REPORTING

THE STATE OF THE INDUSTRY 2019

KEYSOURCE

CONTENTS

FOREWORD

The data centre sector is continuing to experience a significant period of growth which is being driven by advances in technology and the need to support increasing user demand, as well as an exponential explosion in data.

This transformation represents a significant step change in the way we use data centres, which are increasingly being recognised as essential assets that drive innovation for business survival and growth.

Advances in automation, 5G, IoT, robotics and artificial intelligence are some of the developments which influence global demand as well as the need for increasingly lower latency. And more than ever before, these technologies present a very real 'human life' dependant factor.

This has prompted us to take a moment to understand how the market perceives some of these current and future challenges. Our research focused on standards and accreditations, and this paper provides a full analysis of the results, exploring the potential impact on our industry and its global users.

Our data was gathered from polling over 110 senior IT decision makers from across the UK. Partnering with techUK, one of the UK's leading technology associations, and Censuswide, the data was independently verified and has uncovered some very interesting results.

As you will see, the results are compelling and suggest that there is a huge demand, now more than ever, for clarity and adoption of appropriate standards. It seems that we are at risk of not knowing if our highly critical applications of today are underpinned by suitable infrastructure. Nor do we have the ability to validate suitability for what may come in the future.

This in turn raises the question – should we be doing more to protect an 'unregulated industry' which plays such a vital role in both business and society?

Jon Healy, Managing Executive, Keysource

THE MUDDY WATERS OF DATA CENTRE STANDARDS

In this section:

- **80% of respondents say they require DC accreditations or standards.**
- **88% say they will become more important in the next 2 years.**
- **77% believe the landscape is confusing.**

So, the message from the research about standards and accreditation was loud and clear, with three quarters of respondents stating that the current situation is confusing. I doubt this is a surprise for many of us and is even perhaps something of an understatement.

Perhaps more than in any other industry, in the data centre world, accreditations and standards should play a vital role in bridging an industry language barrier between the data centre professionals and the end users. However, anyone looking for suitable standards and accreditations faces a dizzying array of options from commercial business, trade associations and European and international organisations.

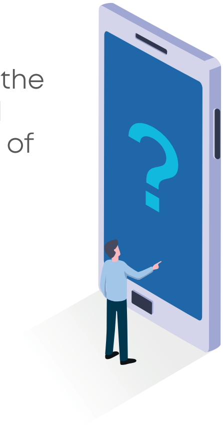
Because of this plethora of different options, each with its own criteria and governing body, we are seeing an increase in the number of owners and operators choosing to take advantage of this confusion and self-certify. Reverting to self-qualification or certification against their own standards schedule, represents a number of risks, and from an end user perspective only muddies the water further.

With the research also showing that nearly 90% of the people surveyed saw accreditations and standards becoming more important over the next two years, what do we as an industry need to do to provide this clarity? There is most certainly no 'one size fits all'.

In simple terms is what is missing a single standard or accreditation which gives the user or owner/

operator confidence in key areas such as design, security and operational management and that is recognised and trusted by all internal and external audiences?

If so the question is – how feasible or desirable is a single standard given the fast-paced and complex nature of our industry?



TECHUK TAKE

Whilst we agree that the standards landscape is complex, we would argue that it is not incoherent. Where the confusion tends to arise is between international, peer reviewed public standards like those developed by CENELEC, BSI, ISO, ITU etc and commercial or proprietary ratings like Uptime Tiers, which are often described as standards.

There is also confusion between standards and best practice tools like the EU Code of Conduct, and between standards and performance metrics. This is in part because a number of performance metrics are underpinned by standards and could therefore be described as “standardised”. In addition, things also get really complicated when you talk about certification and accreditation as anyone can be certified against set criteria but accreditation is a much more formal process.

We welcome the adoption of standards across the industry, irrespective of the capability being assessed. Accreditation will improve confidence because it demonstrates competence – and moreover provides peace of mind that it has been checked by a qualified third party.

