Technology Provider Due Diligence

A guide for Community Finance lenders

Last updated: November 2023

Contents

Introduction

> 'The use of the right technology (or indeed the lack of it) will make or break the sector in terms of remaining relevant to the up-and-coming generations'
>
> Fair4All Finance, Understanding the role of technology in Community Finance

Information and Communications Technology, here after referred to as ICT, is ubiquitous for almost all commercial enterprises and is seen as a critical success factor for most organisations, especially those operating in the Financial Services sector. This ubiquity is recognised in the quote above reproduced from a survey, carried out in 2020 by Fair4All Finance, of the role of technology in the Community Finance sector.

This survey also identified significant levels of need in the sector for technological development and change:

- **93%** of providers expect they'll **need to substantially increase their technology** in the next five years - in many cases in order to survive
- **37%** of lenders **are undertaking or planning significant technology change**, with many looking at replacing their core technology
- **Funding is by far the main perceived barrier** to the sector optimising its use of technology, with insufficient capability and inappropriate products from suppliers behind in second and third place
- **70%** of providers **use open banking** for affordability and credit risk checks
- **43%** or providers are **collaborating with others**, while 26% aren't currently but would like to

The quoted survey also identified that the sector is short of technology capability and is overly reliant on incumbent and prospective suppliers for ICT support, development, and change.

Most financial service providers we surveyed are planning to increase the deployment of ICT in the next five years.

We have also heard from lenders that they are not as confident as they'd like to be appointing ICT providers. Effective procurement of ICT and associated services, subject to a set of robust controls, helps to make sure that technology investments achieve their objectives and that organisations with finite ICT budgets do not fall into the trap of swapping one form of technological debt for another.

ICT is also recognised as critical to the sector by various regulatory bodies and the use of technology is specifically referred to in key regulations.

The Appendix - Technology obligations on lenders in the regulations on page 27 sets out some of these obligations.

Thus, regulation already has a strong focus on ICT, and this is only set to increase as ICT capabilities further develop with innovations such as Artificial Intelligence and Machine Learning.

Purpose of this guide

This due diligence guide is aimed at providing outlines for a series of steps to take when procuring ICT, and to provide indicative factors against which to measure possible investments.

In most cases the advice offered here is understandably generic as the circumstances, capabilities, and needs of individual organisations will differ. However, we hope that the guidance, and templates, provided are easily adaptable to individual organisations.

This guide is designed to be used alongside external advice where organisations don't have the requisite skills in house.

This can be achieved in various ways from hiring in temporary consultants, placing consultants with the proposed vendor, drawing on the experience of members of the organisations' board, or recruiting permanent members of staff with the requisite skills.

If engaging external consultants, it is likely that they will bring their own methodology and artefacts which will supersede those provided with this guide, however the advice offered here is still relevant even if it is only used as a checklist against which to measure other work.

Scope of this guide

This guide covers the process of Due Diligence for ICT procurement including the initial Request for Information (RFI) and Request for Proposal (RFP) stages of a traditional procurements process. It does not mandate any stage and is meant for guidance only. Indeed, the RFI and RFP stages may not be appropriate dependent on the scale and nature of ICT investment being made.

Equally the guide is agnostic of the type of technology being procured. Whilst examples in this guide will refer to the procurement of a Core Banking System for illustration, it should not be read that this guide is only applicable to such a large and critical procurement. The principles expounded here are relevant to a wide variety of ICT procurement activities.

This guide will step through the process sequentially; however, it should be recognised that many procurement activities are not linear and that there may be levels of iteration for many of the stages.

Importance of Due Diligence

Due diligence is a vital part of the vendor management process and involves a comprehensive assessment of key measures of a technology provider including:

- Technological capability
- Financial stability
- Security
- Customer satisfaction ratings
- Compliance
- Contractual arrangements

Taken together and examined carefully these factors will assist Community Finance institutions in making critical and, often, significant financial investments in ICT providers and their systems.

Requirements analysis

Before any procurement activity commences it is vital that the key requirements to be addressed by ICT are understood and documented in some detail. This is a critical process in the procurement of any major ICT system. It involves identifying, analysing, and documenting the needs and goals of the organisation to ensure that the selected system, or systems, meets the specific requirements of the business.

It may be that, at an RFI stage in the process, requirements might only need to be defined at a high level. This process is subject to several iterations as the procurement process continues.

It is not possible to provide a comprehensive manual on the detailed and complex art of Requirements Engineering which is an activity often best sub-contracted to specialist personnel or organisations, although some organisations can resource this phase from internal personnel. Regardless of how the Requirements Analysis phase is resourced it is likely that there will multiple personnel forming a Requirements Team addressing this phase.

The following steps are important in executing this analysis:

1 **Identify the stakeholders**

The first step is to identify the stakeholders who will be impacted by the new system. The stakeholders may include the organisation's management, staff, customers, regulatory authorities, and vendors. The analysis needs to gather information from all stakeholders to understand their requirements and expectations.

