Aceni

White paper

Validating your Vendor

Six questions to ask before sharing personal data with a third-party supplier

Powered by Datagraphic

The importance of validating your vendor

Technological advances, such as smartphones, the Internet of Things (IoT), social networks, cloud systems, wearable tech; are making it possible to capture, process and share huge amounts of data on a truly global scale. The widespread and intensive use of data makes data security and protection critical requirements, especially with the introduction of the General Data Protection Regulation (GDPR) in May 2018. There is now, more than ever, an incredible amount of accountability on an organisation to protect and secure personal data.

When processing customer or employee data, it is not uncommon to share this data with third-parties in order to carry out certain processing requirements. However, before data is shared, the third-party vendor needs to be carefully selected and their credentials validated, forming a relationship that's based on trust, transparency and respect.

Establishing that your vendor is ISO 27001 certified is the first step to validating their credentials, but your vetting process should go much further.

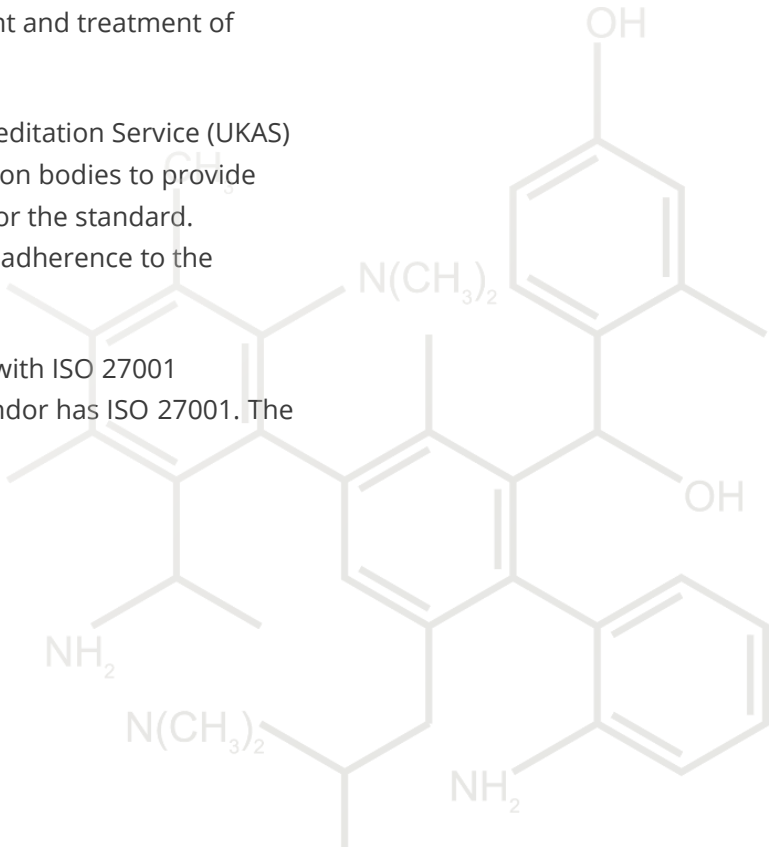
This white paper will help you understand the fundaments of ISO 27001 and provide you with six core questions to ask a potential vendor: so you can make an informed decision about who you select to share data with.

What is ISO 27001?

ISO 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS). It also includes controls for the assessment and treatment of Information Security risks.

The standard is written by ISO. The United Kingdom Accreditation Service (UKAS) is the national body that accredits independent certification bodies to provide certification, testing, inspection and calibration services for the standard. Consultancies, like Alcumus ISOQAR, then assess a firm's adherence to the standard.

The challenge for organisations looking to find a vendor with ISO 27001 credentials, is understanding the extent to which that vendor has ISO 27001. The levels of implementation can vary.



How an organisation becomes ISO27001 certified

1. DRAFT
In a relatively short period of time a firm can work with an ISO consultant to draft an ISO compliant manual.

2. PRACTICE
Once the manual is drafted, the next step is to bring it in to use, starting to work to the principles of the standard as a company *

3. CERTIFY
Stage three of the process is certification. A UKAS accredited auditor will visit the vendor to validate that the manual and processes are being followed.

4. SURVEILLANCE
The final stage is surveillance, where the vendor is independently checked annually by a UKAS accredited consultancy.

Be aware

* You might be surprised to learn that some vendors choose to stop their ISO implementation at this stage. Having completed part of the process they select to use wording such as “working to ISO 27001 standard” rather than gaining certification to the standard.

How to check a vendor’s ISO 27001 credentials?

If you buy or specify a third-party outsourcing partner to print and/or present online your data driven business documents, you’ll want to validate your potential vendor’s ISO 27001 credentials against the four stages of the process above.

The place to start, is to ask for a copy of your potential vendor’s ISO 27001 certificate. This document should include the scope and locations covered by the standard.

