
KPMG
Private Enterprise
Startup
cyber
guide
kpmg.com

Contents

Introduction

UK SMEs are underestimating the impact a cyber attack could have on their reputation and must take steps to protect it – this was one of the key findings of the Government's report on Small Business Reputation and the Cyber Risk.

Traditionally cyber security has been a risk associated with big business, as the threats have come from sophisticated hackers. However, as the global digital landscape has become more accessible, the range of threats has extended and protection cannot be taken for granted.

At the same time, the availability, scalability and convenience of cloud services have meant that these solutions have become the norm for startups who are looking to rapidly and economically build their IT infrastructure. Many of these services have aspects that are open to the wider public and hold sensitive data. Cyber security is therefore becoming a risk that needs to be considered early on for a fast-growing company.

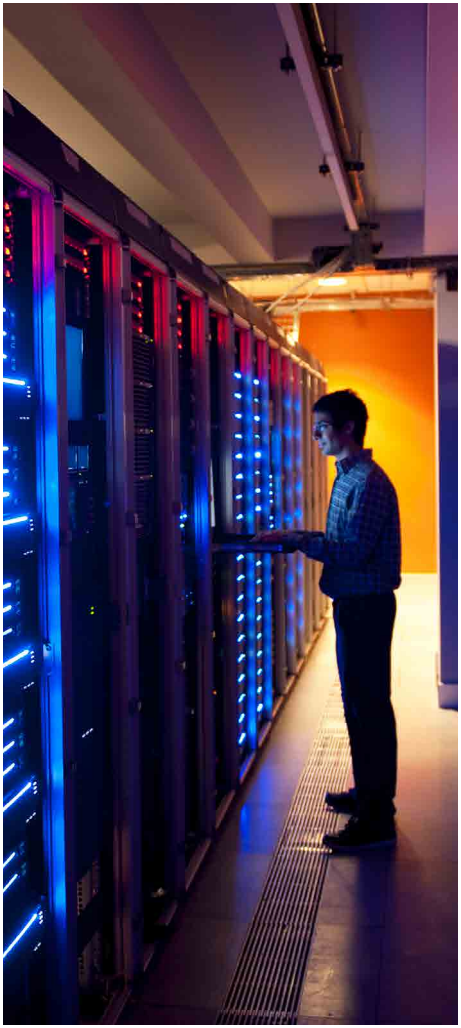
Cyber security is by no means an all or nothing approach but should be something that scales as the business grows. Over the next few pages, we aim to demystify some of the key elements of cyber security that are relevant for fast-growing tech businesses and help you ensure that you are starting to take the necessary steps to improve your cyber security environment.

Cyber security is becoming a risk that needs to be considered early on for a fast-growing company.

What is cyber security?

Put simply, cyber security is about an organisation's ability to protect its information assets and its preparedness against cyber threats.

This takes into account a rounded view of people, process and technology to reduce vulnerability and the long term impacts of any breach.



Why is cyber security important for your business?

In the digital economy, the valuation of a business is based heavily on its intangible assets, whether this is digital intellectual property (IP), customer information, transactional data or other similar data assets.

A breach of this data could lead to competitors gaining access to valuable IP, loss of customer trust and/or potential legal and financial implications. For this reason, growing companies can't afford to ignore cyber security.

A breach of this data could lead to competitors gaining access to valuable IP, loss of customer trust and/or potential legal and financial implications.

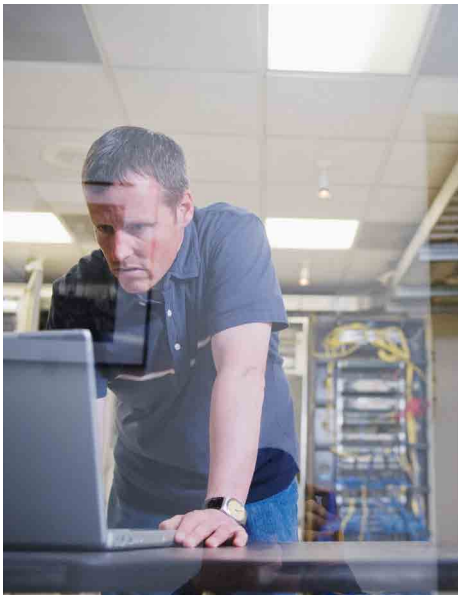
Penetration Testing

What is it?