Emma Fryer, Associate Director - Data Centres, techUK

IS REGULATION THE ANSWER?

In this section:

- **78% say we need a regulated standard for data centre design and operation.**
- **72% believe not having a standard will damage the growth of edge and IoT.**

The issue of regulation has always been controversial but what is clear from our research findings is that the industry wants a regulated standard. More than that, they believe that failure to achieve this will have a detrimental effect on the growth of the industry and areas such as IoT and Edge.

One reason that our respondents may have this view could be due to the fact that the criticality of the applications using the data centres has significantly evolved from traditional storage, and now includes high risk activities such as control of semi-autonomous vehicles or undertaking surgical procedures.

In addition, an industry skills shortage is creating a bigger disconnect between those who develop and manage the applications and those with data centre and engineering capability.

The danger here is that we could see a 'perfect storm' situation where a fast-paced technology industry continues growing to support user demand, without clarity around standards, and a skills shortage, which is unable to protect suppliers or users from the risk. Service disruption through outages caused by design, operation or security failures are likely to rise having economical, business and personal impacts.

Furthermore, with change in the industry a certain and the increasing inter-dependability of discrete services, our ability to confidently determine suitability throughout a particular service, or ecosystem of services, is potentially compromised.

The other consideration is providing a consistent mechanism for service providers to demonstrate confidence to the user, especially when considering the top four tech giants (Microsoft, Facebook, Amazon and Google) who can dominate a service with limited competition.

Other industries have recognised this and have a single third party that can assess and give a standard certification. Consumers are then able to make an informed decision, whilst also driving suppliers to meet higher standards. Euro NCAP would be an example in the automotive industry.

TECHUK TAKE

For a so called “unregulated” sector, data centres are subject to an astonishing array of compliance requirements. Many of these are inappropriately targeted and, as a result, unduly burdensome, making the balance between standards and regulation an interesting area.

There is no doubt that it is beneficial to have harmonised standards, and, in fact, significant progress has already been made on this front with a dedicated group whose sole purpose is to track and review environmental standards for data centres and ensure that they are harmonised.

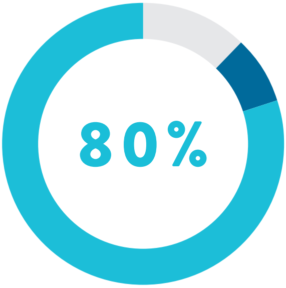
But regulating standards is another matter. We certainly want to see increasing reference to standards in regulations. However, turning a standard into a regulation gives you the worst of both worlds as you lose the ability to keep pace with rapid technological developments and also move into a one-size-fits-all scenario - something that we all know does not work for data centres.

So, harmonising multiple standards so they can be cross-referenced is good but consolidating them all into a regulation would, in our view, be a disaster.

Emma Fryer, Associate Director - Data Centres, techUK

RESEARCH BREAKDOWN

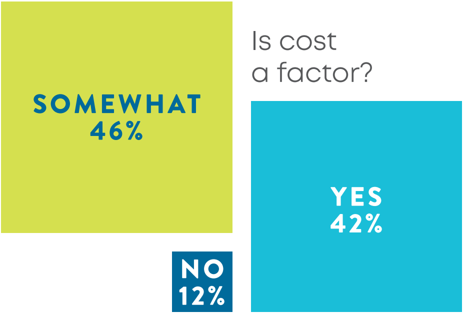
Surveying over 110 industry leaders from across the IT and data centre space, we've pulled out our key highlights below. The full breakdown can be seen on pages 18 - 23.



of respondents say they require data centre accreditations.

88% say they're going to become even more important in the next two years.
Analysis on page four.

72% think that if we don't have a consistent set of standards it will cause problems for the growth of the industry around things like IoT and Edge.