2 **Collect Requirements**

The second step is to collect requirements from the stakeholders. This analysis needs to use a variety of methods to collect the requirements, such as interviews, surveys, and workshops. During these sessions, analysis should focus on understanding the stakeholders' needs, goals, and objectives. In some cases, this information will be highly specific with concrete requirement statements, in others it will be relatively vague or anecdotal. It is the skill of the Requirement Analyst to interrogate and articulate requirements into a cohesive document of set of documents.

An example of anecdotal information would be the documentation of the Customer Journey which will often include 'lived experience' information. In addition statistical data, and persona definitions would need to be brought together to create a list of Customer Journey requirements that can be articulated in a single document.

Requirements should be documented in a structured format that can be easily analysed and prioritised. At this stage these requirements will not have elaborated, validated, or filtered.

It is important to consider non-functional requirements here. These are often hidden and therefore can easily be forgotten. However, it is vital that requirements consider areas such as:

- Security: eg from unauthorised access, data breaches, and other forms of cyberattack
- Performance: eg the ability to handle a high volume of transactions without experiencing significant delays or outages
- Usability: eg ease of use for both customers and employees
- Availability: eg does the system need to be available the system available 24/7/365
- Compliance: eg compliance with applicable laws and regulations
- Scale: eg what does the organisations' wider strategy and plans suggest will be needed in the future? As our Technology 101 webinar covered the ICT strategy has to be considered in the context of the wider organisational strategy

3 Analyse requirements

The third step is to analyse the requirements to determine their feasibility and importance. The analysis should review the requirements against the business objectives and constraints, such as budget, time, and technical feasibility. Technical feasibility can be analysed by doing some background research on what's available in the market and by talking to similar organisations, and trade bodies, about what is being used and what challenges are faced by other organisations, big and small. Requirements should also be prioritised based on their impact on the business and the stakeholders. It is highly possible that, at this stage, some requirements are de-prioritised and/or dropped.

4 Define requirements

The fourth step is to define the requirements in a clear and concise manner. The analysis should use a standard format for defining the requirements, such as a user story or a use case. The requirements should include the stakeholders' needs, goals, and objectives, as well as any technical or functional specifications.

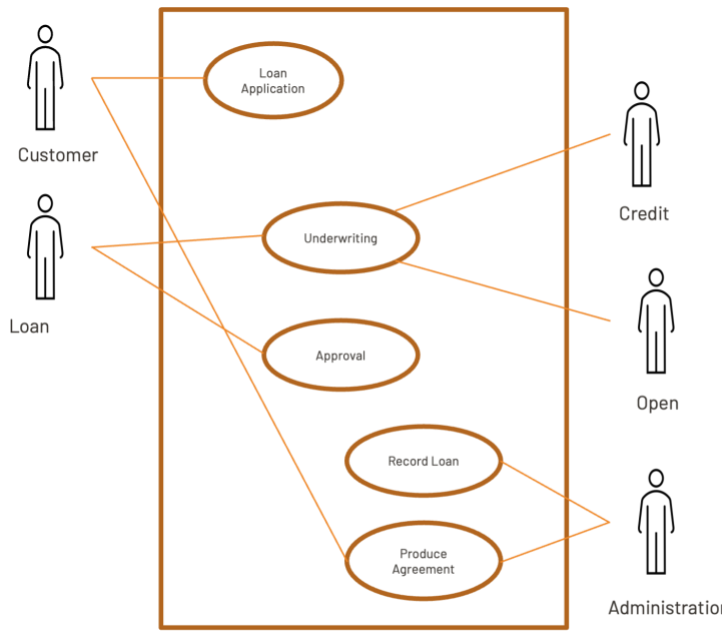
A common method of describing the requirement is the use story which has the common format:

> As a... [who is the user?]
>
> I need/want/expect to... [what does the user want to do?]
>
> So that... [why does the user want to do this?]

This format identifies the actor (user), the narrative (need), and the goal (...so that ...). Of these, priority should be given to the description of the goal or outcome. If this is hard to define then the requirement is

probably not clear, or possibly unnecessary. Talking to team members who regularly handle customer enquiries or customer complaints can be a good way to flesh out what existing systems and processes are and are not achieving for customers.

Combinations of requirements can often be efficiently documented in diagrammatic form, eg a Use Case, to show the interaction required between actors and the system. An example of a use case is:



The fifth step is to validate the requirements with the stakeholders. The analysis team should present the requirements to the stakeholders and seek feedback. The team should ensure that the requirements are complete, accurate, and acceptable to all stakeholders. Any changes or modifications to the requirements should be documented and communicated to all stakeholders.

It is important that these sessions and interactions are robust as the resulting set of requirements will ultimately define the system to be procured.

