CIPS KNOWLEDGE

Supplier Assurance Questionnaire (SAQ's)

An insight into the findings from a workshop held in May 2019 in partnership with SASIG and NCSC.

This knowledge paper is supportive of Procurement professionals operating at Managerial level of the CIPS Global Standard

01 CPD HOURS

CIPS members can record one CPD hour

Supplier Assurance Questionnaire (SAQ's)

What is a SAQ

A supplier assurance questionnaire (SAQ) is increasingly utilised by procurement professionals as a tool to interact with existing and new suppliers to ensure that risk exposure to an organisation is assessed, identified and managed accordingly. Procurement teams are developing their systems and processes to bring current suppliers up to required levels of conformance, however various discussions with procurement professionals has highlighted that many are being weighed down by time consuming manual systems and many are only part way through their current supplier audit process.

Overview of the workshop

Held in May 2019, CIPS Knowledge worked with SASIG and NCSC to build a workshop which was attended by over 150 procurement and cyber specialists, to help identify:

- How the SAQ process is being managed in various organisations
- Who is taking ownership for the process within organisations
- Commonalities and solutions that may be available for consideration to bring to your own organisation

There were presentations from SME's to large corporate organisations during the day to identify how they were managing the process and the resource that they were applying, there was a questionnaire to attendees that we shall identify points from during this paper, and at the end of the workshop there was a question and answer panel session with the guest speakers.

Summary from the workshop

Findings from the workshop identified that many of the attendees were on average half way through the process of reviewing their suppliers, the process is cyclical and there were no attendees identifying that they had completely audited 100% of their suppliers. It was voiced by many attendees that it was certainly easier to take new suppliers through the process than incumbent suppliers.

On the day there were some fantastic tips on managing cyber risk and taking suppliers through a learning journey, highlighting resources such as Cyber essentials, 10 Steps, NIS Guidance, ISO27001 standards and PCI.

The National Cyber Security Centre (NCSC) holds a wealth of information that guides organisations in protecting their systems from cyber threats. Further information is available from NCSC on cyber essentials certification, this scheme is designed to help UK organisations with limited experience of cyber security to improve their defences. A valuable resource to direct suppliers to, whether they are or are not yet ISO27001 compliant.

The biggest point highlighted in the room was that the SAQ process should in no instance be conducted as an arms length tick box process, collaboration was the key to success along with supporting suppliers to meet your organisations standards and taking them on a learning journey where necessary.

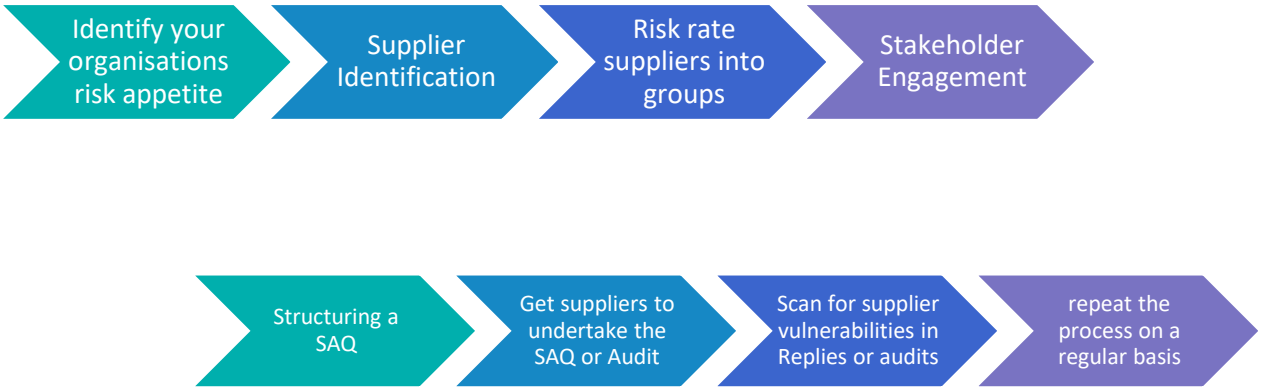
Some organisations had gone into a deep dive when auditing high risk/critical suppliers, and this is because the risks may not come from the tier 1 supplier, but from tier 3 or 4 suppliers that form part of your supply chain. You may wish to hold your direct suppliers responsible and then flow down responsibility through

contract terms and their own use of appropriate questionnaires. By holding face-to-face audits, you can truly understand the depth of your supply chain and where risks lie.