Penetration testing (also known as pen testing) is the process by which a computer system, network infrastructure, native application and/or web application is tested to find vulnerabilities that a hacker could exploit.

Pen tests can be automated using tools that can scan your IT environment to identify possible vulnerabilities, or can be performed manually by "ethical hackers." The goal is to identify any vulnerabilities, ascertain what they are, where they are and provide recommendations to fix them. This exercise provides the insight and feedback necessary to protect the IT environment against an external attack.

As well as aiming to identify technical weaknesses, penetration tests can look to identify weaknesses in an organisation's security policies, behaviour and culture.



Why would I need it?

Many startups are not fortunate enough to have developers that are experts in software development **and** security. Software development best practice is to comply with the principles of building solutions that are secure by design. However, it is almost impossible to anticipate the actions of a knowledgeable or resourceful hacker. A penetration test will allow you to simulate, in a safe environment, a malicious attack and ensure that you minimise the chances of them being successful. It also signals to your clients that you are taking IT security seriously and in some cases will allow your clients to rely on the certification issued by your penetration testers.

Software development best practice is to comply with the principles of building solutions that are secure by design. However, it is almost impossible to anticipate the actions of a knowledgeable or resourceful hacker.

How do I go about getting it?

A number of organisations will offer penetration testing services at various prices. The key things to keep in mind when choosing your supplier are:

Is the organisation reputable?
In some cases you are giving them quite sensitive access to your system; do you trust them with this?

What is the technical expertise of the testers?
Your penetration test is only as good as the technical expertise of those carrying it out. An organisation with highly skilled penetration testers is likely to find vulnerabilities that may be harder to spot.

What does the test mean to your customers?
The results of some penetration tests are worded in such a way that they can only be relied upon by the organisation commissioning the test. If you want to be able to use the certificate when negotiating with customers, you may need to find an organisation of testers who can issue a certificate that can be relied upon by third parties – this is often more expensive.

Cyber Essentials

What is it?

Cyber Essentials is a scheme set up by the UK Government to provide businesses with clarity on good, basic cyber security practices. It is mandatory for Central Government contracts that involve handling personal information and/or providing certified IT products and services, but it also acts as a baseline for other business selling outside of the public sector.

Why would I need it?

Depending on the industry that you are working in, some clients will require you to be accredited under the Cyber Essentials programme. When not specifically required by your clients, Cyber Essentials demonstrates that you are performing the basic requirements and complying with a widely acknowledged cyber security baseline. It is often seen as the first step on an organisation's roadmap towards their desired level of cyber security and is a good place to start in order to understand where your weaknesses may lie.

When not specifically required by your clients, Cyber Essentials demonstrates that you are performing the basic requirements and complying with a widely acknowledged cyber security baseline.

How do I go about getting it?

There are two levels of accreditations that an organisation can get under Cyber Essentials:

1. **Cyber Essentials:** This requires the organisation to complete a self-assessment questionnaire, with responses independently reviewed by an external certifying body.

2. **Cyber Essentials Plus:** As well as the requirements of Cyber Essentials, tests of the organisation's systems are carried out by an external certifying body, using a range of tools and techniques.

Information on both levels can be found on the UK Government's Cyber Essentials website.

ISO 27001

What is it?

ISO 27000 is a global family of standards relating to Information Security Management. Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details and information entrusted to you by third parties. ISO 27001 is the best known standard in this family, providing requirements for an Information Security Management System (ISMS).

The standard covers a variety of areas including physical and environmental security, information security policies, access control and operations security. Once a company has been certified as ISO 27001 accredited, they will undergo recurring audits to ensure compliance is maintained.

Why would I need it?