5 The fifth step is to validate the requirements with the stakeholders. The analysis team should present the requirements to the stakeholders and seek feedback. The team should ensure that the requirements are complete, accurate, and acceptable to all stakeholders. Any changes or modifications to the requirements should be documented and communicated to all stakeholders.

   It is important that these sessions and interactions are robust as the resulting set of requirements will ultimately define the system to be procured.

6 The final step is to prioritise the requirements based on their impact on the business and the stakeholders. The analysis should use a prioritisation matrix to assign a priority level to each requirement. The matrix should consider factors such as business value, technical feasibility, and stakeholder impact.

An often used, and simple, method of prioritisation is the MoSCoW Method which labels requirements against the following criteria:

Must Have: these are the non-negotiable needs for the product or technology platform

Should Have: these are features that are essential to the product or technology platform, but they are not vital, in other words the technology will work without them, but it is likely to be sub-optimal

Could Have: these could also be labelled ' nice to haves', ie they are not needed for the core function of the technology platform

Will Not Have: these are requirements that are not needed now but may be prioritised for the future. As such these should not be discarded as they may help in evaluating a technology road map

An example of the output of the MoSCoW analysis could be as follows:

Must Have	Should Have	Could Have	Will Not Have
Administration • Create new user • Restrict access control Loan Origination • Application Processing CRM • Contact History	CRM • Contact Preference	Loan Origination • Loan Pre-Qualification • Credit Info Processing	CRM • Chatbot

Output

The outputs of the above requirement analysis process would probably include a detailed requirements document, a prioritisation matrix, and a validation report, all of which will be used to evaluate potential technology providers and products.

The requirements document should include all the requirements in a structured format, along with any technical or functional specifications as this can be used as a valuable input to any Request for Information, or Request for Proposal document.

The prioritisation matrix should assign a priority level to each requirement based on its impact on the business and stakeholders. The validation report should document the feedback received from the stakeholders and any changes made to the requirements.

Taken together these outputs will serve as the basis for selecting the most suitable ICT platform for the organisation.

Request for information (RFI)

Often the first stage of a procurement process is the issuance of a Request for Information. This is typically sent to many potential vendors and is useful as an elimination process, especially where many potential vendors exist for a particular ICT category. In some cases it may be a statutory requirement to enter into a formal RFI and RFP process to satisfy certain principles such as:

- non-discrimination
- equality of treatment
- transparency
- mutual recognition
- proportionality

At the stage of an RFI the requirements issued will typically be at a high level but should, nevertheless, be robust and measurable against any response. For example, if, at this stage, the indicative cost of an ICT system is critical then a request for these costs must be included in the RFI documentation. It's also important to consider at the RFI stage what other costs are going to be incurred. A bid IT change project can absorb a huge amount of internal time and this needs to be costed too.

Typically the RFI document would contain the following:

Procuring organisation details
Procurement or Project Title
Date issued
Date due

Overview and objectives: (a brief summary, in a short number of paragraphs, describing the project and objective of the procuring organisation).

Information to supply: (a request for key information such as: high level functional coverage of ICT, high level technical details, indicative costs, indicative implementation timeline, etc.)

Response: (it is often helpful to template a response format for a vendor as it allows them to quickly answer the request and allows the procuring organisation to evaluate responses on a like for like basis)

An example RFI for a small Credit Union looking to move to cloud-based services might be structured as follows:

Subject: Request for Information - Cloud Services for Example Credit Union

Dear [Vendor/Supplier Name],

Example Credit Union, a small community financial services provider, is seeking information and proposals from qualified vendors offering cloud services. We aim to procure cloud-based solutions that can enhance our operational efficiency, data security, and scalability while meeting the unique requirements of the financial services industry.

We kindly request your company's participation in providing information and details about your cloud services offerings. This Request for Information (RFI) aims to gather information about your company, services, capabilities, and suitability for meeting our cloud computing needs.

Please provide the following information:

Company Overview:

- Company name, address, and contact details
- Years of experience in providing cloud services
- Brief description of your company's background and expertise in serving the financial services industry

Cloud Services Offered:

- Overview of the cloud services you offer, including infrastructure, platform, and software as a service (IaaS, PaaS, SaaS)
- Description of the cloud architecture, scalability, and availability of your services
- Details about your data centres, their locations, and certifications (e.g., ISO 27001, SOC 2)
- Information on the performance, reliability, and uptime of your cloud services

Data Security and Compliance:

- Description of your data security measures, encryption protocols, and access controls
- Compliance certifications (e.g., GDPR, PCI DSS) and adherence to financial industry regulations
- Disaster recovery and business continuity capabilities
- Privacy and data protection policies

Service Level Agreements (SLAs):

- Overview of the SLAs offered for uptime, performance, and issue resolution
- Guaranteed response times for critical incidents and support availability
- Compensation or penalties in case of SLA breaches