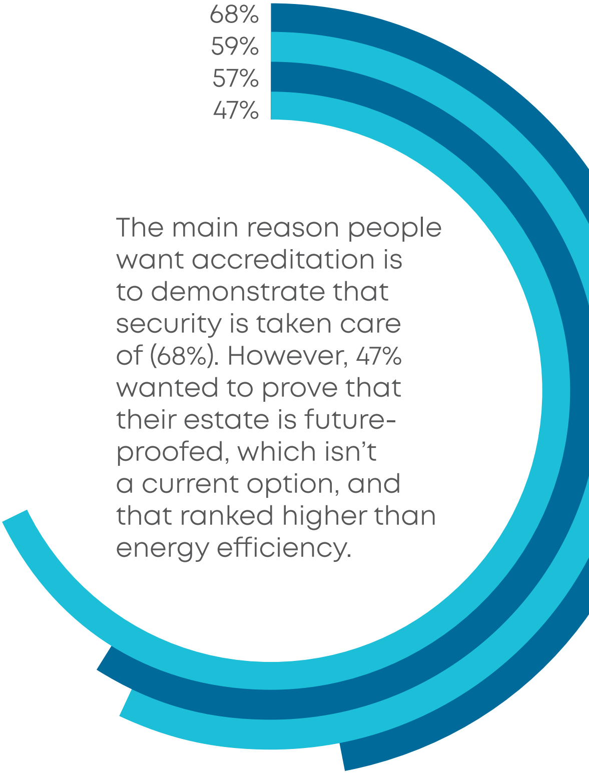


77%?

think the current data centre accreditation landscape is confusing and 78% say there needs to be a regulated standard for data centre design and operation.
Full report on page six.

1/3

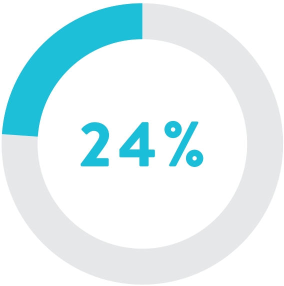
Nearly a third of respondents say they're often asked about what data centre accreditations they have (only 5% say they're never asked).



The main reason people want accreditation is to demonstrate that security is taken care of (68%). However, 47% wanted to prove that their estate is future-proofed, which isn't a current option, and that ranked higher than energy efficiency.

71% are concerned about the pressure they face against cyber-attacks and security breaches and 70% say that the average hacker could outwit the average IT director.

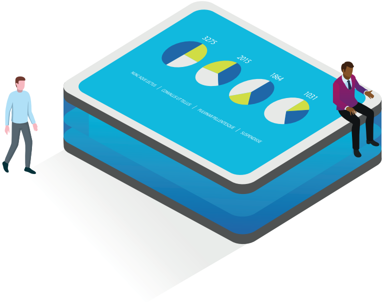
See page twelve.



of people say that they don't consider the limits of their data centre infrastructure before deciding to deploy new hardware.

80% of respondents feel that they take on high or medium risk by storing data in off-site premises / co-location facilities.

See why on page ten.



A RISKY BUSINESS

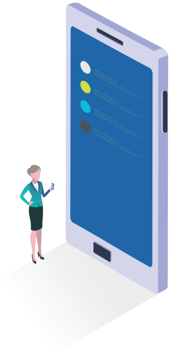
...

In this section:

- **80% feel they are taking on high or medium risk by storing data in offsite or colo facilities.**

That 80% of all respondents feel that they take on high or medium risk by storing data in offsite or colocation premises was perhaps the most surprising finding from the survey.

This manner of data storage is increasingly the norm and the benefits of having a specialist, highly skilled third-party team responsible for your infrastructure are well documented. Therefore, we have to consider the context around these concerns.



It could be that in this age of booming technology the type of data and associated sensitivity is increasingly a key consideration for any business, as it can represent intellectual property and is business critical. This means that the risk of commercial exposure is a major concern and more so when data is distributed across a geographically wider physical footprint. (Of course, this is at odds with the need for network access to be more readily available to meet agile working environments.)

