and the future road-map and support arrangements.
9.2	Platform readiness	The readiness of the fintechs product or platform will help to drive the type of the discussions being had with potential partners. The fintech should be clear about the current state of the product or service that is being or has been developed e.g. alpha, beta, MVP, market ready.
9.3	Technology architecture	An explanation of the technology architecture. This information should be documented in detail along with high level architecture diagrams showing system connectivity as well as data flow. An architecture diagram, should also detail differences between, development, test and production services.
9.4	Development roadmap	An explanation of the direction of the solution during the proposed period of the contract. The roadmap should be in as much detail as possible over the near term (6-12 months) with an indication of future direction beyond this.
9.5	Support arrangements	Definition of support arrangements including details of SLAs, change control processes, support times, escalation and reporting arrangements.
9.6	IT resilience	An understanding of the scenarios/responsibilities where there is provision of IT solutions or services which, if lost, would disrupt one or more critical activities. This would include arrangements for recovery and resiliency and contingency testing.

5 Proposition and market positioning

COMMENTARY ON CLAUSE 5

The reason financial institutions want to engage with fintechs is to access talent, technologies and business models which will rapidly bring to market innovative products and services to better serve customers. This clause provides guidance for fintechs on how to present their proposition and position themselves in the market.

5.1 Proposition overview

5.1.1 The basics

Prepare a short summary pitch deck that explains what your proposition is by answering:

- What is the problem (for customer or financial institution) that you are solving?
- What is your solution and how does it help to solve the problem? The use of journey mapping is a useful technique to show how the solution could fit into the customer journey.
- What is the functionality of your proposition, and how does it work? (use business terminology, high-level technical concepts are acceptable, but don't get too deep into it at this stage)
- Where is the solution positioned on the value chain? Does it replace any existing players or make the chain shorter?
- What is the relevance to the financial institution? Do your homework (you wouldn't turn up for a job interview without researching the company; you need to do the same with your proposition to explain the relevance to the organisation you are approaching) – why should the engagement happen? What are the benefits for both parties? Are they equally weighted?
- Any key risks the financial institution should be aware of and how the fintech would address these.

5.1.2 Other considerations

There are other aspects to consider when preparing a pitch deck, such as:

- There are generally two audiences within a financial institution: those more familiar with fintech and external trends and those closer to the business problems and opportunities. A fintech's initial contact points are likely to be those with external facing roles in innovation or business development; use the shorter pitch decks for these initial emails and meetings. Follow-on meetings with the 'subject matter experts' will go into more detail on your proposition.
- Short summary documents and small files (<5MB) make things easy to email (file share sites are frequently not accessible on bank corporate networks for security reasons).
- Focus on what your proposition does really well, with only one or two use cases and give a clear reason as to why it does so well. What is/was the benefit realised? Make it relatable to the audience.
- Componentise the proposition if possible; replacing existing solutions is risky and expensive – can your proposition replace an element initially to prove itself, and be expanded subsequently into broader offerings?
- Consider what issues and requirements there may be with respect to implementing and integrating the solution and the steps required to mitigate.
- The engagement/sales cycle in financial institutions can be much longer than you anticipate, so be prepared for building your case over time.
- Internally, the bank will try to fit your proposition against internal programmes, customer segments and business opportunities. Though they may not share the specifics here, you should try and help them understand clearly how you could fit in.
- Successful presentations are about style as well as content.

5.1.3 Common pitfalls

Fintechs can avoid proposition pitfalls by:

- remembering that the financial institution is neither an investor nor a customer, but a potential partner and collaborator; therefore don't pitch material that is focused on fundraising or customer sales;
- avoiding generic marketing speak;
- avoiding unclear functionality and overloading the latest jargon into your summary; explain how any technologies being applied (e.g. AI, blockchain) add to the proposition;
- making it clear what is already part of your solution and what is part of your roadmap (there is no problem with not having everything built yet). Be clear about your capabilities but avoid overselling what you are able to do;
- not listing too many products and use cases as this will detract from your core message. 'We can do anything' confuses people and might impact on trust;
- having awareness of future technology. A number of fintechs have a great idea; however with the rate of change in the industry, the idea can be subject to technical obsolescence and therefore the window of opportunity to gain value is too narrow to progress.

5.2 Customer pain points addressed and example use cases

5.2.1 The basics

5.2.1.1 Fintechs should include customer pain points in their pitch deck by:

- clearly articulating what the customer pain points are, and for which segments;
- explaining how the customer or bank colleague will benefit from using your solution;
- giving examples of each and bring the examples to life with a specific use-case for a customer journey; and
- tailoring these to the bank you are engaging and the jurisdictions and clients they serve.

5.2.1.2 Financial institutions are looking to engage with fintechs that can help them better serve their customers, or solve internal problems. It's crucial that you demonstrate a firm understanding of a customer need and explanation of how the solution you have built meets that need. Try to narrow it down to the essence of the need and solution; most likely, you are not a "one-stop-shop" as an early-stage company. Equally important is to articulate which segment in the market you are serving. Remember, financial institutions usually service a wide range of market segments and sometimes will have different people within the organisation working on similar propositions but for different segments, so be clear who your target audience is. It's also less credible that you are capable of effectively serving numerous market segments. In order to make the engagement process as quick and efficient as possible, give real-life examples or specific use-cases for a customer journey; the financial institution will want to understand how this engagement would benefit their customer or colleagues.

5.2.2 Common pitfalls

Common pitfalls in this area include:

- claiming that your reach is greater than it really is, or that you solve all problems for all segments – be realistic;
- offering services that are irrelevant to the target customer-base; and
- not understanding who the financial institutions market is, and share of that market.

5.3 Market insight

5.3.1 The basics

5.3.1.1 Explain your view of the market and assessment of the opportunity. This section is important, as it shows that you do not just have a "solution looking for a problem"; you understand the product-market fit concept and that the problem is substantial enough to warrant the investment in a solution. Make sure you are explaining the market opportunity in two dimensions. Firstly for you as a company, and secondly the market opportunity for your partner using your solution and the value for their business, with the realistic chance of utilizing this opportunity. The better you tailor this, the less thought is required to understand why it's valuable to partner with you. If you can present customer references and indicators of traction, that brings to life the projection of the business opportunity.