Pricing and Contractual Details:

- Pricing model (e.g., pay-as-you-go, subscription-based) and pricing structure for your cloud services
- Details on any upfront costs, recurring fees, and pricing tiers
- Contract terms, duration, and provisions for contract termination or renewal

Migration and Onboarding:

- Migration process and support for transitioning our existing systems and data to your cloud platform
- Onboarding assistance, including training, documentation, and technical support during the migration process

Customer Support:

- Description of the customer support services provided, including support channels, availability, and response times
- Account management and escalation procedures
- Customer satisfaction references or testimonials

Integration and Interoperability:

- Compatibility with existing systems and databases commonly used in the financial services industry
- API availability and documentation for integrating with third-party applications

Future Roadmap and Innovation:

- Description of your cloud technology roadmap and commitment to innovation
- Any upcoming enhancements, features, or expansions planned for your cloud services

Please submit your response to this RFI no later than [deadline]. The response should be in electronic format (PDF or Word document) and emailed to [contact email]. If you have any questions or require further clarification, please reach out to [contact name] at [contact email] or [contact number].

Please note that responding to this RFI does not guarantee your selection as a vendor, nor does it commit us to proceed with any further engagement.

We appreciate your time and effort in reviewing and responding to this Request for Information

Request for proposal (RFP)

An RFP is a more complete and comprehensive document than the RFI and, often, would form part of the contractual agreement with a vendor as the vendor will be stating, in their response, the capabilities of the ICT system being offered. If this contractual position is to be enforced, it should be stated up front to the vendor.

The RFP document will encapsulate the detailed requirements documented in the Requirements Definition process described above and will include additional specific information requests.

The format of the RFP is highly subjective however the following provides and indicative table of contents:

fair4allfinance

Request for Proposal

Supply, installation, commissioning, and maintenance of <<example>> system

Closing Date for Submission: dd/mm/yyyy

Table of Contents

contents:

In this document an introduction section would describe the procuring organisation and provide a high-level view of the project and its objectives. This helps the vendor position their ICT system in context.

Typically the document would then describe the submission process, including timelines, with which the vendor is expected to comply.

It is useful, for the vendor, to understand how the proposal will be evaluated, what weighting will be applied to different aspects of the proposed ICT system, how compliance will be evaluated, etc

An example of this might look like the following:

fair4allfinance

Technical Evaluation Criteria

This RFP will be evaluated using a two-stage process. The First stage will comprise the **Technical Evaluation** which will be based on the **Technical Proposal** whilst the second Stage will comprise the **Financial Evaluation** which will be based on the **Price Proposal**. It is the Bidder's responsibility to ensure that it has responded to both evaluation criteria. Failure to meet the evaluation criteria may result in lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa. Fusce posuere, magna sed pulvinar ult libero, sit amet commodo magna eros quis urna. Nunc viverra imperdiet enim.

Technical Evaluation

Technically the submission will be evaluated against the listed requirements with compliance weighted as displayed in the requirements listing. The bidder must provide information and evidence of the ability to satisfy the requirement.

The response will be scored against the following functionality groupings and each element will be awarded points to reflect the completeness of coverage identified by the vendor.

Criteria No.	Functionality Group	Points available
1.0	**Loan Account Management**	**24**
1.1	Maecenas porttitor congue massa.	8
1.2	Fusce posuere	8
1.3	Nunc viverra imperdiet enim.	8
2.0	**Fusce est.**	**32**
2.1	Vivamus a tellus.	8
2.2	Proin pharetra nonummy pede.	8
2.3	Aenean nec lorem.	8
2.4	Donec laoreet nonummy augue.	8

The bulk of the document should be taken up with the requirements specification developed from the previously executed requirements process. It is usually helpful, both for the prospective vendor, and for the evaluation team, to present these in a table which might look like the following

fair4allfinance

Requirements

Req. #	Description	Response	Coverage
1. Functional Area <<In porttitor>>			
1.1. Proin	Proin nec augue.		
1.2. Aliquam	Aliquam erat volutpat		
1.3. Etiam	Etiam eget dui		
1.4. Donec	Donec ut est in lectus consequat consequat		
1.5. Integer	Integer nulla		
2. Proin			
2.1. Suspendis	Suspendisse dapibus lorem pellentesque magna		
2.2. Fusce	Fusce aliquet pede non pede		
2.3. Ut	Ut nonummy		
2.4. Mauris	Mauris eget neque at sem venenatis eleifend		
2.5. Vivamus	Vivamus a tellus		

Complete
Partial
Minimal
None
Future

This section should also ask questions about:

- System Architecture
- System Security
- System Scalability
- System Extensibility

RFP Evaluation

Once completed and returned, the Analysis Team will need to evaluate all vendor responses against the following:

