PKF
FRANCIS
CLARK
Shared Ambition

Cyber services

Cyber threats continue to develop and evolve exponentially. Your organisation can take proactive and measured steps towards a more secure 'cyber secure' world.

Cyber maturity journey

Cyber threats continue to develop and evolve exponentially. Your organisation can take proactive and measured steps towards a more secure 'cyber secure' world.

	Where you are	How we can help
Stage 1	• Insufficient time and expertise in-house to assess IT and cyber risks • We have outsourced processes and systems, so everything is in-hand	Talk to us, we can help you to understand why you need to be aware of the issues. We can look at the risks to your organisation and assess your next steps. We can work with you to map out your cyber maturity journey and make it relevant to your organisation.
Stage 2	• Awareness that cybercrime is a real threat and some knowledge of general risks to the organisation • Some controls and processes in place but have never tested or do not formally test them	Your cyber maturity journey has already started. We can work with you to understand where you are at on that journey and where you would like to get to. Cyber Essentials PLUS is a fully audited assessment, testing your systems and devices provides you with independent assurance using a nationally recognised baseline.
Stage 3	• Begun cyber implementation plan but wanting further assurance • Formalisation of policies and procedures around cyber security are starting to be implemented	IASME Cyber Assurance is a great way to show your Board/Trustees, customers, suppliers (and more) that you take cyber security seriously in your organisation. Vulnerability management services are a great way to proactively manage external threats to your organisation and stay on track for your cyber implementation plan
Stage 4	• Seeking ongoing assurance your systems are protected	We can manage your vulnerability scanning and reporting to suit your needs and demands. We provide industry recognised reporting, but tailor it to meet your needs and audiences. Undertake a detailed attack vector analysis and find out ways in which external threats could become realised.
Anytime on your journey	• Seeking bespoke assurance projects	At any stage of your cyber journey we'd love to have a conversation about how we can meet your demands and needs, whether that be providing training to your staff, providing point-in-time assessments and vulnerability scans, helping you to align to specific standards like PCI-DSS or anything else.

Detailed attack vector analysis

Detailed attack vector analysis

What are attack vectors?

- Attack vectors are the different methods of gaining unauthorised access to an IT network or computer system
- An attack surface is the total number of attack vectors a cyber attacker can use to access a network and extract data
- This service seeks to understand many ways in which cyber attackers will attempt to access your network and systems, identify, and assess the severity of weaknesses identified, and provide detailed feedback on what should be remediated

Why should you seek this service?

- A team of professionals will provide a friendly and professional service, working with key individuals in your organisation to provide a quality and information-rich output
- Gain an understanding of your IT estate. Building knowledge of your physical devices and your operating systems and software
- Formally take responsibility and accountability for cybersecurity in your organisation
- Communicate effectively to your organisation on the collective responsibility for cybersecurity
- Provide assurance to your Board, employees, customers, vendors and interested parties that you are taking proactive steps towards a positive cybersecurity posture

What is included in a detailed attack vector analysis?

- External vulnerability scan
- Web application scan
- Domain squatting assessment
- Internal vulnerability scan
- Mobile device assessment
- Email security configuration assessment
- Credential compromise analysis
- Social networking and engineering analysis

What is included in a detailed attack vector analysis?

Refer to page 20 and contact our Director of IT Audit, Assurance and Cybersecurity.

We also perform this service as part of financial due diligence processes to provide valuable insight to the buyer.

Cyber and information security certifications

Cyber and information security certifications

Cyber Essentials verified self-assessment (VSA)

A good start…

- An excellent starting point to help ensure you have the basic security measures in place to safeguard against c.80% of the most common forms of cyber-attack
- Nationally recognised baseline cybersecurity standard
- A team of qualified assessors will be on hand to guide you throughout the process
- Qualifies your organisation for free cyber insurance[1]

Unsure if your organisation will pass the assessment?

- Undertake a readiness assessment with our team of assessors. Receive feedback and recommendations on how to achieve compliance with the standard

Cyber Essentials PLUS (CE+)

Testing that your technical controls are fit for purpose

- An industry-agnostic benchmark certification for all organisations to achieve to address the most common forms of cyber-attacks
- A highly recognised certification across all industries and insurance providers
- Identify critical weaknesses in your IT infrastructure before an attacker does
- Promotes credibility and reputation of your organization. Shows customers that you take the security of their data seriously
- A prerequisite when bidding for government contracts. It can provide additional organisational opportunities
- Our qualified assessors conduct seven tests across your technical and system controls
- Qualifies your organisation for free cyber insurance[1]

What is included in a detailed attack vector analysis?