The introduction of GDPR and the associated penalties has, in many cases, put these issues more firmly on the radar. In addition, in 2019 we have seen a number of high profile examples of disruption caused by data centre outages.

It was reported in January, CenturyLink cloud communications network experienced an outage across the US, which blocked 911 emergency services; in March Google experienced a global outage that affected its Gmail and Google Drive services; whilst later that month a 14-hour Facebook outage affected millions of users around the world. This has continued to highlight the potential commercial and reputational risks.

It may also be that the confusion identified in the research around standards and accreditations means that users simply don't know what they are buying when choosing a third party and, as a result, see this as a risk. Would a common standard or more regulation help allay these fears?

(See page six for more)

Finally, we should consider why offsite / colocation providers are failing to address these concerns, given the strong levels of resilience that they regularly deliver. Could this be a lack of communication? Does the blame lie here?

TECHUK TAKE

From a colocation perspective these results were really surprising. Our experience is that outsourcing to a purpose built, secure facility should reduce security risks.

We would also be curious to compare these scores with the perceived risk of staying where they are, and also to understand more about the type of in-house facility those who responded have in mind, whether it is on-premises in server rooms, or a purpose-built facility within the corporate HQ.

Emma Fryer, Associate Director - Data Centres, techUK

A CHALLENGING YEAR FOR IT DIRECTORS

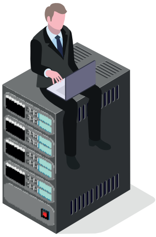
...

In this section:

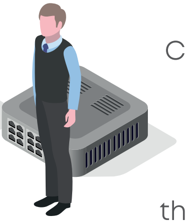
- **70% believe the average hacker could outwit the average IT Director.**
- **71% are concerned about the pressure they face in meeting cyber security challenges**
- **80% feel support at board level.**

It has been a challenging 12 months for IT Directors who have continued to see their remits evolving from the traditional responsibility for hardware and software to focusing on business critical activities such as data security and IP protection. In many cases they are expected to guide the business rather than just support it.

The results of the survey highlighted these changes painting a picture of operating within a fast-changing environment which is at times inconsistent, confusing and failing to reassure.



Over two thirds of those questioned stated that security is the number one challenge they face, with over 70% concerned about the pressure they are under to prove resilience against breaches and cyber-attacks. These concerns are exacerbated by a belief that the average hackers could outwit the average IT Director. This theme runs throughout the responses, driving a desire for accreditation, regulation and common standards.



Closely linked to this is the perceived risks of storing data offsite, despite strong evidence to the contrary, with 80% stating that they believe this to be a high or medium risk. As a result, almost three quarters of organisations are becoming less reliant on third parties.

Other challenges include the pressure to adopt new technology (45%) with almost half of respondents stating that they didn't have enough time to develop their skillsets to accommodate this. On a more positive note almost 80% felt that they have board level support to drive change.

In simple terms this research shows an increasing groundswell of opinion from IT Directors that the industry must make significant changes, and make them soon.

TECH UK TAKE

The stats on cyber security mirror results seen across other sectors, with the government's own Cyber Breaches Survey revealing that 2/3 of businesses view cyber security as a top priority topic.

There is a mismatch, however, between the number of businesses highlighting cyber security as a top challenge, and the number of businesses that have effective policies and processes in place to deal with the threat.

As this survey shows, significant changes need to be made in the industry – and fast. The cyber security landscape can at times be confusing and difficult to navigate, and with exploits at times being easy to deploy and deliver, IT Directors and data centres need continuing board support to deliver meaningful change.

Talal Rajab, Head of Cyber Security, techUK

TECHUK CONCLUSION

...