Technological capability

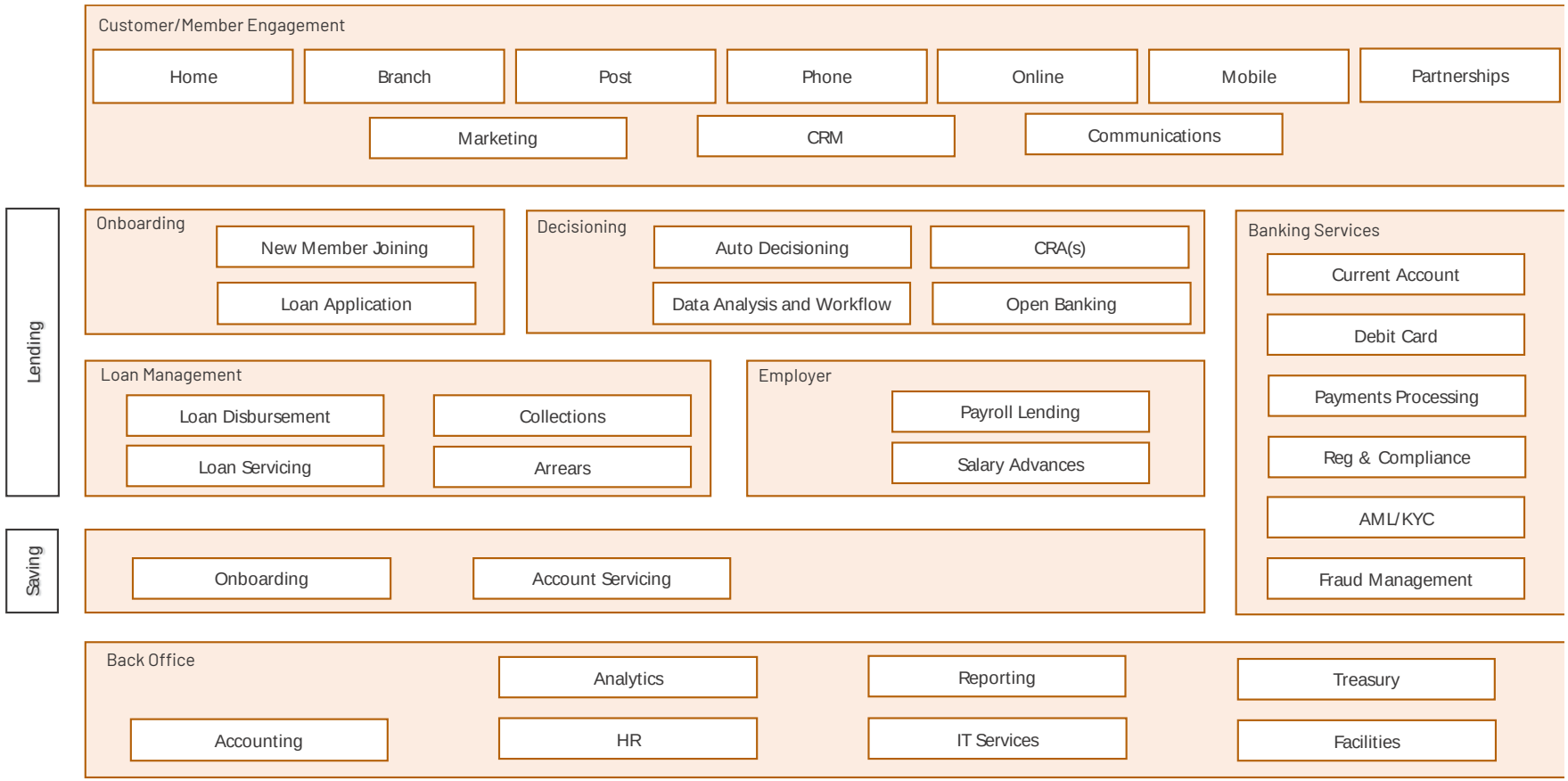
When evaluating the technical capability of an ICT solution it is tempting to look for perfection, however all technological solutions involve some degree of compromise, and it is important to be aware of the trade-offs involved before commitment is made. By understanding the potential benefits and drawbacks of an ICT solution, informed decisions can be made about whether it is correct for the organisation.

When evaluating an ICT product the organisation should consider the following elements:

1 **Functional coverage**

When measured against the requirements documentation produced in the previous section the ICT product should be 'scored' against those requirements.