ISO 27001 is a widely recognised accreditation that many large organisations will require from their suppliers. This is often because they are certified themselves and will want assurances that any sensitive data processed externally is done in a controlled environment.

In an environment where accreditation is not required, ISO 27001 compliance will often provide a market edge and demonstrate that you take customer data security seriously. It will also lower the risk of data breaches from accidental or malicious incidents and ensure that appropriate processes are in place for managing these incidents.

ISO 27001 is the best known standard, providing requirements for an Information Security Management System (ISMS).

How do I go about getting it?

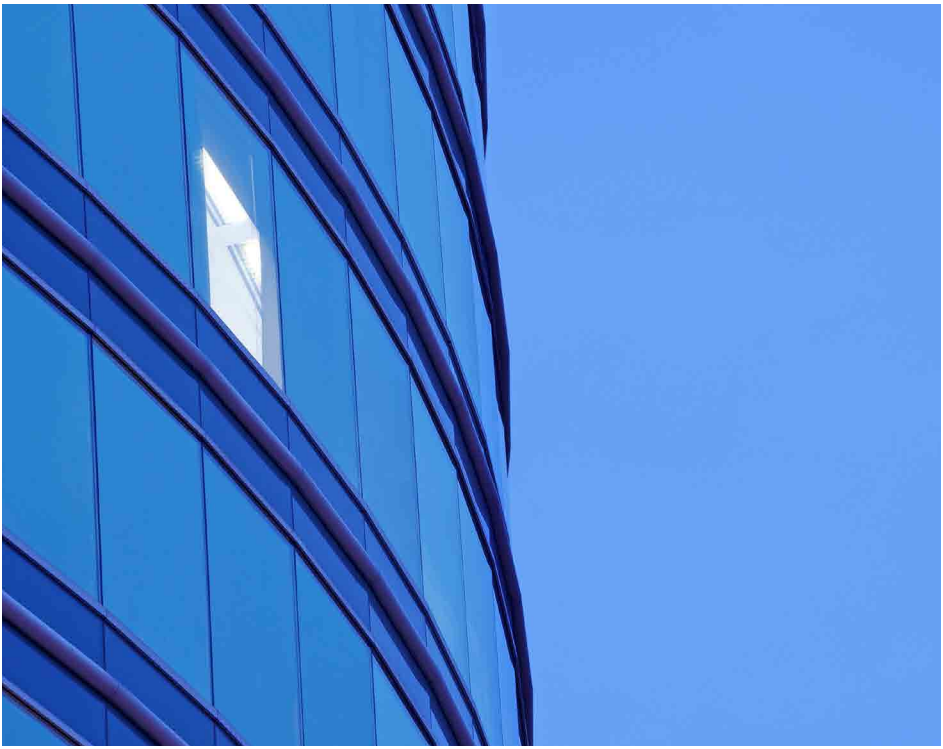
For many, ISO 27001 is seen as the natural progression after Cyber Essentials, which will help to lay the groundwork for your ISMS

It is rare that a company will be ready for an ISO 27001 audit immediately. A number of external organisations can therefore come in to assess your ISMS and conduct a gap analysis against the ISO 27001 controls. They will then work with you to produce a remediation plan to help you get up to the required standard.

When ready, you can undergo a formal audit, where the implementation of the ISMS will be assessed to ensure it is operating effectively, as required by ISO 27001.

When you have passed the formal assessment you will receive an ISO 27001 certificate, along with a statement of applicability which denotes the controls you have been audited against. This is valid for three years, within which you will receive regular visits to ensure you remain compliant and continually improve your ISMS.

When choosing your ISO27001 auditor, it is important to choose an auditor who is reputable in the market – you may find that many large corporates will only recognise audits that have been conducted by specific auditors.



PCI DSS Compliance

What is it?

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organisations that handle branded credit cards from the major providers. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.

The standard represents a common set of requirements to help ensure the safe handling of sensitive payment card information. Compliance with the DSS is reported to the merchant's acquiring bank.

Why would I need it?

The PCI DSS applies to any organisation, regardless of size or number of transactions, that accepts, transmits or stores cardholder data. The number of annual transactions being processed will define the "Merchant Level", which range from 1-4 and are set by Visa.