Refer to page 19 and contact our Director of IT Audit, Assurance and Cybersecurity.

We also perform this service as part of financial due diligence processes to provide valuable insight to the buyer.

Cyber Assurance – Level 1 (self-assessment)

Assessing information security across your organisation

- Cyber Assurance (CA) assesses the formality of your information security and governance processes
- CA goes further than the Cyber Essentials scheme and assesses policies and procedures in place to respond to a data breach or cyber-attack
- Critical to ensuring you have the appropriate safeguards to protect against a data breach
- Qualified assessors will be on hand to guide you through the process

Cyber Assurance – Level 2

A comprehensive assessment of your people, policies, and procedures

- An affordable and achievable standard for SMEs, an alternative to other internationally recognized standards
- Accepted by the UK Ministry of Justice as an appropriate certification standard to maintain
- Assess your compliance status with UK Data Protection Act 2018 (UK DPA) and UK General Data Protection Regulations (UK GDPR)
- Our qualified assessors will review your information and interview heads of departments to assess how you identify, classify, and protect data, detect, and deter unauthorised access, and how you respond and recover to incidents
- Reassure your customers and client base that you are taking proactive steps to keep their data and personal information as secure as possible
- A formal report is issued on your organisation, evidencing adherence to the standard
- A triennial certification[2]

Vulnerability scanning and patch management services

Vulnerabilities an overview

Vulnerabilities – an overview

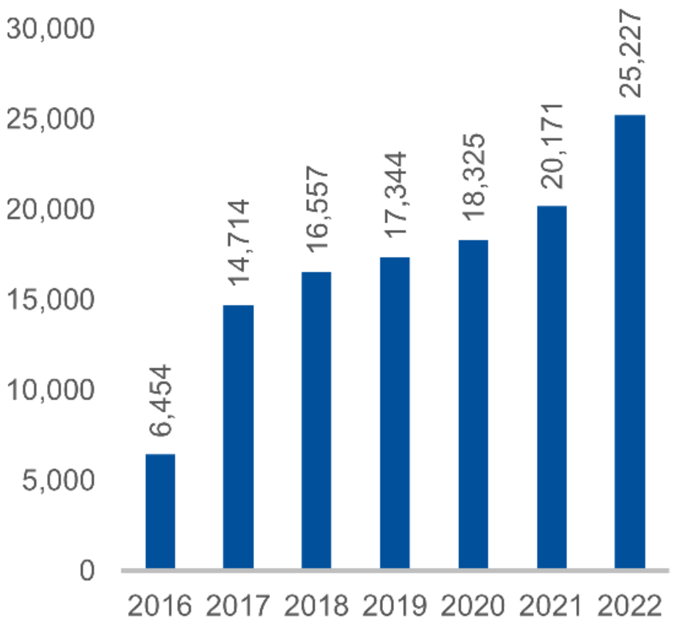
What are vulnerabilities?

- A vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack
- They can occur through flaws, features or user error, and attackers will look to exploit any of them, often combining one or more, to achieve their end goal
- They can arise through:
  - Poor design and mistakes during implementation
  - Functionality which can be misused by an attacker
  - Making mistakes (human error)
- In 2022, there were 25,227 vulnerabilities identified. This is an increase of nearly 20% on the previous year
- Vulnerabilities are on the increase with over 7,000 vulnerabilities identified in Q1 2023
- New vulnerabilities are identified daily. By performing a vulnerability scan, you identify vulnerabilities and can fix them before they become a longstanding issue

Getting on top of vulnerabilities

- Contact our specialist team to conduct vulnerability management services on an ongoing basis to provide you the assurance you require
- Focus your time and attention on remediating the vulnerabilities and allow our team to focus on identifying and reporting them to you
- Better prioritise and organise your vulnerability remediation/patch management strategy with criticality scorings
- Gain an understanding of your IT estate. Building knowledge of your physical devices and your operating systems and software
- Communicate effectively to your organisation on the collective responsibility for cybersecurity

Vulnerabilities over time



Web application scanning an overview

Web application scanning – an overview

What is web app scanning?