The following schematic could be helpful in considering the functional coverage required and offered, and how the various elements of a system might communicate with each other and with other, external, applications:


Customer/Member Engagement
Home
Branch
Post
Phone
Online
Mobile
Partnerships
Marketing
CRM
Communications
Lending
Onboarding
New Member Joining
Loan Application
Decisioning
Auto Decisioning
CRA(s)
Data Analysis and Workflow
Open Banking
Banking Services
Current Account
Debit Card
Payments Processing
Reg & Compliance
AML/KYC
Fraud Management
Loan Management
Loan Disbursement
Collections
Loan Servicing
Arrears
Employer
Payroll Lending
Salary Advances
Saving
Onboarding
Account Servicing
Back Office
Analytics
Reporting
Treasury
Accounting
HR
IT Services
Facilities

2 **Technical architecture**

Consideration should be given here to how the system organised? There are many ways to organise a system, but the main options usually fall in to one of the following categories:

- Client-server architecture

In a client-server architecture, the system is divided into two parts: the client and the server. The client is the part of the system that interacts with the user. The server is the part of the system that stores data and performs calculations. The client and the server communicate with each other over a network.

- Three-tier architecture.

In a three-tier architecture, the system is divided into three layers:

  - the presentation layer responsible for displaying information to the user
  - the application layer responsible for processing user requests
  - the data layer responsible for storing data

Typically, the three layers communicate with each other through a well-defined interface.

- Microservices architecture

In a microservices architecture, the system is divided into a collection of small, independent services. Each service is responsible for a specific task. The services communicate with each other through well-defined Application Programming Interfaces (APIs). This architecture makes the system more scalable, flexible, and easier to maintain.

Each architecture has its own merits and limitations, and it is important to assess these in the light of the needs of the organisation.

3 **Development roadmap**

The proposed roadmap of the ICT system being considered is important as it will indicate the longevity of its applicability to the organisation and indicate what new features may be expected (eg to address the Should Have requirements previously identified)

4 **Development approach**

The development approach, and the location of the various teams, can be an indicator of the responsiveness of the vendor to changes.

5 **Data access and exportability**

Data needs to be accessible for analysis and reporting purposes so it is important to consider how easily data in the ICT system can be extracted and used by external systems.

6 **Scalability and extensibility**

It is important to consider how adaptable the ICT system is to increases in business volumes of the organisation. It is equally important to consider how easy it is to extend the functionality of the ICT system either by adding capability to the system or by interfacing with other external systems.

7 **Integration capabilities (eg APIs)**

As APIs are ubiquitous it is perhaps important to consider these specifically. An API is a way for two or more computer programs to communicate with each other. It is a type of software interface, offering a service to other pieces of software. A document or standard that describes how to build or use such a connection or interface is called an API specification.

APIs are used to share data and functionality between applications. For example, an API can be used to allow a web application to access data from a database or to allow a mobile app to control a device.

Some of the benefits of APIs include:

- Reusability
  - APIs can be reused by multiple applications, which can save time and money
- Scalability
  - APIs can be scaled to handle increasing demand
- Security
  - APIs can be secured to protect data
- Documentation
  - APIs are typically well-documented, which makes them easy to use.
- Community
  - There is a large community of API developers who can help with troubleshooting and support.

8 **Implementation approach and support**

The implementation of a new system and migration from an incumbent system are critical to the success of a new ICT system within an organisation. These are rarely painless exercises and consideration must be given to how the ICT system provider supports the implantation of and transition their system.

Financial stability

An investment in CTI is usually a long-term commitment and consequently it is vital that there is confidence in the long-term viability of the vendor. To gain this confidence it is important to scrutinise the financial stability of the vendor organisation. As part of your due diligence process, you should validate the vendor through the relevant company registration database, as well as carry out credit and

anti-money-laundering screening. You should also ask questions to satisfy yourself if the ability and position of the provider to offer the product/services

Several years audited accounts are useful, and more recent management accounts are a sensible thing to review. This scrutiny needs to cover:

- Installed base of customers – this involves understanding how many organisations the provider already supports and usually how complex or large those organisations are
- Financial statements, cash flow, and debt-to-equity ratio, where a high ratio may indicate the inability of the organisation to invest in development due to the need to service debt
- Liquidity which, related to the above, can indicate if the vendor can cover their short-term obligations, and to what degree
- Solvency which can indicate the ability or the vendor to service long-term debt obligations
- Profitability which should be carefully considered. It could be legitimate for a software vendor to have low, or even negative profitability, dependent on their stage of development and growth
- Growth (historical and potential)
- Risks which should include self-identified financial risk as well as ones derived from the above analysis. Where risks are identified it is also good practice to provide mitigating measures to manage the identified risks
- Ownership structure, sometimes vendor organisations can be part of a complex ownership structure and it is important to understand this to identify if there are any inherent risks or conflicts of interest present. It is also worth asking explicitly if the potential vendor is considering any changes to its structure eg if it is in discussions about purchasing or being purchased by another entity
- Operational financial stability – in addition to using records kept at Companies House in the final stages of diligence it is often also useful to consider other checks of a suppliers' resilience eg seeing whether there are any county court judgements against them and using 3rd party checking tools to make sure that their payment arrangements are reasonable so that any working capital issues can be identified eg using CreditSafe

Security

Security is one of the key non-functional factors to assess when considering an ICT system. It is important to understand security from both the perspective of a malfeasant actor attempting to break into the system and steal data or pervert its function in some way, as well as a legitimate user of the system where security should not unnecessarily impede their ability to use the system effectively. It is also important to understand how the system cares for the security of the data it maintains and stores, what data resilience exists, etc.