5.3.1.2 Setting the market context can help you align your thinking with that of your potential partner. It can also help colleagues within your partner upskill those who are less familiar with the problems and solutions being offered. The better you tailor this, the less thought is required to understand why your solution is valuable. In addition, address the following:

- show your understanding of the market size, the addressable market within it, your realistic chance of gaining a share and how big that share might be;
- show you know your market by presenting good-quality data and analysis, with reliable sources quoted; and
- highlight any indicators of where you have gained traction; e.g. customer reference sites.

5.3.1.3 Giving an overview of the market is an opportunity to build your credibility and show that you understand why your solution is needed. It is also a great opportunity to align your thinking with that of your potential partner and set the scene; your partner may use this as an opportunity to upskill those in his organisation who are less familiar with the problems and solutions being offered.

5.3.2 Common pitfalls

Not understanding your partner's market and share (i.e. which specific segments they serve), can lead to exaggerated evaluation of benefits for partners

5.4 Competitive positioning

5.4.1 The basics

5.4.1.1 The basics of competitive positioning are as follow.

- articulate your competitive space;
- when comparing to competitors, make clear on what dimensions you are better or worse.

5.4.1.2 Articulating your competitive space is a great indication of whether you understand your market. Try to understand where else your potential partner might be looking for solutions and explain how you differentiate. Few things are unique, so do not try and pitch yourselves as such. When comparing, remember that price and adaptability are equally valuable as well as product quality. Do not be afraid of offering solutions in the same space as established institutions as there are very few 'new' markets; problems often have a range of solutions.

5.4.1.3 When comparing to competitors, make clear on what dimensions you are better or worse, being clear about the current operations and product state (rather than any future road-map). If you only try and show areas where you believe you excel, you will reduce the overall value of your analysis. This is classically demonstrated by companies that use testimonials rather than all available feedback on their websites.

5.4.1.4 A fintech's initial engagements with a potential partner might relate to pilots or small rollouts rather than enterprise-wide deployment. Think about how you can appropriately position yourself to be selected for the work being offered, rather than the work you would like to win.

5.4.2 Common pitfalls

Common pitfalls in this area include:

- not highlighting differentiating factors – most banks will have significant search capabilities and will have a good understanding of the market so fintechs should highlight what makes their proposition unique;
- claiming you have no competitors without solid evidence and explanation to back this up;
- not demonstrating a longer term view of the market;
- expecting your potential partner is always look for solutions – it would be expected that the fintech will appreciate that most solutions have alternatives and sometimes those are maintaining a status quo, which can include doing nothing.

6 Business and team

6.1 General

The people involved in the collaboration are as important as the technology itself. The financial institution will therefore be interested in understanding the team make-up, key individuals and insight and the intellectual capital within the start-up.

6.2 Team make-up

6.2.1 With regards to team make-up, the fintech should address the following points:

- who holds key roles, including ownership of the company?
- what is the team size and organisational structure?
- what resources would be assigned to the engagement?
- where are people located geographically?
- who are the key people and brief resumes?
- illustrate the depth of insight and specialist knowledge of individuals with key skills.

6.2.2 Employees of fintechs who provide goods and services and who will be provided with unaccompanied access to premises, systems or information should have had their identity and probity for employment established (e.g. right to work, residency and activity).

6.2.3 The fintech would normally be responsible for completing screening/checks in accordance with the screening requirements detailed in their contract before the fintech's employee can provide goods or services to the Institution; and on an ongoing basis during the life of the contract. The screening process should be documented and sample checks might also be undertaken by the financial institution.

6.2.4 The fintech would be responsible for ensuring any sub-contractor screens its staff in line with requirements specified by the financial institution. All obligations on the fintech will flow down to any sub-contractor working on behalf of the fintech.

NOTE *Particular attention should be given to any legal or regulatory requirement such as access and audit, data protection and information security.*

6.3 Development model

6.3.1 Fintechs should be able to communicate the mid-term business plan of the company and how much of the development of the service will be handled in house, compared to outsourcing.

6.3.2 Understanding the mid-term business plan can help the financial institution to see if the fintech has a credible plan to grow and sustain itself as an independent company, or if it plans to be acquired in the mid-term. Change in future ownership or a strategy leading to a change of positioning at a later stage can inform decision making about an engagement relationship after the current project is delivered.

6.3.3 The financial institution will typically want to understand what work is outsourced, and to what company, in order to manage its risk efficiently.

NOTE *For example, a financial institution will want to check that any liability is covered with the same level of standard between the fintech and its suppliers, than between the financial institution and the fintech. There are sometimes specific aspects, for ex on Customer Data Protection, where the jurisdiction of the fintech's supplier will be key ingredient of the decision making (e.g. customer data processed in the UK, in EU, outside of EU).*

6.4 Branding

6.4.1 It should be established at the outset whether the final product will be branded by the fintech itself, co-branded with the financial institution, or distributed as a white-label product.

6.4.2 Having these discussions upfront prevent structural issues from surfacing at a later stage in the project. Different financial institutions have different approaches on branding so all options can be discussed.

NOTE *For example, white label, light branding e.g. "powered by fintech X in the small print, fintech X brought to you by financial institution Y.*

6.4.3 Any use of the financial institutions brand marks, in marketing on websites or in presentations or pitch decks will likely require express permission. It is likely that where the product/service is being tested (PoC stage), the financial institution will not want or agree to any publicity.

6.5 Advisors and investors

6.5.1 The financial institution will be interested to understand whether the fintech has an advisory board and, if so, who its members are. This can give further credibility to the capabilities of the fintech, particularly those that are earlier stage.

6.5.2 It will also be of interest from the perspective of identifying any potential conflicts of interest (see **7.4**).

6.5.3 Any investors in the start-up will similarly be of interest, including the stake held and any special terms that may apply.

7 Legal, regulatory and commercial

7.1 General

It's paramount for fintechs to understand the structure of the agreements they are entering into. At the same time, the financial institutions should only engage with fit and proper companies as they have various regulatory obligations to be satisfied.

It is highly likely that the general agreement/contract is a baseline for best known practices, and might not be fully aligned to a fintech environment or such governance models run by fintechs. Negotiation and education is key to a successful agreement, for both parties, ensuring you are comfortable with the obligations set out in the agreement/contract.

7.2 Non-disclosure, PoC and pilot agreements

7.2.1 General

7.2.1.1 When financial institutions consider entering into an engagement with a fintech there are usually requirements to draw up appropriate legal agreements between the two parties. Often these agreements are 'mutual', meaning there are restrictions and protections afforded to both the financial institution and the fintech.