- Web app scanners are software specifically designed to assess an organisation's internet-facing websites and web assets to identify potential vulnerabilities
- A web app scanner simulates hacking attacks to reveal potential weaknesses in a web application's configuration. This enables organisations to assess and remediate the vulnerabilities prior to attackers exploiting them
- It is difficult to catalogue an organisation's complete inventory of websites and web assets
- Discovering and cataloguing an organization's entire inventory of web assets. A web app scanner supports organisations in identifying and cataloguing all web assets to support an environment where they can be actively managed

Why is web application scanning important?

- According to the 2022 Verizon Data Breach Investigation Report, basic web applications were the top attack vector
- As an attack vector, they were a far more common method of attack to an organization than other well-known and expected exploits such as email and software updates
- More than 25% of organisations knowingly ignore critical security flaws due to not knowing how to fix them or not having the required time to investigate them

Internal vulnerability management

Monitor your desktops, laptops and servers

Continuous vulnerability scans are the core of an organisation's security strategy. They provide regular IT security health checks to your organisation to facilitate effective and swift decision making. Cybersecurity is most effective when performed proactively.

- Detailed scans of your network to identify all devices including laptops, desktops, and servers (including devices used by remote workers)
- We conduct an agent-based scanning service, which has a negligible impact on your day-to-day business and operations
- The agents are deployed on each device in a non-intrusive manner, and devices provide an update to our management system every 15 minutes
- We will liaise with you throughout the process to understand any sensitivities or individual requirements related to your system architecture
- We report to you on a frequency which is chosen by you (commonly monthly) to help you keep on top of vulnerabilities across your IT estate
- We can provide bespoke reporting, cutting down on the jargon and getting right to the issues, making it great for sharing with your Board

External vulnerability management and web application scanning

Monitor your websites, ports, and routers

Websites are always the face of an organisation, and with a new attack happening every minute, more than 30,000 websites are successfully breached each day.

- Using state of the art technology, we utilise the same techniques as an attacker to provide either a point in time, or ongoing scan(s), capable of identifying weaknesses within your website
- We will provide a full report of the vulnerabilities identified ranked according to their risk rating. We also provide recommendations for every vulnerability or misconfiguration identified in an easy-to-understand format
- We will liaise with you throughout the process to understand any sensitivities or individual requirements related to your web architecture
- We report to you on a frequency which is chosen by you (commonly monthly) to help you keep on top of vulnerabilities across your web assets
- We can provide bespoke reporting, cutting down on the jargon and getting right to the issues, making it great for sharing with your Board

Risk based vulnerability management (RBVM)

Focus on the vulnerabilities that matter

Risk based vulnerability management is a way for your organization to effectively prioritize the most critical and urgent vulnerabilities. Let us give you more time to focus on the areas that matter most to your organisation.

What is different about RBVM?

- We understand your network infrastructure to identify assets and the information, which is most critical, and most exposed.
- We provide a bespoke accompaniment to the vulnerability management report, leveraging our knowledge of your systems and infrastructure to highlight where your time and attention is needed more urgently

What is the same as the standard vulnerability management service?

- Detailed scans of your network to identify all devices including laptops, desktops, and servers (including devices used by remote workers)
- We conduct an agent-based scanning service, which has a negligible impact on your day-to-day business and operations
- The agents are deployed on each device in a non-intrusive manner, and devices provide an update to our management system every 15 minutes
- We will liaise with you throughout the process to understand any sensitivities or individual requirements related to your system architecture

Patch management

Automate your patching process

Patch management is time intensive for any organisation. Finding time to identify and prioritise vulnerabilities, allocate personnel with the right skillset, and then resolving is a monumental task. This service can regularly update your organisation's software to safeguard against the latest vulnerabilities.

- Tailor the service to focus on the software and systems you want to automatically patch, leaving the more bespoke fixes to your in-house IT team[3]
- With an effective patch management schedule, it will help to reduce any downtime across your network

What is the same as the standard vulnerability management service?

- Detailed scans of your network to identify all devices including laptops, desktops, and servers (including devices used by remote workers)
- We conduct an agent-based scanning service, which has a negligible impact on your day-to-day business and operations.
- The agents are deployed on each device in a non-intrusive manner, and devices provide an update to our management system every 15 minutes
- We will liaise with you throughout the process to understand any sensitivities or individual requirements related to your system architecture

