



PKF
Francis Clark

Are you exposed to cyber risk?

And what would it cost your business?

Helping organisations understand,
manage and reduce cyber risk.

Reducing financial and operational
impact while increasing return on
investment.







Are you exposed?

Many organisations believe they are protected against cyber risk.

The reality is often different.

The real question is not whether an incident will happen, but whether your business could continue if it did.

If your systems were unavailable, could your business operate?

- How long could you run without your core systems - hours, days or weeks?
- What would a month of lost revenue look like?
- Which business activities would fail first and what would that cost?
- How many days could you operate before the impact became material?
- Could your team continue to work effectively without access to systems?
- How quickly could you restore operations and in what order?
- Do you know how recovery would actually work in practice?

Beyond immediate disruption



Cyber incidents rarely affect just one area of a business.

The impact can spread quickly across operations, finances, customers and suppliers.

Questions to consider

- Could you lose key contracts due to operational disruption?
- Do customers or suppliers rely on your systems to do business?
- How widespread would the impact be if those systems became unavailable?
- Would your cyber insurance pay out in full if controls were missing or untested?
- Are you managing real risk, or relying on assumed protection?

For many organisations, these questions are difficult to answer.

We help businesses not only answer these questions but also feel confident in the answers.

What this looks like in practice

We see first-hand how cyber incidents impact organisations.

The cost of an incident is rarely limited to recovery spend. Revenue can be impacted. Operations can be disrupted. Management teams can find themselves focused on incident response rather than running the business.

When organisations are forced to react under pressure, the consequences can be immediate, costly and difficult to reverse.

Operational disruption

A manufacturing business experienced a ransomware incident that halted production for several weeks.

- Revenue was lost as orders could not be fulfilled
- Critical operational data became inaccessible
- Employees were unable to work effectively without key systems
- Customers experienced delays and reduced service levels
- Full recovery took more than a year

“The most stressful period of my entire working life.”

Finance Director

More real-world examples

Third-party blind spots

An organisation experienced a cyber incident originating from its managed service provider (MSP).

- Day-to-day IT services had been successfully outsourced for many years
- The provider had extensive access to critical systems and data
- Internal controls were well established and regularly reviewed
- Security arrangements within the provider's environment had not been independently assessed

The organisation assumed the risk was being managed.

In reality, it had limited visibility of exposure outside its own environment.

The value of cyber due diligence

A business with a successful ecommerce platform was preparing for sale when it suffered a significant data breach.

- Customer, supplier and business data was exfiltrated
- An ICO investigation followed
- Operations were disrupted while systems and controls were reviewed
- Buyer confidence reduced as cyber risks became clearer
- The agreed transaction value was revised during negotiations

The cost of responding to the breach was significant. The effect on the transaction was greater.

Are you carrying hidden risk?

In many SMEs, cyber risk is managed through trusted third-party providers, allowing internal teams to focus on day-to-day operations.

While this approach works well in many areas, it can sometimes limit visibility over how risks are being managed in practice.

As a result, organisations can find themselves exposed without a clear understanding of where the risk sits.

Maintaining that visibility is key to managing risk with confidence.

You may have unrecognised exposure if:

- Cyber risk is not regularly discussed at Board or senior leadership level
- Financial and operational impact has not been clearly assessed or modelled
- Controls exist but have not been independently reviewed
- Responsibility sits solely within IT
- You rely on outsourced IT providers without independent oversight
- You rely on cyber insurance without validating coverage conditions
- You do not have a clear incident response and recovery plan
- You would find it difficult to evidence controls to auditors, insurers or investors

Understanding your exposure early allows you to act in a controlled, proportionate way, rather than under pressure.

That is where we come in.

Our approach

We approach cyber risk in the same way you approach financial risk:

Structured.

Evidence-based.

Aligned to decision-making.

Cyber health assessment

Immediate risk visibility

A focused snapshot of your current exposure, identifying immediate risks and practical actions.

We help you answer

- Are there vulnerabilities that could be exploited right now?
- Are we exposed to ransomware or disruption risk?
- Are we at risk ahead of an audit or insurance review?
- What are the fastest improvements we can make?