7.2.1.2 There are a variety of requirements that financial institutions seek to cover which generally reflect the stage of the engagement. In broad terms these are:

- non-disclosure agreement – used during the qualification stage to set out the terms upon which confidential information will be disclosed and treated;
- proof of concept terms – used at the proof of concept stage to set out responsibilities and requirements, responsibilities and any financial considerations; and
- pilot terms – used at pilot stage. Similar to the proof of concept terms, but with additional requirements given the involvement of customers.

7.2.1.3 Most financial institutions have looked to streamline the process of working with fintechs and will have standard NDAs and agreements which enable engagements to be set up quickly, easily and cheaply. However, the fintech should check that they are comfortable with the terms they are signing up to.

7.2.1.4 Financial institutions will generally prefer not to sign agreements from the fintech.

7.2.1.5 If modifications are required to the financial institutions standard terms these will normally have to be reviewed and agreed with their legal advisers. The discussion and negotiations that can result between the legal advisors of both the financial institution and the fintech can be lengthy and the resultant legal costs can escalate quickly.

7.2.1.6 Similarly, if the financial institution were to agree to use the fintechs legal agreements, this often results in changes to, or additional terms being, requested. Again these legal discussions can lengthen timescales and come at a significant cost. A way to shorten the amount of time this might take, would be to ensure relevant stakeholder (in addition to lawyers) are involved in discussions and that changes made are tracked and visibly auditable to both parties. Make sure that these discussions are decision driven and that action and comments are actively closed in these discussions.

7.2.1.7 It is recommended that the fintech should take independent legal advice before signing any agreement and they should only sign if they are willing to be legally bound by the terms.

7.2.1.8 Each party will normally be required to meet their own legal costs.

7.2.2 Non-disclosure agreement

7.2.2.1 A non-disclosure agreement (NDA) is a legal contract between two parties that defines and protects how intellectual property, proprietary or confidential material and information can be used and shared. It is sometimes also referred to as a confidentiality agreement. An NDA is usually mutual in nature covering both parties and is required to allow in-depth discussions of interest to be entered into. During the course of those discussions, each party may have access to, or have disclosed to it, confidential information of the other party. The NDA sets out the terms upon which their confidential information will be disclosed and treated.

7.2.2.2 The NDA normally covers:

- specification of the legal entities entering into the agreement;
- definitions and meaning of key terms within the agreement;
- undertakings relating to confidentiality and restrictions of use;
- exceptions where restrictions and obligations do not apply; or where disclosure is required by law or other legislation e.g. to HMRC;
- the term for which the agreement and terms apply;
- the measures which each part should take to protect information, including aspects such as copying, storage and deletion;
- reservation rights relating to any confidential information, copyright, patent or other intellectual property rights;
- treatment of the information of any third party involved;
- other miscellaneous terms which might include aspects such as: giving of notice, loss or damages, assignment to third parties, variation to the terms and the definition of escrow;
- a statement that the agreement will be governed by and interpreted in accordance with the laws of England & Wales and the Parties submit to the jurisdiction of the English courts. If this is not to be the case specialist legal advice and terms will be required; and
- signatures of authorised signatories, name, title and date the agreement was signed.

7.2.3 Proof of concept and pilot terms

7.2.3.1 Once engagement initiatives move beyond initial conversations around use cases and feasibility, there may be a requirement to put into place legal agreements covering the scope, purpose and commercial terms for the engagement. For a proof of concept, this will include access to various technology environments and test data, and for pilots further controls and protections, including various security, compliance and data security checks will need to be done, given access will be granted to a subset of customers.

7.2.3.2 Whilst these terms are normally less wide-ranging than a full scale engagement agreement, the fintech will normally need to progress through an acceptance process that ensures appropriate due diligence, governance and contractual protection is in place covering aspects outlined within the clauses of this PAS.

7.2.3.3 The purpose of this process, from the financial institutions perspective is to ensure delivery of the new service does not materially impair the quality of controls, the relationship and obligations towards customers, and the compliance with various regulatory and sustainability responsibilities.

7.2.3.4 Engagements with any third-parties, including engagements with fintechs, is normally subject to a formal written agreement based upon the financial institutions standard contracts.

7.2.3.5 In the event that material changes are required to the standard clauses, or if the use of the fintechs terms and conditions is unavoidable, it is likely that there will be the requirement to engage both legal and other specialist teams (e.g. procurement) to review and agree the terms, as well as due diligence from teams such as IT Security.

7.2.3.6 The discussion and negotiations that might result between the legal advisors of both the financial institution and the fintech can be lengthy and the resultant legal costs can escalate quickly.

7.2.3.7 It is recommended that the fintech should take independent legal advice before signing any agreement and they should only sign if they are willing to be legally bound by the terms.

7.3 Company legal structure and conduct

7.3.1 Financial institutions are committed to acting with integrity, fairness, due skill, care and diligence in all business dealings and commercial relationships. They will therefore be interested to undertake due diligence around the legal structure and set up of the fintech including identification of holding companies, subsidiaries and other related companies. Most financial institutions will not deal with non-incorporated entities.

7.3.2 The financial institution will likely have a zero tolerance to actions and activities that knowingly breach legal or regulatory requirements. Accordingly, they will want to ensure that there are no aspects relating to the fintech which disregard appropriate controls, activities or processes relating to:

- anti-bribery and corruption laws and regulations;
- anti-money laundering, tax avoidance or terrorist financing laws and regulations;
- sanctions relating to restricted countries or individuals; and
- regulatory rules and requirements.

7.4 Conflicts of interest

7.4.1 A conflict of interest is a situation in which the concerns or aims of two or more different parties, if not managed, are incompatible. Financial institutions conduct business on the principle that they identify and manage conflicts of interest fairly and effectively. The financial institution will therefore seek to have procedures and controls in place to identify and manage any potential conflicts of interest. This may require segregation of employees if the fintech is working on confidential projects for more than one financial institution.

7.4.2 The financial institution will be interested in understanding any relationship between the financial institution and the fintech, including key personnel on both sides, financial holdings or beneficial interest to ensure any engagement has been introduced, selected and contracted with integrity and transparency to avoid the perception of, or actual:

- bribery, corruption, questionable conduct, seeking to obtain any improper influence;
- advantage obtained as a result of the giving or receiving or gifts, hospitality and entertainment by any of its employees or third parties; and
- breach of any law, regulation, code or policy.