Organisations that are not compliant may be liable for non-compliance fines if they do not work towards compliance with their merchant bank (known under PCI DSS as the acquirer). Ultimately, the acquirer may be forced to terminate the relationship, which will prevent the organisation from accepting card payments.

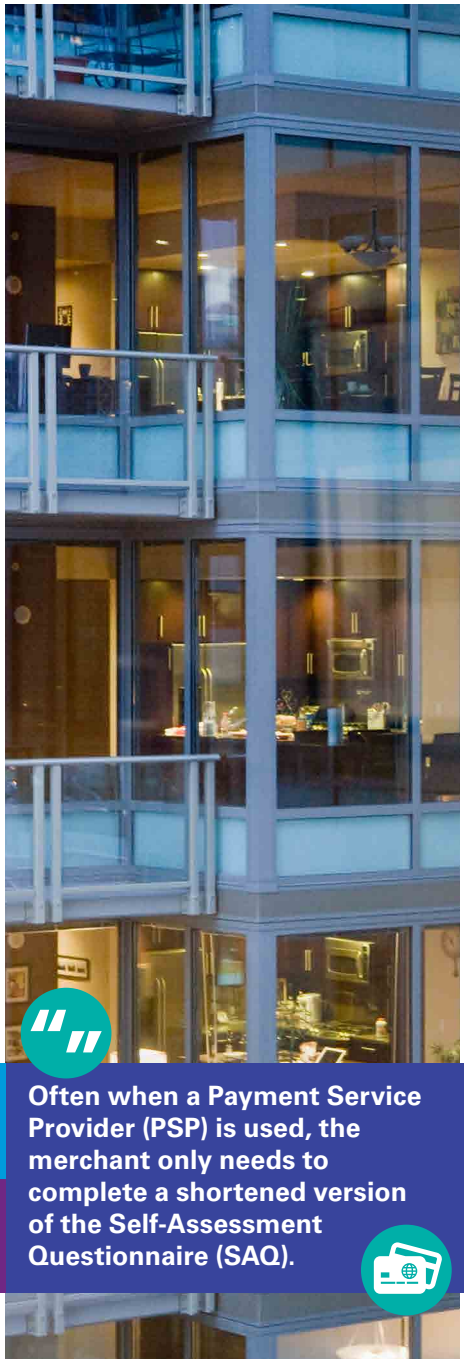
The PCI DSS applies to any organisation, regardless of size or number of transactions, that accepts, transmits or stores cardholder data.

How do I go about getting it?

The first thing an organisation needs to do is fully understand how they process card payments. In particular, if the e-commerce environment is capturing, storing, processing or transmitting card data then they should think very carefully whether this is really necessary.

The most secure approach to processing e-commerce transactions is to outsource your card data to a Payment Service Provider (PSP). When the card data is outsourced, it is totally segregated from your environment and consequently the capturing, processing, storage and transmission of card data is totally removed from your e-commerce environment. This is commonly known as a 'fully hosted solution.' Often when a PSP is used, the merchant only needs to complete a shortened version of the Self-Assessment Questionnaire (SAQ). The criteria for this can be found under Part 2g of the PCI Security Standards SAQ A form.

If a PSP is not an appropriate solution, the organisation needs to consider the twelve high level requirements of PCI DSS, which fall into six categories. These cover: building and maintaining a secure network, protecting card holder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy.



Often when a Payment Service Provider (PSP) is used, the merchant only needs to complete a shortened version of the Self-Assessment Questionnaire (SAQ).

Third Party Controls Reporting

What is it?

Organisations are increasingly outsourcing activities to third party service providers. It is often difficult for an organisation to monitor the actions of the third party and this can introduce risk.

A third party assurance report, also known as a Service Organisation Assurance Report (SOAR), demonstrates an appreciation of clients' risks through obtaining third party assurance on effective processes and controls under an established international framework.

Why would I need it?

