Law Society of Scotland

Guide to IT Procurement

In association with

amiqus MITIGO CYBERSECURITY

Contents

Introduction

The IT industry is extremely fast paced with multiple new products and technologies entering the market at any given time. Identifying and procuring the right product can be a challenging and time-consuming process, particularly for small businesses who do not have a dedicated IT team.

While IT procurement processes will vary in different organisations depending on their own sets of needs, the starting point will usually be identifying a business requirement. This may be a problem that needs to be solved, digitalising a manual process or gaining advantage by making the organisation better, faster and more efficient.

Once you have a clear understanding of what your business requirement is, the next steps are exploring the market and starting conversations with vendors. At this point, it is important to know what questions to ask to ensure you end up with the right product or service.

Specific considerations will depend on the product/service you want. For example, if you are buying a product that you want your clients to interact with - you would ask if the client needs to install specific software. If you are installing a financial accounting software – you would ask if it is compliant with Law Society accounts rules.

A web version including guidance on professional obligation considerations can be found at **lawscot.org.uk/guide-to-it-procurement**

More general considerations will include:

- Value/return on investment
- Price
- Company reputation and background
- Quality
- Ability to meet relevant standards
- Five year total cost of ownership
- Provider's understanding of sector/your business
- Support
- Implementation process
- References
- Risk mitigation
- Staff time required for the project options
- Cyber security and operational resilience

This document is intended as a guide to assist you when going through an IT procurement process. It provides examples of questions that may help you when considering a product or service and negotiating with a vendor. It is not a definitive list and as your firm will have its own unique requirements, you will need to adapt the questions to suit your own circumstances.

Technical specification

It is important to consider the technical specification of the system/product you are looking to purchase and get as much information from the vendor at an early stage to ensure they can provide what you need. You should also consider how the new system/product is compatible with your existing infrastructure, software and hardware. Technology specifications often refer to API in relation to system integration. API is an abbreviation for Application Programming Interface which is the ability for one system to integrate with another system, to transfer data or connect them. One of your main considerations when looking at a system is whether it is cloud-based (i.e. hosted on the internet) or hosted on your premises. You should clarify these options with the supplier at the start of the process.

Example questions:

Software and connectivity

- What software technologies are being used to provide your solution?
- What database solutions are being used to store information?
- What browser software is the solution compatible with?
- Is any additional software needed if a client is to use the system?
- Are any other third-party products required to be installed on client machines other than a browser?
- What is the minimum specification of internet connection to connect and use the system?
- What access will the provider require to any of our existing software or systems?
- Will we need to undertake any adaptation or development of our existing systems?
- How do you maintain your system?
- What is your system down time?
- How do you manage system/version updates and how are we informed of these?

Compliance

- Please outline the compliance status of the system in relation to disability discrimination, usability and accessibility.
- Does the system comply with W3C accessibility guidelines (www.w3.org) and has it been independently tested?
- Is the system compliant with Law Society accounting rules? Can the system produce the correct reports for this?
- Does the system have any anti-money laundering functionality?
- What audit trail, and level of detail, will be recorded by the system when we make changes or record information?

Integration

- Please confirm if your system has API facilities. If yes, how do they work and what are the security arrangements?

Cloud solutions - benefits and risks:

+ Potential cost savings
+ Efficiency and accessibility
+ Integration possibilities

- Security and control
- Location of data centre
- Business continuity and access issues

For more information on cloud computing, visit:
www.lawscot.org.uk/members/business-support/technology/cloud-computing-guide/

Training, support and maintenance

It is essential that the vendor offers adequate training and ongoing support for their system. You should get full details of this and any additional costs ahead of signing up with them.

Example questions:

Training provision

- What training will be provided and what will be the duration?
- Will this be provided directly by you or subcontracted? If subcontracted, specify name and address of subcontractor.
- Is the cost of the training included in the price?
- What materials (e.g. user guides) will be provided?
- Will we be assigned a dedicated account manager during the onboarding process and/or on completion of any set-up period?