The fintech should ensure that any interests that might not align with the financial institution are disclosed upfront (for example that a competitor personnel sits on their board).

7.4.3 If there has been significant media coverage relating to key individuals within or the fintech itself, these should be disclosed.

7.5 Company financials

7.5.1 Financial institutions will be interested in understanding the ongoing financial viability of any fintech it is seeking to engage with, particularly if the product or service relates to a business critical or customer activity. The financial institution will therefore seek to undertake a reasonable level of financial due diligence to provide peace of mind that the fintech is financially viable by analysing and validating its financial position.

7.5.2 It is recognized that fintechs might still be relatively early stage and therefore seek to put into place arrangements to protect service to customers or to the financial institution. Given early stage fintechs may not pass financial criteria required it may therefore be necessary to put in place insurance or escrow arrangements in the event the fintech can no longer meet agreed support arrangements so that the financial institution can directly pick up support.

7.5.3 The financial institution will likely be interested in understanding financial viability in terms of:

- capital availability, funding stage and sources;
- existing revenues and debts;
- profit and loss account, and balance sheet;
- cash flow;
- existing engagement commitments;
- resourcing levels; and
- financial forecasts and growth/scaling plans.

7.5.4 Credit rating reports might be sought as part of a broader appraisal, but it is unlikely that these would be used as a sole assessment tool.

7.6 Commercial model

7.6.1 The financial institution will be interested in understanding the commercial terms on which the fintech is seeking to engage, including the proposed use, by either party, of brand marks or marketing collateral associating the organisations.

7.6.2 Considerations regarding commercial model will include aspects such as:

- proposed pricing model e.g. per transaction, user or enterprise level;
- revenue share;
- license fees to be charged;
- services levels and cost tiers, if costs change by volume or other factor;
- support arrangements and service level agreements, including third parties used and associated costs;
- protections, guarantees and/or indemnities expected or given;
- responsibility for any liabilities; and
- penalties relating to non-performance.

7.6.3 It is recommended that there should be flexibility to how pricing is presented to the financial institution, each may have different preferences on how to pay e.g. flat fee vs per use – having multiple models can be helpful in this case

7.7 Intellectual property agreements

For fintechs where entire businesses are often based on a single technology developed for a specific purpose, intellectual property is one of the biggest legal considerations when it comes to working with financial institutions. As such, it is vital to have a complete understanding of how the two businesses will work together, and to be very clear upfront about:

- what intellectual property already exists;
- who owns the existing intellectual property;
- how existing intellectual property might be used by each party, and on what terms;
- who will own any new intellectual property created as a result of working together;
- how intellectual property might be combined, where necessary; and
- where the fintech has licensed intellectual property rights from or to a third party, that it has the appropriate rights to sub/re-licence freely to the financial institution. Any restrictions should always be disclosed at the initial stages of the process so there are no surprises.

7.8 Fraud prevention

7.8.1 The financial institution will be interested in understanding supplier scenarios/responsibilities which relate to fraud risk. This may be applicable when:

- introducing customers/clients/employees to the financial institution;
- processing transactions of money and/or information or transactional items;
- collecting/handling/storing/transmitting classified information (including customer data); or
- supplier has remote access to infrastructure & can change or view static data.

7.8.2 There is also likely to be a review held on a periodic basis to reaffirm appropriate controls are in place.

7.9 Business resilience

7.9.1 The financial institution will be interested in understanding the fintech's scenarios/responsibilities where it provides goods or services which, if lost, would disrupt one or more critical activities, and if their services/goods cannot be readily sourced from other suppliers within an acceptable timescale. Such scenarios/responsibilities can include:

- responsible for supporting or maintaining equipment or systems processing any information whether on-site or off-site;
- responsible for supporting or maintaining facilities or infrastructure containing or processing any information whether on-site or off-site; or
- where provision of the goods or service is essential for continuation of service to the Institution and its customers.

7.9.2 The fintech should have business resilience plans in place in case their premises/staff fail to enable them to continue to operate and supply the financial institution with the contracted service or product within an acceptable recovery time.

7.9.3 The financial institution will want to understand the fintech's business resilience and disaster recovery plans and any related test results. This should include:

- testing schedule;
- risk assessment;
- defined recovery roles;
- contact information;
- invocation procedures; and
- data recovery plans.

7.9.4 Consideration should be given to detail and evidence recovery capability for any services where the fintech has outsourced the service to a third-party. The fintech should be able to demonstrate and evidence that any services outsourced to a third-party have disaster recovery plans in place.

7.10 Regulatory compliance

7.10.1 Financial institutions are subject to a mass of industry-specific regulation that is constantly being revised and updated. In comparison, there is no specific 'fintech regulatory framework', and instead the regulations which apply can depend on a fintech's business activities. Certain changes have already been made to the UK regulatory framework in response to the growth of fintech, such as specific regulations for peer-to-peer lending – a form of crowdfunding – and further change is likely in the future.

7.10.2 Fintechs often work on the edge of the financial services industry, and might therefore have limited exposure to regulatory scrutiny prior to the roll out of a product. But they and their financial institution (which are likely to have a sophisticated regulatory understanding) will still need to ensure that any regulatory requirements that apply to the fintech are taken into account. For a fintech, it is important to understand the financial institution's likely concerns, and the financial institution should be clear about what it requires from the fintech and engage on regulatory concerns early in the relationship. This might include the need for regulatory approvals and/or notifications in a mergers and acquisitions context, or structuring joint venture arrangements in compliance with rules on outsourcing. While this can be a slow process, it is an integral part of bringing a fintech's product to market. Early and productive engagement and the persistence to see the process through should ensure that everyone stays on the right side of the regulations.

***NOTE** Regulatory obligations are likely to result in some degree of contractual complexity.*

7.10.3 Fintechs should be able to provide confirmation of:

- relevant FCA/PRA authorisation and relevant permissions held or confirmation of application to regulatory bodies;
- what regulatory rules, guidance and laws apply to activity; and
- no outstanding regulatory enforcement action or investigation.

7.10.4 Additional points for fintech's offering customer facing products/services either directly or indirectly to consider:

- confirmation of what customer facing products/services are to be offered;
- assessment of the complexity of the products/services and any customer groupings they might be unsuitable for;
- view on what types of customers the products/services are aimed at;
- viewing of all customer facing screens in the customer journey.