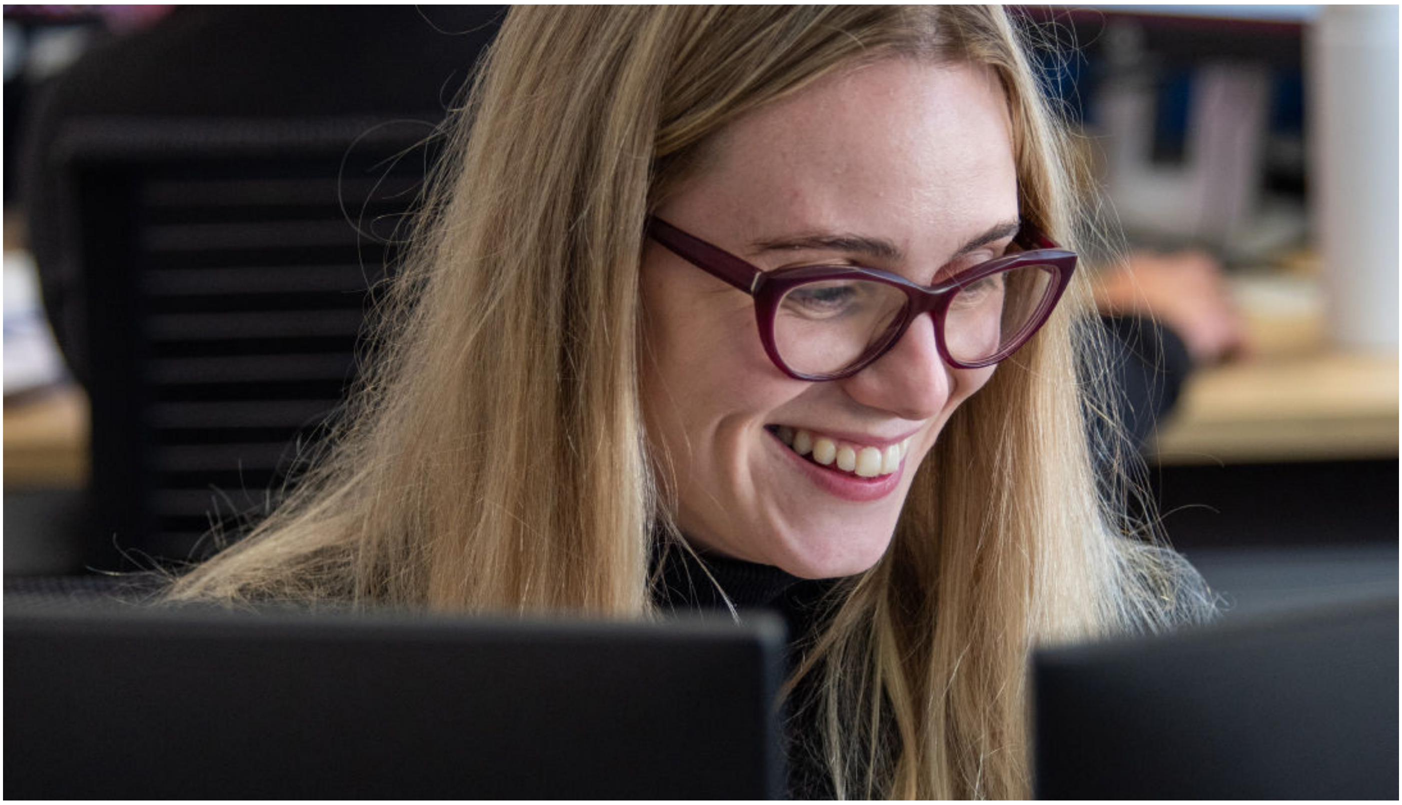
Cyber and information security control reviews

Bespoke organisational IT risk and control review

Assess information security across your entire organisation.

A well-designed and effective control environment is the best way to manage risk to any organisation.

- Leading professional services experience, specifically identifying, and assessing organisational and IT risks
- A bespoke framework, designed by Francis Clark, personnel to focus on the areas which matter most to organisations.
- Take the best in class from industry leading frameworks such as NIST 800-53, ISO27001 and more.
- Receive formal recommendations on how to design robust, effective controls and frameworks to proactively manage risk[4].
- Critically assess internal policies and procedures and advise on best practice.
- Areas include, but not limited to:
  - Finance and organisational processes (e.g. order to cash, purchase to pay, etc)
  - System access administration
  - Program change management
  - Finance and IT system implementations
  - Vendor due diligence and responsibilities
  - Incident and problem management
  - Physical security
  - Organisational continuity
  - Disaster recovery
- Our teams have experience with complex, international auditing standards such as SOx (Sarbanes-Oxley).