If you have outsourced certain aspects of your business to a service organisation, it may be important to you and your customers to know that the service organisation is following formal processes and policies when handling your data. In this scenario, you would want to obtain a SOAR report from your suppliers covering their processes.

On the other hand, if you are acting as a service organisation to your clients, they may require you to be covered by a SOAR report.

In both scenarios, the requirement may be the result of regulation that is specific to your industry, or may otherwise be a requirement of the procurement frameworks enacted by your clients.

If you have outsourced certain aspects of your business to a service organisation, it may be important to you and your customers to know that the service organisation is following formal processes and policies when handling your data.

How do I go about getting it?

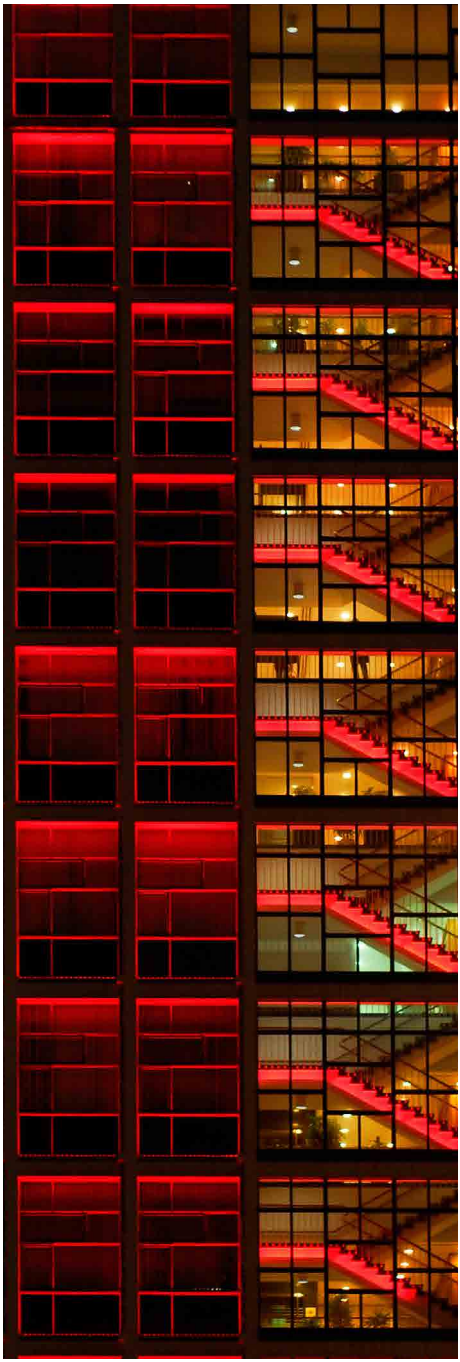
The main international reporting standard for SOAR is ISAE 3402. There is also an American standard, which is similar to ISAE 3402, known as SSAE 16 (which superseded SAS 70).

Unlike ISO 27001, there is no standard set of processes or controls that are covered by a SOAR report. The service organisation will work with the auditors providing assurance to draw up a relevant set of controls that will be adhered to and audited.

Under both reporting standards, there are two types of report:

Type 1: This is a snapshot, single point in time, view. It assesses the design of the controls and whether they are suitable to cover the control objectives set out in the agreed framework. An independent report will be issued for that agreed date.

Type 2: This will cover a consecutive period of 6 months or more, and will assess the design and effectiveness of the controls, set out by the agreed framework, during that period. This includes the steps involved in the Type 1 assessment plus the additional evaluation of the operating effectiveness of the controls.



Business Continuity and Disaster Recovery (BCDR) Planning

Drawing up policies that define ownership and processes during an incident, as well as testing how your business would react to a real incident, are all good ways to start planning.

What is it?

Business continuity and disaster recovery (BCDR) planning are the set of terms that cover the preparation and testing of measures that protect your business operations in the event of a disruptive incident.

Planning will cover the governance and processes related to an incident, such as who would contact and inform staff, where staff would work and how clients would be notified, as well as the technology in place, such as automated backups, fall-back servers and monitoring systems.

Why would I need it?