7.10.5 Additional points for fintech's trading live with actual customers:

- examples of customer feedback with the best summary available;
- ratings from consumer rating organisations or consumer bodies where available;
- where relevant a summary of complaints statistics showing most complained about areas, root causes and resolutions;
- where relevant a summary of any remediation activity undertaken;
- where relevant a summary of press reports both positive and negative;
- ratings on usability, accessibility and security confidence.

7.11 Other ethical policies

Depending on the solution there may be other policies or requirements that the financial institution will be interested in. An example of this is sustainability policy, as many financial institutions will be committed to sustainable sourcing. A sustainability policy will include economic, ethical (social) and environmental considerations.

As a minimum requirement, suppliers will likely be expected to adhere rigorously to all relevant human rights, labour, health and safety and environmental laws. The fintech would also be expected to apply any policies the financial institution have committed to, e.g. living wage vs minimum wage and this is extended to any suppliers the fintech may use.

8 Information security and data protection

8.1 General

There is a need to ensure that both customer data and the financial institutions data are safe and adequately protected through appropriate physical, procedural and technological protection and controls.

8.2 Information security, back-up and archiving

8.2.1 The financial institution will be interested in understanding the activities and responsibilities of the fintech in the following areas:

a) capturing, creating processes for storing, or disposing of records, customer transactions, data or assets either on the financial institution's premises or at an offsite location;

b) handling information created, processed, transferred or collected by, to or from the fintech; where the data is one or more of the following:
   1) employee personal data;
   2) sensitive personal data;
   3) mergers and acquisitions;
   4) financial information;
   5) has a significant effect on the financial institution's balance sheet;
   6) customer personal data;
   7) customer financial data;
   8) data concerning the security of the financial institution's assets; or
   9) payment card or transaction data.

c) supporting or maintaining equipment or systems processing any financial institution information whether on-site or off-site;

d) supporting or maintaining facilities or infrastructure containing or processing any financial institution information whether on-site or off-site; and

e) having remote access or connectivity to the financial institution's infrastructure, or access to their data or premises.

8.2.2 Requirements and are often aligned with the international information security standards Service Organisation Control (SOC 1/2/3) compliance, ISO27001 and ISO27002. This will include the need to have documented security polices for the:

- solution;
- security design for products (e.g. security testing);
- ownership of security policies including segregation of duties;
- independent security testing on periodic basis;
- periodic audits across legal & regulatory requirements; and
- security review and risk assessments of any 4th parties.

8.2.3 Where the service is of particular significance in addition to any pre-contract review, the fintech may receive ongoing assurance checks, carried out on a periodic basis. The purpose of this review is to confirm that the service still continues to meet the financial institutions requirements taking into account the risk profile of the service and assessing if there has been a material change in the service or in the supplier.

8.3 Payment security

8.3.1 The financial institution will be interested in understanding the activities and responsibilities of the fintech where they undertake any aspect of the end to end payment process, including:

- accessing payment systems; including access to the Institutions payment systems and passes debit or credit entries over the Institutions bank accounts;
- authenticating customer instructions;
- debiting the financial institutions bank accounts; and
- initiating manual or electronic payments on behalf of the Institution.

8.3.2 Where Payment Card Industry Data Security Standard (PCI DSS) is a requirement, there will be a need to understand if the fintech has to be registered with the respective card schemes and ensure any required registration is completed prior to contract commencement.

8.4 Physical security

The financial institution will be interested in understanding the activities and responsibilities of the fintech where they have:

- access to, manage, processes or store the Institution's assets; or
- unescorted access rights to the Institution's premises.

This will include the fintech clearly demonstrating understanding of activities for outsourced activities, including but not limited to any sub-contracted/ contracted hosting, or other facilities partners, including cloud providers.

8.5 Access rights and controls

The financial institution will be interested in understanding the activities and responsibilities of the fintech in terms of:

- technical and support personnel having administrator or special access rights to systems and data relating to the financial institution's deployment of a solution;
- how identity, rights and privileges are appropriately monitored, controlled and audited; and
- how joiner, mover and leaver access within the fintech is governed; and
- insider threats e.g. user access management to protect from toxic combination (separate roles for data entry and auditing) and access to data which unauthorised individuals shouldn't have.

8.6 Data protection

8.6.1 General data protection regulation (GDPR)

*COMMENTARY ON **7.6.1***

On 25 May 2018, a new EU regulation came into force that has an impact on how an individual's personal information is accessed, processed and managed. The GDPR brings a new era in safeguarding personal information and guaranteeing that businesses take greater responsibility for the role they play. GDPR will furthermore provide high level guidance on the requirement to protect personally identifiable information (PII).

Fintechs will be required to evidence that they and any third parties they use are fully compliant with the requirements of the GDPR.

***NOTE** Full definition and requirements can be found on the EU GDPR (www.eugdpr.org).*

As such this section provides an overview rather than an exhaustive checklist of regulations and requirements.

The agreement with the financial institution will normally contain extensive GDPR/data protection (DP) clauses within it to cover these DP obligations.

The financial institution will be interested in understanding the activities and responsibilities of the fintech where a supplier has access to any data, however stored, (including electronic data, systems and printed records and confidential waste) relating to:

- potential or actual customers/clients/users;
- staff (including contractors, job applicants, pensioners, etc.); and
- shareholders.

The GDPR replaces the existing data protection laws across the EU which governs the use of personal information. Personal information is any information from which an individual can be identified or singled out either from: the information on its own (such as their name); or from two or more combined pieces of information (such as their address and date of birth). It includes all information, including expressions of opinion about a person, whether held in electronic form or structured paper files.

The GDPR increases and strengthens the rights of individuals in relation to the information held about them:

- individuals can already request to see the personal information held on them (this is called a subject access request) and can ask for inaccurate data to be corrected or to update incomplete data.
- under certain circumstances, they can also request to stop processing their data or delete it completely.
- under certain circumstances, they can also request an electronic copy of their data or have it sent to another provider (this is called "data portability").
- the financial institution is required to process and respond to these requests within thirty days of receipt, free of charge. It will therefore be necessary for the fintech to demonstrate that they are able to support the financial institution in meeting these obligations.