Support and maintenance

- Will we be provided with a dedicated, low-cost helpdesk number?
- What hours will the helpdesk be available?
- What will be the response time for calls?
- Do you expect any queuing or automated call routing system?
- Is there any limit to the number of helpdesk calls? Please detail any additional costs that are included in the contract.
- Will it be possible to email the helpdesk at a unique email address? If so, what is the expected turnaround time for responses?
- Will we have access to a dedicated online support portal? Will this offer a live chat facility?
- Do you offer remote access for support enquires? If so, please detail.
- Please provide details of the extent of the support the help desk will provide.

Accreditations, insurances and data protection

Ensuring that the vendor has the right accreditations and insurances is an important part of the procurement process as these will help protect you as a customer. You also need to find out about their cyber security and data protection policies to ensure your data will be kept safe. If you are transferring data outside of the EEA, the GDPR imposes some restrictions. This is important if you are handling client data. It is also important to undertake an independent assessment of the cyber security risks which any new technology introduces.

Example questions:

Accreditation and insurance

- Do you currently hold accreditation under ISO 27001 international standard for information security systems? If you do not, do you plan to obtain it and when?
- If trading partners are used, please specify their names, addresses, and roles.
- Which of these organisations, if any, are accredited to BS7799 /ISO 17799:2000?
- Please provide a list of any other accreditations that you consider relevant and important to the submission.
- Please provide copies of current insurance policies which would be relevant (including for instance professional indemnity and business interruption).

Data protection and cyber security

- What is your organisation's Data Protection Registration Number?
- Please provide a short statement about the security measures you have in place to protect and manage personal data, addressing Article 5 and in particular Article 5 (2) of GDPR.
- Where is your data stored? If it is held off-site, please provide full details of where it is stored?
- Do you hold Cyber Essentials or Cyber Essentials Plus certification?
- What security configuration and additional controls will be necessary as part of the system set up? How will they be maintained and by whom?
- Please provide a short statement on the business continuity plans you have in place to protect your organisation and its continued business function.
- What are your protocols if you suffer a data breach? When and how will you inform us?

Due diligence and warranty position

As part of your due diligence process, you should run the vendor company through the relevant company registration database, credit and AML screening. You should also ask questions to satisfy yourself if the ability and position of the provider to offer the product/services. Some products and services may offer a pay as you go service, this is worth considering if you are unsure of a longer-term commitment.

Example questions:

- Please confirm that you warrant the full capacity (staff, finance, technical skill, hardware etc) and all necessary consents and licenses to provide the stated service/product.
- Please confirm that you will remedy and/or indemnify our firm/organisation for any failure arising from the preceding warranty.
- Please confirm that you are not subject to any insolvency or similar processes.
- Please confirm you have no material litigation pending (with a value specified).
- Please confirm that there are no reasons (e.g. project commitments) that the work cannot proceed immediately upon agreement to proceed.
- Please give indicative timetable from project start to launch.
- Please detail what input, resources and commitments you expect from us at each stage of the set up.
- How do we secure/retain our data in case your organisation ceases or changes hands?
- Do you offer a trial period?

Costs and contract

You should get a clear picture of the set up and ongoing costs ahead of any contract commitment. Make sure you consider these costs and any contract commitment for the service in detail and explore the scope for any negotiation.

Example questions:

- Please summarise all costs (excluding VAT) relating to the project. If costs are dependent on number of users or active users, please provide details.
- Please provide itemised costs i.e. costs that can be split into capital and recurrent for each year.
- Consultancy or services costed on a per day rate must be defined. Where a cost is fixed or variable this must be made clear.
- All costs must be listed upfront including initial set-up costs and subsequent years.
- Please confirm the length of contract you require us to commit to.
- Please provide a copy of the standard contract/terms and conditions to be provided.
- Is there a finance agreement needed, if so what are the exit conditions if the system isn't satisfactory?
- What are the exit provisions and costs, in general?