Finally SME's, they are often the innovators or can be the sole supplier to a specialist item along with being a necessary element of diversity in your supply chain. They can be completely overwhelmed with the SAQ process, so partnering with them and supporting them on their learning journey to compliance will only strengthen the working relationship.

Steps to developing your SAQ

The next elements of this paper are designed to support you through the stages to developing your SAQ's and to highlight some tips and guidance.



Due diligence

Within the workshop discussion it was very clear that one of the first steps was to identify your own organisations risk appetite. Once you understand how your organisation would like to position any risk exposure then you can start to focus areas on priority areas.

Supplier identification

An exercise of identifying all suppliers that deliver goods or services into your organisation should be performed, but be sure to remove any duplicate information such as subsidiary company information so you do not duplicate work flow.

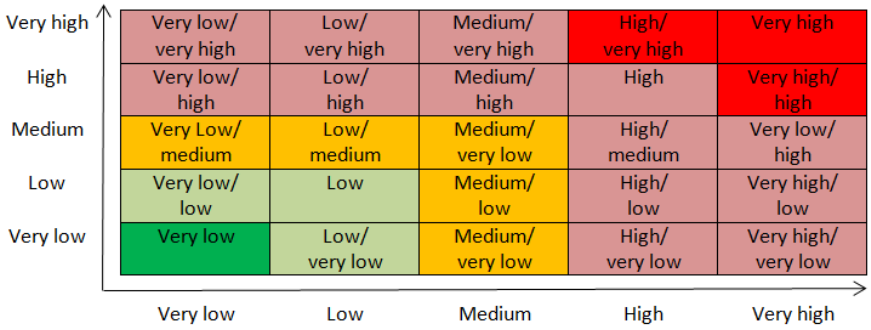
Risk rate suppliers

Consider tiering your suppliers risk to your organisation in the areas such as:

- Value of spend
- Exposure based on geographical location or length of supply chain
- Dependency such as critical goods/services
- Sensitivity of product/service supplied
- Access provided to your network to manage devices/services
- Criticality/sensitivity of data held or processed by a third party

For example, if you spend 10% of your annual spend with a supplier, this would classify them as high dependency and a significant risk to your organisation if they were compromised, from a financial, reputational, cyber or supply risk.

Scope each supplier into risk categories:



This would then enable you to classify the risk threat that each supplier has towards your organisation. You could tag the suppliers on a 1/2/3 basis or set a red, amber, green (RAG) rating system against current suppliers.

The aim is not to dismiss small spend suppliers, as they may also come with an increased risk exposure based on their own business maturity model, but this system may give a start point to your SAQ process.

The SAQ process is not designed to simply be a pass or fail exercise, it is about working in collaboration with your suppliers to educate and develop them, to meeting your organisations needs in order to continue to have a successful working partnership.

Stakeholder engagement

As procurement teams are the main interface between suppliers and internal stakeholders, procurement teams or specialist "supply chain information managers" in most instances take ownership of the SAQ process.

However, from the outset it is important that key stakeholders from around the business are consulted, each stakeholder will have their own focus on areas of risk mitigation, so the building of an SAQ should be undertaken in collaboration with skilled professionals from within your organisation.

Stakeholders will have their own areas of risk that they need to report on and take responsibility for, so ensure that you leverage key information on your SAQ that will meet your stakeholders needs, this should in turn mitigate regular requests for supplier information from within your organisation, but also be mindful that stakeholders may ask for an excess of questions to be included in the SAQ process, so look for information overlap between stakeholders and manage the expectations of stakeholders.

Stakeholder relationship is critical because once a supplier has completed the SAQ should there be any issues raised, it is at this point that you would look to consult with the applicable stakeholder internally as to how

they would like to progress the issue and seek further clarification with the supplier so building strong relations in the early part of the process development will support you when issues are raised with suppliers.

Survey respondents from the workshop gave a mixed response to identify who takes responsibility for progressing risk once identified with a supplier, there seemed a clear divide between procurement acting as an interface between the supplier and stakeholder, and the stakeholder being introduced to the supplier to undertake further deep dive conversation.