What you get

- Identification of exploitable risks
- A prioritised remediation plan
- Practical actions that can be implemented within weeks
- Increased confidence ahead of key deadlines

Typically includes

- External exposure review
- Vulnerability assessment
- Access and privileged account review
- Dark web exposure checks
- Immediate risk prioritisation

Best suited to

Organisations needing immediate clarity and practical risk reduction.

Cyber maturity assessment

Strategic resilience

A broader, strategic review of your cyber risk exposure and long-term resilience.

We help you answer

- What is our financial and operational exposure from a cyber incident?
- Would an incident have a significant business impact?
- Are we meeting stakeholder expectations?
- Do we have appropriate governance and oversight?

What you get

- Board-ready view of cyber risk
- Identification of material control gaps
- Prioritised roadmap linked to risk reduction
- Evidence to support audit, insurance and due diligence

Typically includes

- Governance review
- Framework assessment and benchmarking
- Third-party risk review
- Financial impact assessment
- Strategic roadmap development

Best suited to

Organisations seeking a strategic understanding of cyber risk and long-term resilience.

In simple terms:

Cyber health assessment

- Immediate risk visibility
- Focused assessment
- Quick wins and rapid action
- Immediate priorities and practical next steps

Cyber maturity assessment

- Strategic resilience
- Broader organisational review
- Long-term risk reduction
- Strategic roadmap and governance improvements

Tailored to your organisation

We tailor our approach based on your size, complexity and risk profile, ensuring proportionate and relevant assurance.

Why work with us

Why organisations choose us

- Trusted by organisations undergoing audit, investment and due diligence
- Expertise across finance, audit and cyber not just technology
- Focus on practical, commercially proportionate improvements
- Clear outputs that support governance and decision-making
- Independent: providing evidence-based insight, not selling solutions
- Responsive results: insight within days, reporting within weeks

Cyber and IT risk advisory

Independent, experience-led guidance to support management decisions around technology, controls and risk.

We help you understand what matters most, what to prioritise and where to focus, without adding unnecessary complexity.

Part of the PKF network

As part of the PKF network, we can access broader expertise across cyber, risk and advisory services, both in the UK and internationally.

Other services we provide:

Cyber due diligence

Supporting transactions by identifying cyber risks that may impact valuation, integration or future investment.

Continuous vulnerability monitoring

Ongoing identification of technical weaknesses that could be exploited, helping you stay ahead of emerging risks.



Start with a conversation

Whether you're looking for immediate reassurance or a broader understanding of your organisation's cyber resilience, we can help you understand your exposure and identify the most appropriate next step.

Experienced cyber, audit and risk professionals



Meet Phil

Phil leads our IT assurance and cyber services teams and helps organisations understand cyber risk in business terms, not just technical ones.

A qualified accountant with more than 16 years' experience in audit, assurance and cyber risk, including 12 years with a Big Four firm, Phil has advised organisations across a wide range of sectors on cyber resilience, governance and risk management.

His experience spans external audit, due diligence, technology assurance and real-world cyber incidents, giving him a unique perspective on how cyber risk impacts operations, financial performance and strategic decision-making.

Phil Osgathorpe CISSP ACIIS FCCA

Head of cyber assurance and IT audit
01752 301010

phil.osgathorpe@pkf-francisclark.co.uk

What our clients say

"Phil translated complex cyber risks into clear business outcomes, helping us make informed decisions with confidence. A trusted advisor who combined technical expertise with a practical understanding of our organisation."

Paul Jones

Chief Information Officer,
Delt Shared Services Limited

"PKF Francis Clark delivered practical advice, high-quality insights and a genuinely collaborative approach. Their support gave us clarity, confidence and reassurance throughout the engagement."

John Bennett

Information Security Lead,
Logiq Consulting Limited

"PKF Francis Clark took the time to understand our business, worked around our needs and asked the right questions throughout. This wasn't a box-ticking exercise, it was a partnership."

Gio Wallace

Data Protection and Compliance Officer,
Airport Direct Travel Limited T/A Rezcomm

Our focus is practical: identify exposure, prioritise action and support better decisions.



PKF
Francis Clark

www.pkf-francisclark.co.uk

Francis Clark LLP is a member firm of the PKF International Limited network of legally independent firms and does not accept any responsibility or liability for the actions or inactions on the part of any other individual member firm or firms. FC-5016-240826-06