You can use details from the certificate to contact the ISO consultant to validate the certificate’s authenticity. You can also visit the UKAS website, to validate that the ISO consultant issuing the certification is UKAS approved.

Asking your potential vendor for the certificate including the scope and locations will help you verify a vendor’s claims. You should for example be able to see if the business processes you wish to purchase are within the scope and whether the location that work is to be delivered from is also within scope.

Having established your vendor’s ISO 27001 credentials the next step is to understand the scope of their data security provisions. Asking the following six questions will help you gain a deeper knowledge of the processes in place to protect your data during transfer, processing and storage.

Be aware

Some vendors reduce the scope of their ISO27001 certification to keep costs low for implementation and auditing.

#1 Who will be processing the data: third-party Sub-Processors?

Third-party Sub-Processor relationships often play a role in the success of an agreed service. A vendor may seek to work with Sub-Processors for all or specific parts of the processing. This could increase the number of points where your data is accessed: introducing potential risks.

As data protection laws start to increase scrutiny and control of third-party relationships, Sub-Processor arrangements should be carefully documented and managed.

It's vital that your vendor is transparent with you. Explicitly ask what third-parties will have access to your data and to what extent these Sub-Processors will be involved in the processing. Find out the stages that your vendor went through to ultimately choose those suppliers and what agreements are currently in place for data sharing. Request to see these agreements — often it's your right. Find out as much information on those third-parties and if need be, conduct your own security reviews.

The GDPR states that as a Data Controller, you "must be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject" so take time to understand who else is involved in the process.

#2 How are staff handling personal data trained?

The importance of internal Information Security training is often overlooked, but increasingly untrained individuals are opening their organisations up to being targeted for numerous cyber-attacks and damaging data breaches. In 2016, 33% of data breaches across the UK stemmed from an internal source.

Asking your vendor what Information Security training their staff has undertaken enables you to test the extent of which the topic of Information Security runs throughout the organisation. More often than not, Information Security sits within its own department or within the IT department, isolated from the rest of the company and its employees. It's so important that every person that works for your vendor is aware of their Information Security responsibilities as well as common attacks that take place within the industry, and how they should respond to them. Good training should consist of regular security updates, video tutorials and ongoing support and training.

The key is to ensure that training is continuous and isn't a one off presentation. Cyber-attacks come in many different forms and are always evolving so instilling an Information Security culture into a company, where everyone is fully aware, is very important. Organisations may have the most up-to-date security systems in place, but they could be of little use if staff aren't adequately trained.

#3 How will the risks from cyber-attacks be reduced?

Establishing your vendor's ISO 27001 credentials is a solid first step in demonstrating they have the systems and procedures in place to reduce or mitigate the risks of potential data breaches.

Your vendor should also be completing compliant risk assessments which are conducted on all information processing facilities. You have the right to see these.

Ask to see your vendor's Information Security Incident Management Procedure. This will detail what your vendor's process is if they were implicated in a real or suspected data breach. It's important to read the procedure and check what processes they have in place so you are aware of how breaches are handled and the steps the organisation takes to fix such breaches. A vendor's ability to react quickly and sensibly to a data breach is a great barometer of their overall approach to Information Security.

A vendor may develop the most technologically advanced and user-friendly application or service, but if their system is not regularly tested, how can they guarantee it's secure enough to protect the data it's holding? "Patching" is the process of updating software or an application to reduce or eliminate it's susceptibility to a known vulnerability. Examples could include various bug fixes that could be exploited to gain access to confidential information. Your vendor should be patching their systems regularly, so ask them what their frequency of Patching is.

A penetration test evaluates the security of the system or application by performing an authorised simulated attack. Its purpose is to uncover any vulnerabilities or weaknesses within systems to enable the supplier to then install measures to fix those issues. If you're using a vendor for Internet based systems or applications, it's vital that they are regularly conducting penetration tests and critically implementing fixes to identified vulnerabilities.

Cyber-attacks in 2017

Just under half (46%) of all businesses identified at least one breach or attack in 2017. The most common types of breaches related to staff receiving fraudulent emails (72%), followed by viruses and malware (33%).

Ask about these tests. Who is conducting them? Is the penetration testing being driven from within the organisation or are they using a third-party to bring expertise in? A human's mind is much better than a machine when attempting to replicate a data breach, so be cautious if your vendor describes their penetration tests as "completely automated". It's also important that you request to view a summary of the penetration test reports to not only see the vulnerabilities that have been found, but to ensure there's evidence that they have been fixed.

Penetration testing does cost money and many organisations do opt out due the significant investment involved. If your vendor doesn't penetration test their systems or it's obvious that the tests are not holistic, re-evaluate whether the vendor is worth working with. If they don't see the value in testing, they obviously don't value the importance of Information Security.