In considering this aspect it is important to pay attention to the following elements:

- In built security capabilities, data security, transactional integrity, segregation of duties, levels of authorisation, access limitations, etc.
- System Certification which could include compliance with such international standards as ISO 9000 and BS ISO/IEC 27001:2022. Both are part of a family of standards and cover different areas. A system vendor organisation may also claim compliance with the TickIT certification standard.
  - ISO 9000 is a Quality Standard and compliance with this would indicate that the vendor organisation has processes and monitoring in place to ensure that the vendor's customers get reliable, desired quality goods and services.
  - BS ISO/IEC 27001:2022 is a security standard and a vendor organisation may reference this to indicate that they have in place functionality to manage the security of assets such as financial information, intellectual property, employee data, and information entrusted by third parties.
  - TickIT is a certification programme specifically aimed at software development organisations. It encompasses ISO 9001 and cross references with ISO/IEC 15504 (Information technology — Process assessment) and ISO/IEC 12207 (Systems and software engineering — Software life cycle processes)

  What is important for the purchasing organisation is not to know these standards in depth but rather to be able to see independent audited verification of the standards and certification the vendor organisation is claiming.
- Evidence of security tests and audits especially third-party tests. Where the system is internet facing the results of the most recent Penetration Test should be reviewed and the provider should be able to set out their plans for regular Penetration testing

Vendor resilience

All vendors should be able to provide details about their organisation that give an indication of its resilience as a trusted provider. This diligence can cover questions like:

- Organisational change and number of people in key roles (eg technical support)
  - Key person risk is often an issue of critical concern, for example if there is only one individual who understands a key component of the system this could represent a continuity risk if that key person became unavailable at the same time as a system failure with the component on which they are expert
- Disaster recovery arrangements including fail over / redundancy in hosting arrangements.
  - For example, if a system, either on-premise or cloud based, suffered a catastrophic failure what level of data loss could result
- Number of minutes of outages per customer on average by year and time to resolve
- Disaster Recovery (DR) testing plans and frequency of live testing scenarios

Compliance

Another factor to consider and one which also touches on the non-functional requirements of an ICT system is compliance. For example:

- Compliance with the relevant regulatory framework, eg GDPR, AML, etc.
- Compliance policies and procedures of the vendor organisation
- Liaison of the vendor with relevant regulatory bodies – asking open ended questions in the diligence process about the relationships with the regulators can glean information that providers might not otherwise share eg asking if any investigations are being undertaken rather than asking about upheld complaints can give a different picture

Contractual arrangements

Finally, the contract basis is vital to understand. Is the licence fee a recurring item? Is it escalating by being pegged to the RPI or CPI? What additional charges are likely to be levied? Etc.

Consideration should therefore be given to:

- Licence basis (monthly, quarterly, annual) – being clear about the timetable for license cost increase is important – eg how long is the license fee per user set for? The roadmap for supporting licenses of a particular type is also important eg if the vendor is offering licenses for a platform for which the underlying technology will only be supported for a finite period of time – then consideration needs to be given to when upgrade costs are going to be incurred
- Costs and scale - it is important to work these through with the finance lead in the organisation to understand what a vendors' costs are going to involve upfront, on an ongoing basis and in terms of depreciation too this can be broken down into
  - Discovery and design – all systems will require some parameterisation and/or modification to fit the needs of a company (think minor alterations to an off-the-shelf suit). There will be a cost associated with identifying the changes needed and in making these changes.
  - Implementation – this is often the largest cost associated with the take on of a new ICT platform and consequently should consider:
    - Project Planning costs
    - Resource Allocation both internally and externally
    - Data Migration and Integration
    - Testing and Quality Assurance
    - Staged payments linked to key implementation milestones
  - Training costs
  - Licensing basis and costs
  - Maintenance basis and costs
  - Additional service costs
- Service coverage – this covers what level of services will be provided in terms of consistent availability and uptime and planned outages for improvements and upgrades etc.
- Term and termination

Support contracts are often issued separately to implementation and licensing contracts. These need careful specification and consideration. Some vendors offer 'blended rate' costs for technical support beyond first line resolution – this can be cost effective if a range of resources from the Vendor are needed throughout the year as even more senior resources can be charged at an averaged rate. Modelling the assumptions about what support will be needed is key to this kind of consideration.