Information security - contractual compliance reviews

Are you struggling to understand your contractual information security requirements?

- Information security requirements can be complex, full of jargon and difficult to assess whether you have sufficient controls and processes in place.
- Vendors commonly audit other organisations to confirm sufficient controls are in place to safeguard their data and assets.

What can our in-house team do to support you?

- Cut through the complexity of the contract, understand the terms and conditions, and inform you of your obligations
- Support with the completion of returns through conversations with senior management to understand what controls and processes you have in place
- Conduct a gap analysis to assess any shortfalls against the contractual requirements
- Provide recommendations on best practice and how to help ensure your organisation meets the requirements

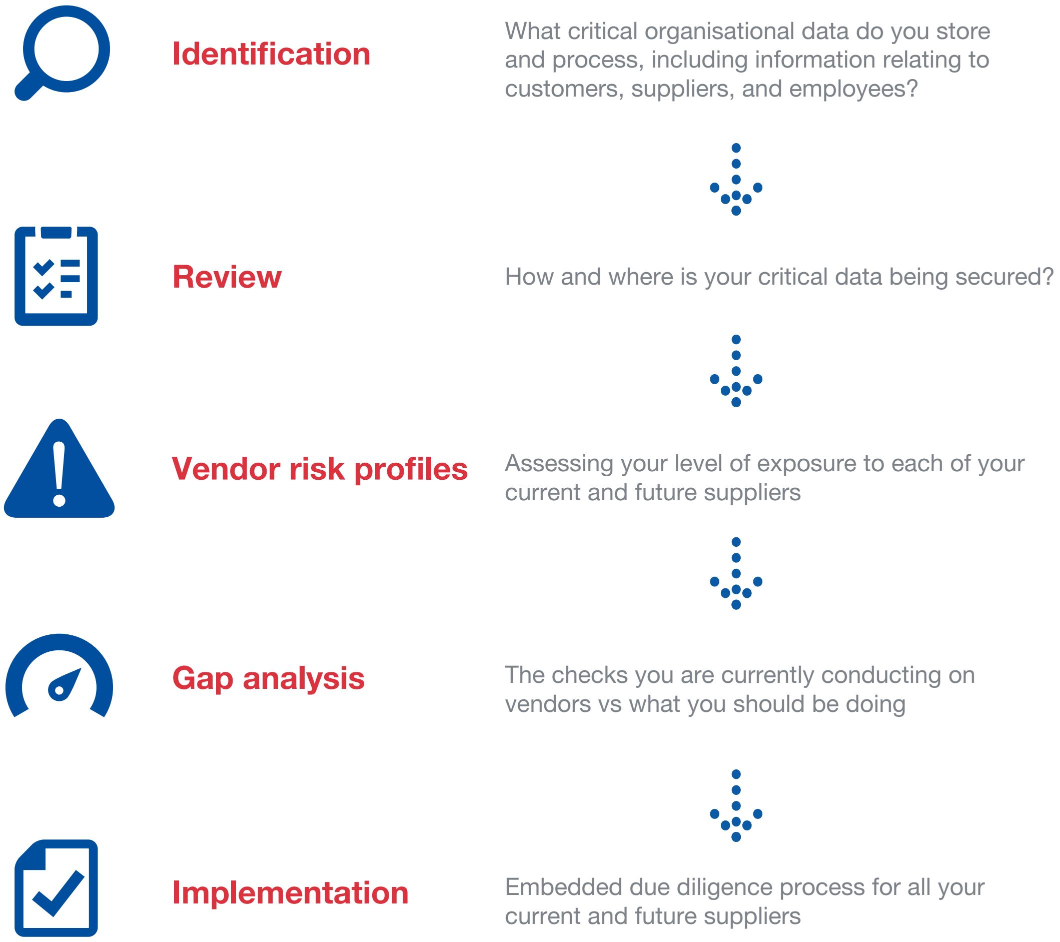
Supply chain security assessment

If I outsource a process to a third party, have I outsourced the risk?

- Unfortunately, not. According to cyber security firm CrowdStrike, 45% of organisations experienced at least one software supply chain attack in the last 12 months
- The Verizon Data Breach Investigation Report (DBIR) showed that supply chains were responsible for 62% of system intrusion incidents in the past year. Our third-party vendor security framework can help you to gain assurance that your suppliers are appropriately securing your data

What can our in-house team do to support you?