Would your business incur significant costs during a period of downtime? Is the availability of timely information essential to your processes and those that rely on them? Do your staff and/or clients expect uninterrupted services from you?

Unexpected incidents, natural disasters, and malicious intent may disrupt information availability and negatively impact key business processes, causing lost revenue and adverse reputational damage.

As your company scales and your customers rely heavily on uninterrupted service, BCDR planning helps you to ensure that the appropriate procedures are followed in the event of a service-disrupting incident, minimising risk, time offline and financial losses.

How do I go about getting it?

Organisations will often have their own BCDR plans which they will work towards. However, if a more formal approach is desired, Business Continuity is covered by the ISO 27031 standard and Disaster Recovery by the ISO 27031 standard, which organisations can be accredited against. Aspects of BCDR can also be included in a service organisation assurance report.

You do not need to have reached a particular company size before you start thinking about business continuity and disaster recovery. Drawing up policies that define ownership and processes during an incident, as well as testing how your business would react to a real incident, are all good ways to start planning.

Cloud Hosting

What is it?

In its simplest terms, cloud computing is an IT delivery model where computing resources can be delivered on a pay-as-you-use basis over the Internet. It allows providers to benefit from economies of scale, while giving smaller organisations access to high performance IT equipment and services.

Large and small organisations now have the confidence that the cloud offers the cost-effectiveness, agility and security necessary to support digital services across both public and private sectors. However, there often remains a lack of awareness of the nature (and associated risks) of cloud computing, potentially jeopardising future competitiveness or limiting an organisation's potential client base.

There often remains a lack of awareness of the nature (and associated risks) of cloud computing, potentially jeopardising future competitiveness or limiting an organisation's potential client base.

What are the different cloud models and associated services?

Private Cloud – With a private cloud, organisations build their own dedicated cloud infrastructure. This dedicated infrastructure could be procured, built and managed by the organisation or it could be provided to the organisation by a third party – either on-site or in a remote data centre. The advantage of private cloud infrastructures is that they can be more straightforward to secure as no other customers of the cloud provider have access to the dedicated equipment.

Community Cloud – Organisations can reap many benefits from working together through a community cloud strategy. The shared service model is well-

established within many sectors and the development of community clouds, based on organisational families with common standards, security needs and regulatory constraints, are a logical extension.

Public Cloud – A public cloud service provider makes applications, data storage capacity and other resources available to organisations or the general public using its own servers. Public clouds offer all the advantages of rapid service deployment and utility pricing. Public clouds can also be very secure and in many cases do not operate on a global, or even cross border basis, i.e. they are based within a single nation.

Hybrid Cloud – Hybrid cloud balances the use of different cloud deployment models and can offer organisations the advantage of flexibility and scalability. Hybrid cloud allows organisations to balance isolation, cost and scaling requirements. One obvious consideration about the hybrid model, which is often missed, is that if data is suitable to go to the public cloud at times of peak demand, why not just operate in the public cloud at all times? Typically however, the hybrid model is often used as a stepping stone towards full adoption of the public cloud model once any remaining reservations or concerns have been addressed through experience.

Infrastructure as a Service (IaaS) – IaaS generally allows users to provision a virtual infrastructure for the processing and storage of data. Organisations can deploy a variety of virtualised servers in a flexible and easily changeable configuration.

Platform as a Service (PaaS) – PaaS provides users with the ability to develop and deploy applications of their own choosing on to a pre-configured "platform". In essence this means that the providers are responsible for the security and maintenance of the underlying virtualised infrastructures that provide the platform.

Software as a Service (SaaS) – SaaS delivers business applications for a usage or subscription-based cost at an agreed service level. In other words, organisations can make use of a shared service, such as a finance application or e-mail service, which removes any requirement for the organisation to develop and secure its own application and infrastructure (although a level of configuration effort will likely be required).

What are the key questions I should keep in mind?

How sensitive is the data, and what are the necessary minimum security controls?

How critical is the service to our organisation, partners and customers?

Is the data subject to regulation?

Do privacy restrictions apply?