8.6.2 Privacy impact assessment (PIA)

A PIA is a legal requirement under the GDPR for any activity which involves the 'processing' (e.g. access, use, store, transfer etc.) of personal data which could result in a high privacy risk to the individual whose data is processed; and/or a policy requirement for any data collected from customers (whether corporate or individual client) in the course of business relationships.

A PIA is an end-to-end risk assessment of the privacy issues within a new or changed, process, product or project. Engagement between a financial institution and a fintech will likely require a PIA to be undertaken.

It will help identify privacy risks throughout the lifecycle of a project, product or service and help influence the design of processes and products in order to mitigate or reduce legal risks (e.g. reducing level of regulatory fines) and operational risks (e.g. remediation, the costs of putting these right).

8.6.3 Client consent

Under the GDPR, there will need to be a legal basis before personal data can be processed. One such legal basis is to obtain the consent of the data subject. The standard for consent is high and requires a form of clear affirmative action. Silence, pre-ticked boxes or inactivity is not valid consent. Individuals have a right to withdraw consent at any time and systems and processes should facilitate this. Generally, financial institutions limit the reliance on consent and where possible will rely on other legal bases, e.g. where they have a legal obligation to process the data or are required to process it under the contract with the customer.

Fintechs will have to state whether client consent will be necessary when utilising their proposed solution.

8.6.4 Privacy notices

The fintech will be required to have appropriate privacy notices with clear information about how they process personal data.

8.6.5 Breaches

In some jurisdictions, financial institutions have a legal duty to report personal data breaches. Within the EU they have to report personal data breaches to the regulator (e.g. the ICO in the UK) within 72 hours of becoming aware of the breach.

The fintech will need to be able to demonstrate that they are able to respond and escalate any data breaches within timescales and requirements of the regulation.

The financial institution will be looking to the fintech to ensure regulatory compliance and collaborate closely with them to allow the financial institution to ensure customers and their data are protected. This includes providing the earliest possible warning where applicable.

8.6.6 Personal data rights of customers under GDPR

At a high level, customers have the following rights:

- the right to be informed (What information are you collecting about me, why and who can see it?);
- the right of access (How can I see my data?);
- the right to rectification (I would like to change something);
- the right to erasure (The right to be forgotten);
- the right to restrict processing (Please do not do that anymore);
- the right to data portability (Let me have my data, I want to take it to someone else);
- the right to object (Stop doing that);
- rights in relation to automated decision making and profiling (what decisions have you made that stop me doing or getting something).

The financial institution will therefore likely seek to:

- identify what data the fintech will have access to and for what purposes;
- clarify if the fintech will be processing the data on behalf of the institution as a data processor for them;
- understand from a business and legal perspective if there is any proposal that the fintech will use the data for its own purposes or for a third party;
- identify whether the data will be transferred to the supplier or to another party, e.g. another company in the supplier's group or another sub-contractor;
- identify which countries the data will be transferred to or accessed from; and
- ensure that the data protection, confidentiality and sub-contractor clauses and any specific data security controls are included in the contract.

8.6.7 Confidentiality

The Institution will also seek to protect its own confidential and secret information about their:

- businesses;
- finances;
- strategy;
- risk positions;
- corporate plans; or
- regulatory information.

8.6.8 Data encryption

Most financial institutions will be interested in understanding how and by what techniques data is encrypted at rest and in transit. They will also seek to understand what data the fintech can access and what data they cannot access (e.g. customer encryption keys).

8.6.9 Data transfer agreements (DTA)

Where personal or other customer/client data will transfer across international borders or be processed on a "cloud" basis, there may be restrictions on data transfers and the ways in which this can be done lawfully. Where required, an appropriate DTA or modified contract clauses will need to be in place before any data transfer takes place.

8.6.10 Contractual disclosure

There will be a need to ensure data categories, flow of data, destination country, data recipient, data processing activities and data security requirements are documented and agreed in the contract(s).

NOTE *This might require the information provided to the fintech, to enable them to supply the service, to be anonymised or aggregated.*

8.7 Records management

8.7.1 The financial institution will be interested in understanding the activities and responsibilities of the fintech which cover creating, using or storing and deleting the institution's records, such as:

- creating records: capturing, creating, and keeping records, data or information either on the financial institutions premises or at an offsite location;
- storing records: storage of records, data or information, particularly noncurrent records in off-site storage warehouses (used for archiving paper records, and the storage of backup tapes or disks;
- using records: where records, data or information are transferred to the custody of the fintech to enable them to provide services; or
- deleting records: where records, data or information are no longer required for the work and are not subject to a legal hold, at the financial institution's discretion they should be permanently and securely destroyed.

8.7.2 Details will need to be specified of how records will be managed, stored and maintained; and what will happen to the records if and when the contract expires or is terminated.

9 Technology

9.1 General

For a technology collaboration to be successful there is a need to understand the technologies being applied, including controls and cyber-protection, how they can be scaled and the future road-map and support arrangements.

This will include requirements for system/services resiliency and any impact to possible environments that hold more than one customer/financial institution (also called multitenancy).

The fintech needs to recognise that the affiliation with a financial institution may in itself make them a target by malicious parties. They should therefore be willing to evidence considerations of this kind, and how they provision for such concerns.

Reputation is a very important concern and there may be requirements to protect against adverse impact on their brand or customer trust in the institution. Financial institutions might therefore require the fintech to adhere to internal social media policies, or at a minimum ensure they have capability in-house to protect against relevant risks.

A financial institution is likely to require involvement in any breach or incident review, and might conduct their own audit after the incident. It is prudent for the fintech to provision for this.

9.2 Platform readiness

9.2.1 The readiness of the fintechs product or platform will help to drive the type of the discussions being had with potential partners. The fintech should be clear about the current state of the product or service that is being or has been developed. Typically a financial institution will look to tailor their engagements depending on the maturity of the product or service. Typical states of development are:

- **pre-alpha** – Idea stage with some elements of the product proven, but not wholly working in a coherent package.
- **alpha** – Product is in a somewhat working state and can be demoed in private, some public materials may be available but this is not ready for use outside of the fintech in an unguided manner.
- **beta** – Product is relatively stable and is ready to be tested at a PoC level by customers, however a number of issues will be expected to remain.
- **MVP** – Product has a minimum set of features that may be considered ready by potential customers to either test or release to customers based on their own evaluation of the product.
- **market ready** – Product is ready and while may have limited use should be considered ready to deploy at production scale.
- **live production** – Product is market ready and has successful deployment, at scale by one or more customers and is proven within the market.