Additional Information

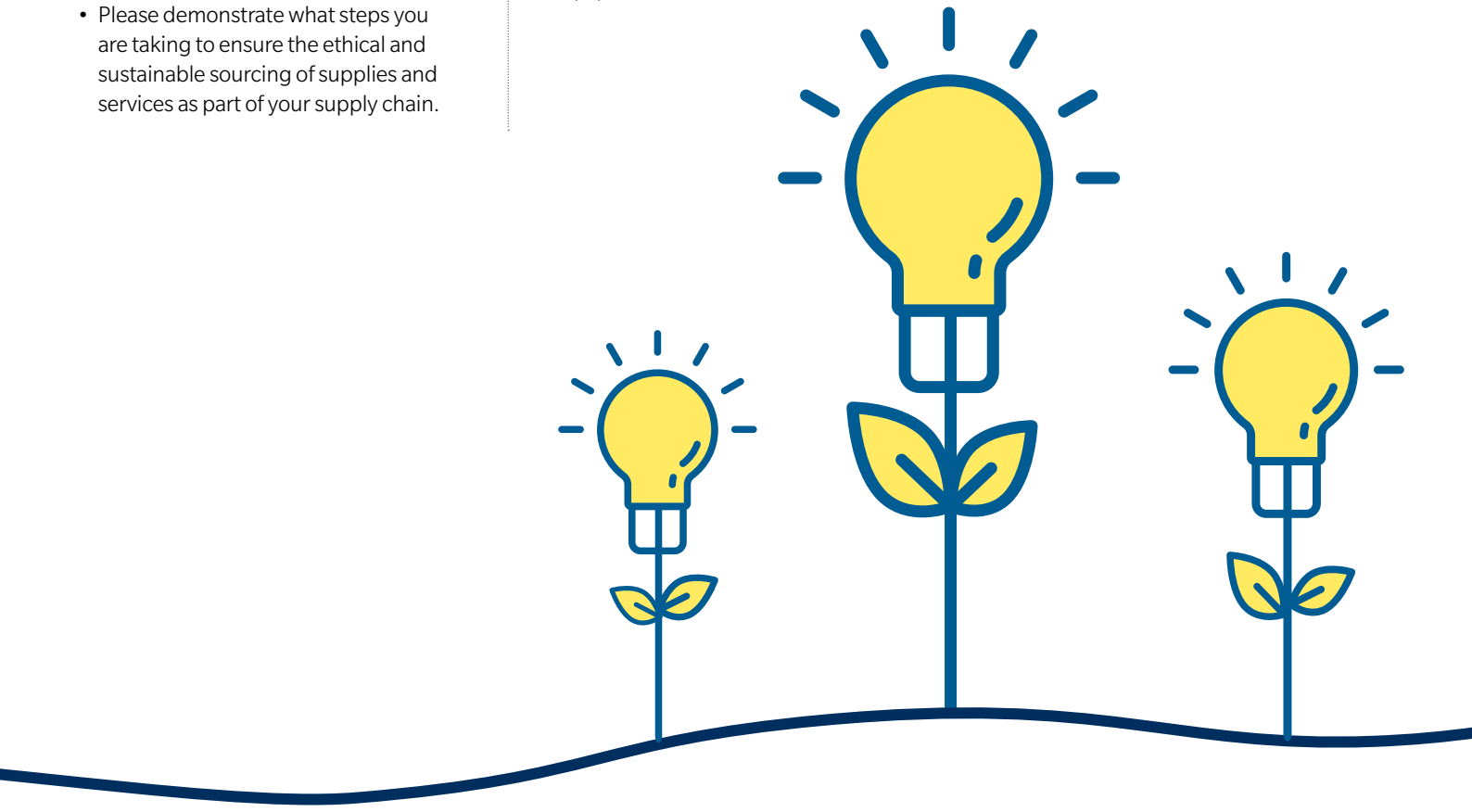
- Seven Steps to sound procurement
- ISO 27001
- Information security - Law Society of Scotland
- Technology Scottish Business Resilience Centre
- SaaS security principals

General ethical and sustainability considerations

Ethical and sustainability issues are increasingly at the forefront of the minds of clients, regulators, employees, investors and other stakeholders. How you handle these issues will have an impact on how you are viewed as a firm. Consideration for ethical and sustainability issues should extend beyond the day-to-day operations of your firm to those who supply you with goods and services. By including these questions in your IT tender, you will have a more complete picture of the environmental impact of your business as well as aligning the ethical considerations of your suppliers with your own. If your firm has published policies on ethics, sustainability, and diversity etc, you should share these with potential suppliers.