- Our framework service follows a five-step process. It will assist you in creating a tailor-made due diligence process enabling you to adequately assess each of your third-party suppliers
- You will be provided recommendations tailored to your organisation, industry, and vendors to develop a security framework fit-for-purpose
- You will have a formal due diligence process which you will be able to user for all your current and future suppliers



Identification

What critical organisational data do you store and process, including information relating to customers, suppliers, and employees?

Review

How and where is your critical data being secured?

Vendor risk profiles

Assessing your level of exposure to each of your current and future suppliers

Gap analysis

The checks you are currently conducting on vendors vs what you should be doing

Implementation

Embedded due diligence process for all your current and future suppliers

ISO27001 readiness and internal auditing services

Work towards an industry recognized and leading standard in information security

- ISO27001 enables you to build a robust, information security framework tailored to the needs of your organisation
- It demonstrates an advanced level of assurance and increases organisational opportunities around the world as well as domestically
- It can help to drive down cyber insurance premiums, support compliance with regulatory frameworks such as GDPR, and show stakeholders a strong, positive cybersecurity posture
- Our qualified team of ISO27001 lead auditors can provide varying levels of support to help you prepare for certification or surveillance audits
- ISO27001 requires that you conduct internal audits at planned intervals to ensure adherence to the standard. Our qualified team can conduct these for you, providing an independent review of your information management framework and drive continuous improvement across your organisation

PCI-DSS readiness and gap analysis service

Does PCI-DSS apply to my organisation?

- It is relevant to all organisations that process, transmit or store cardholder data.
- PCI-DSS compliance is a complex process which requires specific policies and procedures in place to be compliant.
- There are various factors that determine the scope of your PCI-DSS compliance process. It’s important to get this right and we can support you with this key decision.

What can our in-house team do to support you?

- PCI-DSS compliance can be a complicated process. We can work with your organisation and perform a gap analysis against the requirements of the standard.
- Our bespoke PCI-DSS readiness service will review your current internal security controls and policies against the 12 requirements of the PCI-DSSv4 standard
- This service will provide you with a set of recommendations on how best to achieve compliance
- Our qualified cyber security advisors will be on-hand to provide technical advice and support to your organisation and teams throughout the process

Cyber awareness training

Cyber awareness training

Human error is still one of the most common reasons for a successful cyber-attack

Cyber awareness training is one of the most important defences against social engineering attacks.

- Your people can be the weakest link when preventing a cyber-attack against your organisation
- Cyber criminals are constantly targeting your people, with c.85% of all successful attacks due to human error[5]

How can the training help your organisation?

- Demonstrate you are meeting your obligations under the UK Data Protection Act 2018 (UK DPA) that require organisations to raise staff awareness over information security
- Bespoke and interactive training with a wide variety of modules to choose from means that it can be tailored to your individual organisational needs
- Modules include, but are not limited to:
  - Social engineering attacks
  - Understanding individual responsibilities
  - Creating a positive security culture
  - Demystifying cybersecurity
  - Working from home securely
  - Mobile device security
  - Cloud security

PKF FRANCIS CLARK
Shared Ambition

Phil Osgathorpe
Director of IT, audit, assurance and cybersecurity
E: phil.osgathorpe@pkf-francisclark.co.uk
T: 01752 264867

Rhys Chalmers
IT cybersecurity technician
E: rhys.chalmers@pkf-francisclark.co.uk
T: 01803 221822

Stuart Slater
IT cybersecurity technician
E: stuart.slater@pkf-francisclark.co.uk
T: 01392 351844

The fine print

1. Free cyber insurance is up to a maximum liability cap of £25,000 and applies to organisations with an annual turnover of <20M
2. The assessed version is renewed every 3 years, however, there is still a requirement to complete the self-assessment annually
3. We will agree with you upfront how best to address your patch management needs and this will be governed by the terms in our engagement letter
4. We are bound, as an organisation, by the Revised Ethics and Independence Standard 2019. Therefore these services may be restricted or limited if you are also our audit client. If this is of interest to you or your organisation, please contact: phil.osgathorpe@pkf-francisclark.co.uk for more information
5. Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report | About Verizon

PKF Francis Clark is the trading name of Francis Clark LLP - a limited liability partnership, registered in England and Wales with registered number OC349116. The term 'partner' is used to refer to a member of Francis Clark LLP or to an employee or consultant with equivalent standing and qualification. If you wish to be added or deleted from our mailing list, please contact crm@pkf-francisclark.co.uk. You can see our privacy policy for how we handle your data at www.pkf-francisclark.co.uk/policies.