9.2.2 It's important to be clear on the maturity of the product as this will help drive the appropriate level of engagement. Additionally, expected key milestone releases of when future states are expected to be reached should be included in a product roadmap (see **9.4**).

9.2.3 Whilst fintechs should be careful not to breach any NDAs that they may have with other customers, being able to share numbers of users, deployments and countries in production will all be important in showing the maturity of the technology.

9.2.4 Where a product is being proposed or created from a previous iteration, it can engender confidence in the technology by emphasising that the new product is a development of an original product. This will help give confidence in the maturity of the underlying solution while highlighting the offered product is still under development.

NOTE *For example, an existing product might be in Live Production while the new product (e.g. a customizable white label version tailored at the financial sector) may only be in Beta as you are looking to gain feedback from the industry*

9.3 Technology architecture

9.3.1 It's important to be clear up front about the architecture of the solution, for wider deployments of a solution this will required detailed discussions and understanding from a number of SMEs within the financial institution. This information should be documented in detail along with high level architecture diagrams showing system connectivity as well as data flow. An architecture diagram, should also detail differences between, development, test and production services.

9.3.2 Items to cover when detailing your technical architecture will include:

a) Deployment type– What are the deployment options for your solution? e.g.:
   1) on premise – technology stack required;
   2) software install – minimum requirements; or
   3) SaaS/PaaS, hybrid cloud, IaaS or other.

b) Cloud – Which cloud providers do you support? If not cloud agnostic, or a single cloud is supported, the technical rational behind this will be useful in any technical reviews of the solution.

c) Which services for each cloud provider do your solutions require?
   1) Each financial institution will have opinions on which services are appropriate for use on types of customer data and could vary depending on region;
   2) Geographic data residency will need to be understood. Which "availability zones" can your product run from, and the location of your production and contingency zones;
   3) Financial institutions are likely to carry out additional due diligence in relation to cloud deployment.

d) Third party products and technologies used with the solution:
   1) Which other technologies will the solution require to run, particularly key for solutions where the financial institution will be able to host themselves;
   2) Include versions supported and tested against which will need to be understood for the purposes of regulatory requirements.

e) Open source software – What open source software is present in the solutions?

f) Integration options:
   1) plug-ins to major platforms;
   2) APIs - Are these RESTful (which are generally preferred)? API documentation should be available;
   3) out of the box connectors;
   4) data feeds.

g) Shared or dedicated services – as part of the service will the infrastructure be dedicate to the specific financial institution or shared between multiple customers.

9.4 Development roadmap

9.4.1 When engaging in discussions around a long term engagement with a financial institution, they will want to be comfortable that they understand the direction of the solution during the proposed period of the contract. The roadmap should be in as much detail as possible over the near term (6-12 months) with an indication of future direction beyond this. If the contract is strategically important then the financial institution may desire discussions around prioritising certain developments. These should be held periodically, ideally every quarter, and updated to the roadmap.

9.4.2 As part of the roadmap a clear documented policy on change control, notice of feature changes or demising functionality should be stated. Removing key features, changing features or introducing significant new functionality could be covered by any contract ensuring notice is given in a timely manner as the financial institution may require lead times in order to secure resource to implement or support any changes from their side.

9.4.3 The road map should include changes to the product being provided, control based investment (e.g. cybersecurity) as well as expected changes to the underlying technology to ensure any platforms or technologies the product requires are both current and in support.

9.5 Support arrangements

9.5.1 Detailing any formal support arrangements that will come with your product or service will be important to gain confidence, particularly where the fintech will be responsible for hosting the service.

9.5.2 Items that should be considered when detailing support arrangements include:

- what is the expected uptime and SLA for any hosted products and when are release windows scheduled/ updates applied?
- what are your change control/troubleshooting support procedures?
- what is the process for a customer to raise an issue with the product?
- what is the expected time to acknowledge/confirm reported issues and does this vary depending on severity indicated by the client?
- what is the expected fix time once an issue has been logged and verified?
- do you offer 24/7 365 support for production services if so how are this supported e.g.:
  a) staff on-call and agreed response times;
  b) "follow the sun" support from multiple locations;
  c) support agreements with fourth parties.
- for services that are hosted by the fintech, what capabilities have you in place to monitor the health of the system and alert support and when potential issues occur?
- can the alerting be made available to the financial institutions?
- if not how will you inform the financial institution when outages have been identified?
- 24/7 monitoring and incident management capability;
- direct point of contact, available 24/7 for any events and breaches concerns.

9.6 IT Resilience

9.6.1 The financial institution will be interested in understanding the fintech's scenarios/responsibilities where it provides IT solutions or services which, if lost, would disrupt one or more critical activities, for example:

- an understanding of the end-to-end testing strategy, not only for the IT Solution, but testing on how the solution integrates with other financial institution systems;
- managing or operating all or part of a key IT service on behalf of the financial institution;
- supporting or maintaining equipment or systems processing any information whether on-site or off-site; and
- supporting or maintaining facilities or infrastructure containing or processing any information whether on-site or off-site.

9.6.2 Usually an IT resiliency review is undertaken as part of any wider business resiliency review.

9.6.3 Key items that should be covered in an IT resiliency review are:

- Recovery point objective – Following a significant fault or failure on your production service how much data would be lost by restoring from a backup. More important services will require less (or in some cases no) data to be lost.
- Recovery time objective – How long does it take from a live service outage to be fully running on your contingency/backup site? More critical services will require this be a quicker time.
- Frequency of resilience testing – How often do you test your resilience and recovery plans and when was your last test, what were the outputs you can share?
- As part of contingency testing, do you run you live service from your contingency environment for a period of time?
- Results and frequency of performance testing – what performance/load testing has any hosted service been through to show confidence the solution can scale to large number of users?
- Resilience built into service design – where possible resilience should be built into the production service so faults in specific layers of the infrastructure do not result in outages. Clearly documenting these layers in your architecture documentation will be critical to gaining confidence in your solution being ready for a large scale deployment.

Annex A (informative)
The fintech toolkit portal

The Fintech Delivery Panel is developing a portal of documents and examples to sit alongside this PAS to provide fintechs with a further source to inform and support them through the engagement process.