How is the confidentiality, integrity and availability of data maintained?

Where is the data stored?

If the data is stored off-shore, are the additional legal implications and risks assessed and understood?

Can the data be encrypted in transit and/or at rest?

Who generates, holds and distributes the encryption keys?

Where is the data encrypted?

How can you make your users' access to cloud services seamless yet secure?

What is the reliability and security of the cloud provider?

Can the data and service be easily moved to another provider?

Does the provider preclude us from conducting our own penetration testing of our services?

Is the provider and service compliant with applicable regulation?

Is the cloud contract fit for purpose and compliant with all applicable regulation?

EU General Data Protection Regulation (GDPR)

What is it?

The EU GDPR came into effect on 25 May 2018. Whilst the UK will be leaving the EU, the GDPR relates to all EU citizens, and therefore companies will be required to comply if they transact with EU citizens.

The regulation increased fines for privacy breaches to up to 4% of a business' global turnover – transforming privacy into a top ten risk for most organisations.

How does it impact me?

GDPR has impacted everyone, from SMEs all the way up to large multi-national corporations. In order to identify problems correctly, organisations need to ask themselves the right questions. Some of the following should be at the top of your mind and may help you recognise how privacy plays an integral part in your business:

The regulation increased fines for privacy breaches to up to 4% of a business' global turnover

Do I understand my business' privacy obligations, its risks and whether our compliance strategy is fit for purpose?

Am I making sound decisions and plans with regard to technology and business initiatives involving personal information (e.g. customers' and employees' data)?

Do I have a clear view of what personal information is being processed, where, by whom and for what purpose?

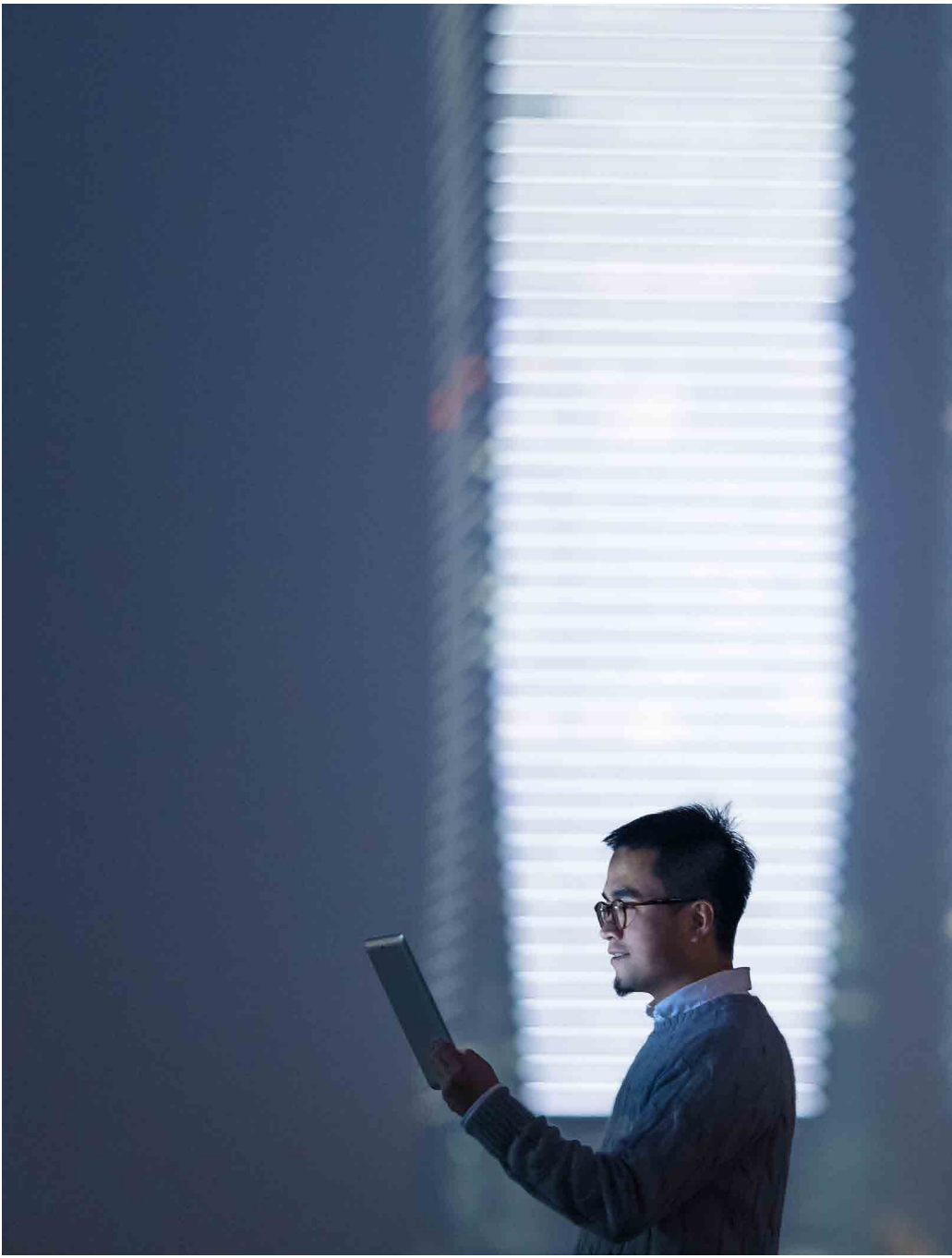
Am I confident in my organisation's ability to detect and manage a data breach effectively?