#4 How will data be securely transferred?

When sharing data with your vendor, encrypted communication links should be in place.

Encryption is an extremely useful and necessary tool to prevent breaches of Confidentiality and Integrity. A variety of encryption methods should be used based on the appropriateness of each method to the situation that it's being implementing within.

Sometimes several encryption methods can be used together to augment each other.

Secure File Transfer Protocol (SFTP) links are an excellent option. SFTP clients and servers automatically encrypt and decrypt all data that is transferred to and from them over the Internet. The older variant of SFTP namely FTP and unencrypted email when used alone should not be considered secure methods for transferring data.

If your vendor insists on using email for certain aspects of data transfer, then it is imperative you explore the techniques they have in place to tighten their email security. Email servers and Firewalls should be operated in a way that enables emails to be automatically encrypted, while they cross the public Internet. This Technology is known as Transport Layer Security (TLS). If information is being attached via email, then these attachments might also need to be encrypted. This can either be done by using PDF encryption technology or Zip file encryption.

Using Secure Socket Layer (SSL) certificates on websites also enables any Internet based communication with the sites to always be encrypted. Ensure your vendor has the most up-to-date certificates in place by checking that modern web browsers do not generate security warning messages. Pay close attention to the http/https prefix places before the web address. Be wary of sites that only switch the "https" after you have submitted your username and password. This is bad practice as credentials should only be transmitted over encrypted connections.

It's important to note that an organisation's use of encryption should be constantly evolving. Reviewing new and emerging encryption technologies should be at the forefront of your vendor's security management plan.

What is Encryption?

Encrypted data is, in effect, random noise. Whilst in encrypted form data ceases to be data. It is only when it is successfully decrypted that it becomes meaningful data once more. Encrypted data must be decrypted before anything practical can be done with it.

#5 Business Continuity and Disaster Recovery, what's plan B?

While some business owners like to believe that they can quickly come up with a "Plan B" to work through a crisis, the best corporate leaders spend time making plans for events they hope will never happen.

A power cut, a network failure, a technical glitch: a Business Continuity plan details the necessary controls required to enable the company to continue to operate. It will ensure systems and procedures are in place to respond quickly without any compromise to the security of customer data. It should be business as usual.

So ask your vendor how they provide availability for the systems that you will be relying on? Have all single points of failure been explored and then eliminated? It's important you find out from your vendor whether they have multiple Internet connections and whether they are able to replicate their information processing facilities between different hardware.

Also ask whether they have a backup power source and have also protected their critical equipment with uninterruptable power supplies (UPS). UPSs are often required to "smooth" the transition between "National Grid" failure and on-site power generators.

Some organisations outsource their business continuity to a third-party. While it's good that they have provisions in place, they often have to wait for that third-party to turn up and fix their systems, with valuable time being wasted.

It's also important you request to see your vendor's Disaster Recovery procedure. DR allows an organisation to maintain or quickly resume mission-critical operations following a natural or human-induced disaster.

In simplistic terms think of Business Continuity controls as ways an organisation can continue functioning when key elements fail. Think of a Disaster Recovery plan as how an organisation continues functioning when site closures occur.

As a Data Controller, you have a responsibility to your data subjects to ensure that the Confidentiality, Integrity and Availability of their data is never compromised and that the service you originally agreed to can continue to be provided. This is why ensuring your vendor offers Business Continuity and Disaster Recovery plans is a vital step in your validation process.

#6 What will happen to the confidential data when processing ends?

CDs, USB sticks, electronic files, confidential data can be transferred and stored on different media, but what happens to that data when processing ends?

It's vital data files are deleted/destroyed at the end of processing. Agree a data retention period with your vendor and ask what their process is for disposing of media containing confidential Information. If they are certified to ISO 27001, they should have in place a Secure Disposal Policy which defines the procedures they follow.

Remember that data is often also present on non-electronic media such as paper documents. How are these being disposed of when no longer required? It's best practice to cross shred documents containing personally identifiable information when no longer needed. There's even a British Standard in secure shredding that defines the maximum dimensions of the resultant shreds.

To ensure items are always properly disposed your vendor should also keep log information, listing who performed the procedure, when, and what method was used.

This white paper has been prepared for you by Datagraphic, a secure UK Strategic Document Outsourcing (SDO) company.

Datagraphic's Aceni suite – six powerful Software-as-a-Service (SaaS) applications – has been developed to transform the way organisations securely automate, control and output time-critical communications.

Learn more:

+44 (0)1246 543000
sales@datagraphic.co.uk
datagraphic.co.uk

Registered companies: Datagraphic Group Limited (Reg No: 01215380) and Datagraphic Limited (Reg No: 02913191). Both registered in England at: Ireland Industrial Estate, Adelphi Way, Staveley, Chesterfield, S43 3LS.