Appendices

Technology obligations on lenders in the regulations

For example, the Credit Union Sourcebook (CREDS) references the Systems and Controls (SYSC) section of the FCA Handbook and:

> requires that a credit union takes reasonable care to make and retain **adequate records** of all matters governed by the Act or the CCA, secondary legislation under the Act or the CCA, or rules (**including accounting records**). These records should be capable of being reproduced in the English language and on paper.
>
> CREDS 2.2.24 referencing SYSC 9.1.1 R

Similarly the Consumer Credit Sourcebook states:

> RTO firms are reminded of their obligations in SYSC 9.1.1R to keep orderly records, which must be sufficient to enable the FCA to monitor the firm's compliance with the requirements of the regulatory system. Records which the FCA would consider to be sufficient to show compliance with the benchmarking requirements in CONC 5B include:
>
> (1) point-in-time evidence of other benchmarking cash prices such as screengrabs or outputs of third party benchmarking data, together with evidence establishing the point in time to which it relates;
>
> (2) evidence to show how the RTO firm took reasonable steps to ascertain whether the same item of goods or bundle of goods was available for sale by other retailers; and
>
> (3) evidence to show how the RTO firm established that goods benchmarked against were comparable to those supplied by the RTO firm.
>
> CONC 5B ..1

CREDS goes on to discuss the appropriateness of systems:

> CREDS 2.2.25 - A credit union should have appropriate systems in place to fulfil its obligations with respect to adequacy, access, periods of retention, and security of records.
>
> CREDS 2.2.33A - A credit union must maintain information systems to enable the governing body to direct and control the credit union's business effectively, and to provide the information required by the FCA.

And further defines principles to apply to third party arrangements:

CREDS 2.9 The following standards apply to all third party ICT arrangements:

- EBA ICT GL, including but not limited to Sections 3.2.3, 3.3.2, 3.4.5, and 3.7 (in particular, paragraph 86). These GL should be interpreted consistently with: the Operational Resilience/Insurance – Operational Resilience Parts, the expectations in this SS, and SS1/21; and
- relevant legal requirements and standards on ICT security (eg Cyber Essentials Plus) and data protection, including but not necessarily limited to General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Referred to above the European Banking Authority's Guidelines on ICT and Security Risk Management (EBA ICT GL) states:

3.2.3 ...

To ensure continuity of ICT services and ICT systems, **financial institutions should ensure that contracts and service level agreements** (both for normal circumstances as well as in the event of service disruption — see also Section 3.7.2) with providers (outsourcing providers, group entities, or third party providers) **include the following**:

1. a) **appropriate and proportionate information security-related objectives** and measures including requirements such as minimum cybersecurity requirements; specifications of the financial institution's data life cycle; any requirements regarding data encryption, network security and security monitoring processes, and the location of data centres;
2. b) **operational and security incident handling** procedures including escalation and reporting.

3.3.2. Identification of functions, processes and assets

15. Financial institutions should identify, establish and maintain updated mapping of their business functions, roles and supporting processes to identify the importance of each and their interdependencies related to ICT and security risks.
16. In addition, **financial institutions should identify, establish and maintain updated mapping of the information assets supporting their business** functions and supporting processes, **such as ICT systems**, staff, contractors, third parties and dependencies on other internal and external systems and processes, to be able to, at least, manage the information assets that support their critical business functions and processes.

Regulators focus on technology providers

Although system vendors are not directly regulated by the FCA or PRA, unless they provide so called critical financial market infrastructures such as payment systems recognised by HM Treasury; central securities depositories; and central counterparties (CCPs), both the Government and Regulators are increasingly paying attention to systems vendors and service providers in this sector. Witness the following extract from a Government Policy Statement on critical third parties to the Financial Sector:

> HM Treasury has been working with the Bank of England, including the Prudential Regulation Authority (PRA), and Financial Conduct Authority (FCA) ('the financial regulators') to understand what 'direct regulatory oversight' of critical third-party services might involve; and come up with a framework to enable them to manage the risks to financial stability and their statutory objectives.

Under the proposed regime:

> The financial regulators will be granted powers to assess whether the resilience standards were being met. These will include powers for the financial regulators to:
>
> - request information directly from critical third parties on the resilience of their material services to firms, or their compliance with applicable requirements;
> - commission an independent 'skilled person' to report on certain aspects of a critical third party's services;
> - appoint an investigator to look into potential breaches of requirements under the legislation;
> - interview a representative of a critical third party and require the production of documents;
> - enter a critical third party's premises under warrant as part of an investigation.

Letters to credit unions 'PRA annual assessment of the credit union sector' – 2023

In the above 'Dear CEO' letter the PRA emphasised the duty of Credit Unions to inform the regulator of

" … material operational changes (by emailing prudential_creditunions@bankofengland.co.uk). Examples of when a notification would be appropriate include:

1. replacement of a core banking system;

2. change of third-party service supplier;

3. digital transformation programmes; and

4. data centre / cloud migration.

When considering operational changes, the board should ensure it has appropriate governance, risk management, and mitigation measures in place."