Do I monitor both internal and third-party supplier compliance in respect of privacy and security?

How does the EU Privacy regulation impact our business operations and risk appetite?

What were the key changes?

	Data Protection Act	GDPR
	**Fines** Fines vary by jurisdiction (e.g. UK £500,000)	**Fines** A tiered fining structure depending on infringement. Level 1 is 2% of global turnover or €10m (whichever is higher). Level 2 is 4% of global turnover or €20m (whichever is higher)
	**Data Protection Officer (DPO)** May have had to appoint a DPO depending on jurisdiction	**Data Protection Officer (DPO)** DPO required for 'government bodies' and organizations conducting mass surveillance or mass processing of Special Categories of data
	**Inventory** Generally there was no need to maintain an inventory of Personal Information	**Inventory** Generally organizations need a personal information inventory
	**Breach Notification** May have had to report Privacy breaches depending on jurisdiction	**Breach Notification** Requirement to report Privacy breaches to the regulator within 72 hours and potentially to the Data Subject
	**Security** Vague requirements around security (i.e. 'adequate level')	**Security** Explicit requirements around monitoring, encryption and anonymization
	**Privacy Impact Assessments (PIAs)** Generally did not have to perform PIAs	**Privacy Impact Assessments (PIAs)** Companies must perform PIAs if the activity is considered 'high-risk'
	**Data Subject's Rights** Right to request a copy of their data	**Data Subject's Rights** New rights including the Right to Data Portability and the Right to Erasure
	**Sensitive Personal Data** This covers things such as political opinions and religious beliefs	**Sensitive Personal Data** 'Special Categories' replace 'Sensitive Personal Data', and includes biometric and genetic data
	**Consent** Potential to rely on "implicit" consent depending on jurisdiction	**Consent** Requirement to gain unambiguous, explicit consent when there is no other legal basis for processing
	**Data Processors (DP)** Processors were subject to limited scope and liability	**Data Processors (DP)** Processors are also covered in scope; controllers must conduct due diligence into processors' suitability



KPMG
Private Enterprise

Contact us

Tech Growth

Patrick Imbach
Director
M: 07766 780 861
E: patrick.imbach@kpmg.co.uk

Eden Dwek
Manager
M: 07876 397 177
E: eden.dwek@kpmg.co.uk

Technology & Cyber Risk

Richard Krishnan
Director
M: 07770 494 840
E: richard.krishnan@kpmg.co.uk

Laurenz Hussain
Manager
M: 07843 683 657
E: laurenz.hussain@kpmg.co.uk

www.kpmg.com

CRT0070002L | June 2018