The portal can be found here: https://technation.io/resources/fintech-collaboration-toolkit

Annex B (informative) – UK regulatory support

B.1 General

UK policy makers have publicly voiced their intention to establish, maintain and enhance the UK as the leading centre for fintech. This innovative stance is mirrored by regulators, who have sought to assist businesses in bringing new financial products and services to the UK markets. For example, in October 2014, the Financial Conduct Authority (FCA) began 'Project Innovate', in which the regulator offers direct financial regulation support and advice to fintechs. As part of Project Innovate, the FCA offers a 'Regulatory Sandbox', where fintechs can operate in the open market on a limited scale, and the FCA Direct Support internet portal benefitting from the FCA's guidance, regulatory waivers and 'no enforcement' relief during the process. Therefore, as fintechs work increasingly within the core of the financial services industry, they and their FSI partners, should try to ensure that they – and any products and services they develop – take advantage of the regulators' progressive stance, as well as complying with all relevant regulations.

B.2 FCA direct support

https://www.fca.org.uk/firms/innovate-innovation-hub

Through their Innovation Hub the FCA encourage and support innovation in financial markets and ultimately promote effective competition. The Direct Support Team provides a dedicated contact for innovator businesses that are considering applying for authorisation or a variation of permission, need support when doing so, or do not need to be authorised but could benefit from our support.

The FCA can also help businesses understand our regulatory regime and the challenges they may face when developing an innovative product or business model.

The FCA decides whether a request is eligible for support through the Innovation Hub using several eligibility criteria, which they review to ensure the fintech is appropriate:

a) Genuine innovation: Is the innovation ground-breaking or significantly different?
b) Consumer benefit: Does the innovation offer a good prospect of identifiable benefit to consumers (either directly or through greater competition)?
c) Background research: Has the business invested appropriate resources in understanding the regulations in relation to its own position?
d) Need for support: Does the business have a genuine need for support through the Innovation Hub? If you are eligible for Innovation Hub we will establish the most appropriate form of support, whether that involves assistance when applying for authorisation or otherwise. If your request is not eligible for Innovation Hub we will direct you to the most appropriate point of contact in the organisation.

B.3 FCA sandbox

https://www.fca.org.uk/firms/regulatory-sandbox

The regulatory sandbox allows businesses to test innovative products, services, business models and delivery mechanisms in the real market, with real consumers.

The sandbox is open to authorised firms, unauthorised firms that require authorisation and technology businesses. The sandbox seeks to provide firms with:

a) the ability to test products and services in a controlled environment;
b) reduced time-to-market at potentially lower cost;
c) support in identifying appropriate consumer protection safeguards to build into new products and services;
d) better access to finance.

The sandbox also offers tools such as restricted authorisation, individual guidance, informal steers, waivers and no enforcement action letters.

The FCA closely oversee tests using a customised regulatory environment for each test – including safeguards for consumers.

Sandbox tests are expected to have a clear objective (eg reducing costs to consumers) and to be conducted on a small scale, so firms will test their innovation for limited duration with a limited number of customers.

B.4 Bank of England fintech hub

https://www.bankofengland.co.uk/research/fintech

The Bank of England take a keen interest in exploring how innovation and developments in fintech might support their mission to promote the good of the people of the UK by maintaining monetary and financial stability.

In particular, they seek to understand what fintech means for the stability of the financial system, the safety and soundness of financial firms, and our ability to perform their operational and regulatory roles.

B.5 HM Treasury fintech sector strategy

https://www.gov.uk/government/publications/fintech-sector-strategy

The fintech sector strategy sets out action the government has taken to make the UK the best place for fintech business, and what it plans to do to maintain this position.

Annex C (informative) – UK Ring-fencing regulations

Ring-fencing is designed to protect the UK economy from crises in the global financial system. It separates essential banking products and services from higher risk activities carried out around the world.

It applies to UK banks with £25 billion of core deposits in the European Economic Area (EEA), which includes the European Union plus Iceland, Norway and Liechtenstein.

From a fintech's perspective it will be necessary to understand which legal entity is being contracted with. Engaging with both parts of the bank within and outside the ring-fence will likely add to the complexity of negotiations and governance requirements.

Figure C.1 – Ring-fencing

Annex D (informative) – What you can expect when engaging with Financial Institutions

When engaging with financial institutions, fintechs can expect to be treated with integrity and respect. The fintech can expect that the financial institution will:

- provide a clear definition of the requirements and needs the financial institution is seeking to fulfil;
- identify the key sponsors, decision makers and stakeholders;
- provide transparency over the process and timescales for actions and decisions;
- conduct the qualification and assessment process in a fair and honest manner, with openness and integrity, and in line with legal and regulatory requirements;
- respect non-disclosure agreements;
- provide clear and timely feedback on any decisions;
- promote the principles of inclusion and diversity;
- be committed to a sustainability policy including economic, ethical (social) and environmental considerations;
- set out their key controls covering operational, regulatory, legal and business risk;
- pay promptly and give clear guidance on our payment procedures;
- make whistleblowing channels available, to allow reporting of unethical conduct with regards to the relationship; and
- encourage and support improvement through collaborative working, develop improvement plans and encourage best practice standards.

Bibliography

Standards publications

BS EN ISO/IEC 27001, *Information technology. Security techniques. Information security management systems. Requirements.*

BS EN ISO/IEC 27002, *Information technology. Security techniques. Code of practice for information security controls.*

Other publications

[1] GREAT BRITAIN. The Computer Misuse Act 1990. London: The Stationery Office

[2] HM TREASURY, *Fintech Sector Strategy*. London: HM Treasury 2018

Websites

Bank of England (BoE): www.bankofengland.co.uk/prudential-regulation

Competition & Markets Authority (CMA): https://www.gov.uk/government/organisations/competition-and-markets-authority

EU General Data Protection Regulation (GDPR): www.eugdpr.org

Financial Conduct Authority (FCA): www.fca.org.uk

Fintech Delivery Panel Portal: https://technation.io/resources/fintech-collaboration-toolkit

HM Treasury (HMT): www.gov.uk/government/organisations/hm-treasury

Payment Card Industry Data Security Standard: https://www.pcisecuritystandards.org/pci_security/

Prudential Regulation Authority (PRA): www.prarulebook.co.uk

Ring-fencing: https://www.gov.uk/government/publications/ring-fencing-information/ring-fencing-information

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI, 389 Chiswick High Road
London W4 4AL
United Kingdom
www.bsigroup.com

ISBN 978-0-539-00165-5