Structuring a SAQ

SAQ's assess risk exposure across several key areas when interfacing with suppliers, some of the areas you should consider focussing on within your SAQ could be in the following areas:

- Cyber security
- Modern slavery/ethics/CSR
- Environmental impact
- Financial outlook and rating
- Health and safety/legal compliance
- Supplier/category/country risk
- GDPR compliance
- Supplier/workforce diversity/equality/HR
- Accreditations/ISO standards

In addition to this, our survey respondents from the workshop highlighted several SAQ resources that are readily available to certain sectors and these may be worth further investigation to prevent the "reinvention of the wheel" by generating your own in-house process or specialised excel version.

- Joscar Hellios
- Sedex
- Shared Assessment
- RiskLedger
- Whistic Vendor Security Assessment

However many of our survey respondents advised that they were working on an excel spreadsheet to manage the SAQ process, in order to capture information and to highlight risk.

Another key area for consideration is the number of questions that you feel appropriate to ask your suppliers, this has to take a manageable approach for your suppliers, whilst still offering the information that you need. A key discussion point from the workshop was "just how many SAQ questions is too many?" With responses varying from 50 questions on the SAQ to over 600, it is then easy to appreciate how suppliers could be weighed down with in-depth questions and therefore make the whole process slow and unresponsive.

Solutions provided on the day of the workshop as to how best to manage the number of questions in an SAQ offered a very clear response, some of the guest speakers highlighted their tried and tested systems that seemed to achieve the best response from suppliers.

Consider having more than one version of a SAQ

After classifying your suppliers, and before issuing any SAQ's think about what you are looking to achieve? What is your end goal? Is there a better way to interact with suppliers?...The solution is in the approach.

High risk supplier	Medium risk supplier	Low risk supplier
• Indepth SAQ • Site audit	• Moderate SAQ • Remote audit, pick up the phone or schedule a virtual meeting	• Light touch SAQ with no more than 20-50 questions • Monitor suppliers

Be realistic on the number of questions that you are asking suppliers to complete. Structure a more in-depth version of your SAQ for high and medium risk suppliers to complete and a light tough version for low risk suppliers.

Think logically, if you have a transactional supplier that may supply printer paper into your company would it be necessary to issue them with a SAQ with over 400 questions?

Try to keep the whole process humanised, be prepared to pick up the phone and give a supplier a call, audit where necessary.

For high risk suppliers book an audit, make sure that you connect with the supplier on a face-to-face environment and at their business premises.

Being on site with a supplier and understanding their operational processes, will support you with gathering snippets of information that you can explore in greater detail, this may open up conversations that may not be picked up on a paper based SAQ.

During your audit, be prepared to ask questions of the supplier and their workers. Work with your supplier to understand who feeds into their supply chain, from a cyber and ethical risk element these conversations will be invaluable and they will help you build a greater understanding of your supply chain.

Contract terms

Whilst CIPS is unable to offer exact legal contract terms, as these should be validated with your own legal team, it was a point of discussion from the workshop that factoring a "right to audit" into your contracts will be beneficial and should be a point of consideration.

Consider a term stating that your supplier is required under contractual terms to identify if they have an incident, identification of incident enables you to work closely with the organisation and to act quickly to prevent any impact on your own organisation.

Insert Cyber Security clauses into your contract, consider the NIS Cyber Assessment framework and GDPR compliance.

Less mature sectors have a tendency to rely on certification for the pass fail element of the certification, however, try to encourage your business to move towards annual audit of suppliers where necessary, this will ensure that the supplier is progressing risk profile. If you are depending on certification, then makes sure you are clear on what the certificate covers, but more importantly what it doesn't cover.

Knowledge paper and facilitating of the workshop

Sheena Donaldson (MCIPS Chartered)
Knowledge Manager at the Chartered Institute of Procurement and Supply (CIPS).

With special thanks to

Peter Yapp
Of the National Cyber Security Centre (NCSC)
for hosting the workshop and presenting and facilitating on the day.

Danny King

Martin Smith OBE

Of the Security awareness special interest group (SASIG), who are passionate about building a strong network of cyber specialists and running such insightful knowledge sharing events.

Also to all of the workshop attendees, who expressed such insight into their own progress and provided plausible solutions to the challenges that may be faced by other procurement and cyber security professionals who are supporting and managing the SAQ process within their organisations.