Example questions:

- What are your ethics and sustainability policies? If you don't have a published policies, are you willing to adhere to our firm's own policies or code of conduct? (This might include reference to your firm's values and statements on your commitment to equality and diversity, inclusion, social mobility, anti-slavery, responsible sourcing of goods and services etc.)
- Please demonstrate what steps you are taking to ensure the ethical and sustainable sourcing of supplies and services as part of your supply chain.
- In the case of hardware procurement, please confirm that you have an effective conflict minerals compliance programme.
- Please demonstrate what steps you are taking to minimise your carbon footprint and provide information that will allow us to assess this.
- Do you comply with industry standards on environmental issues such as WEEE (Waste Electrical and Electronic Equipment) and ISO 14001?



Glossary

Application Programming Interface/API
A way to allow a system to be accessed by other systems and transfer data between the two.

Artificial Intelligence/AI
A problem-solving application that makes decisions based on complex rules or if/then logic.

Chatbot
A way of interacting with a program through a messaging service.

Client portal
A website for use by clients to give them secure access to documents and other information.

Cloud computing
The delivery of computing services such as servers, storage, databases, networking and software over the internet ("the cloud") rather than storing these on your premises.

Contract lifecycle management/CLM
A term for systems that seek to cover all stages of the contracting process (from intake through to contract management).

Contract management system/CMS
A system to help companies manage their contracts after signature. Typical systems will hold a copy of the contract as well as metadata about the contract such as parties and renewal dates.

Cyber security
Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Dashboard
A live summary, normally presented as a web page with charts, that allows a user to see the status of processes and other key data.

Digital/Electronic signature
Electronic data is used by a person to sign or otherwise signify agreement or consent.

Document automation
A system for generating a tailored contract or other document based on the answers to questions.

Document management system
A system for storing documents so that they can be accessed by other members of the team. Some document management systems can also store emails associated with a matter.

E-discovery
A search system for large volumes of emails and documents.

Smart contract
A program that typically is tied to a blockchain and "self-executes" a transaction, e.g., change a registry or perform another act if certain conditions are satisfied.

Virtual private network/VPN
A protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity making it more difficult for third parties to track your activities online and steal data.

Wiki
A system for allowing teams to share knowledge, with users being able to edit and create pages.

Workflow
A system for automatically tracking and directing the flow of a process.

Our sponsors

Thank you to our sponsors, Amiqus and Mitigo, for supporting our Guide to IT Procurement

Amiqus

Amiqus is the Law Society of Scotland's strategic partner, enabling member firms to deliver their services digitally, securely and efficiently. Complete client and staff ID verification and onboarding in minutes and create watertight compliance processes:

- Trusted by hundreds of legal firms across the UK
- Integrated with Clio and Denovo
- ISO/IEC 27001:2013 and Cyber Essentials Plus certified

amiqus.co

Mitigo Cybersecurity

Mitigo is the Law Society of Scotland's strategic partner, providing members with protection against cyber-attacks such as ransomware and email account takeover. Also operational resilience, data security and legal and regulatory compliance. The service covers risk assessment, technology testing, cyber awareness training and governance. Mitigo also provides an emergency breach response and investigation service for law firms and their clients, vulnerability assessments and supply chain cyber management.

mitigogroup.com

The Law Society of Scotland
Atria One
144 Morrison Street
Edinburgh
EH3 8EX
T:+44(0) 131 226 7411

www.lawscot.org.uk