Emma Fryer, Associate Director - Data Centres

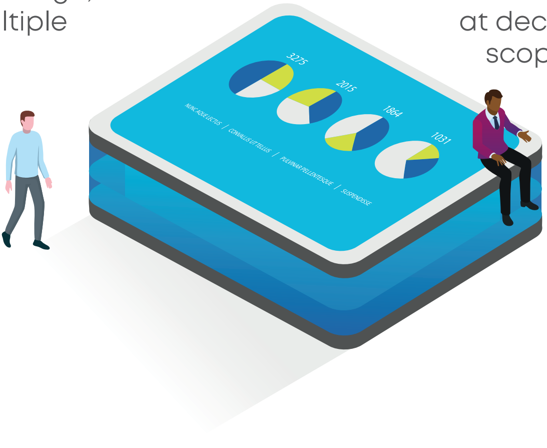
The data centre sector has an unusually rich standards landscape for such a young industry, and we should be proud of this because it demonstrates the sector's commitment to customer service, to professionalism and to self-policing.

However, data centre standards can appear bafflingly complex and this is attributable to several factors. Firstly there is the complexity of the data centre itself: multiple technical sectors converge, so multiple standards apply. Secondly there is widespread confusion between public standards, proprietary or commercial ratings, and performance metrics.

> **"Data centre standards can appear bafflingly complex."**

Trying to make sense of this is a real challenge. We recently mapped data centre standards against two criteria: scope and life cycle stage. Life cycle phases were limited to design and build, use and decommissioning. Scope ranged from the generic (e.g. ISO 50001) right down to specifics like cabling. The map that emerged showed heavy clustering around design, build and use phases, with a notable scarcity of standards applicable at decommissioning. In terms of scope, standards were focused on M&E rather than IT, and we found none relating to software.

On reflection this makes sense: operators compete on resilience and must demonstrate that they can provide continuity

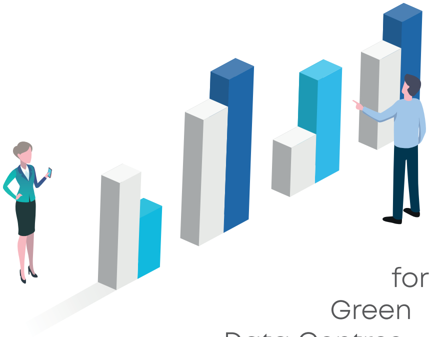

3275
2015
1864
1031
NUNC AQUE LECTUS / CONVALLIS UT TELLUS / PULVINAR PELLENTESQUE / SUSPENDISSE

of service. International, peer-reviewed standards are a good solution, especially where performance can be verified by accredited third parties.

In an ideal world, a single standard for data centres would address all aspects of the business. In reality that is very unlikely because the sector is really a cluster of different industries, because data centres do different things and because customer needs and expectations vary.

The closest we have is probably the EN 50600 series of availability standards developed specifically for data centres, where each part covers a different operational aspect: EN 50600-2-5 covers security, for instance. This confers more flexibility than a monolithic single standard and avoids the shortcomings of a one-size-fits-all approach.

While many believe that data centre standards would benefit from rationalisation, our current priority is harmonisation and groups like the CGGDC (Coordination Group



for Green Data Centres established by all European Standards Organisations) work to eradicate conflicting requirements. We also need improved clarity, explanation and interpretation so that those procuring data centre services can identify those standards that most closely match the performance they need from their supplier.

"Data centre standards are a work in progress; we are going in the right direction, but we are nowhere near the end."

Meanwhile, we continue to support the adoption of standards within the industry and promote reference to existing data centre standards in policy instruments.

Data centre standards are a work in progress; we are going in the right direction, but are nowhere near the end.

KEYSOURCE CONCLUSION

Jon Healy, Managing Executive

This research has unlocked some interesting results and when we look at these in depth there are some important issues that both the industry and end users need to address.

> **"80% of data centre managers said their most recent outage was preventable."**

The main areas to consider, perhaps unsurprisingly, all lead to security and resilience and how best to achieve this. However, it is important to put these findings into a broader industry context.

According to survey results released by the Uptime Institute last year, nearly one-third of all data centres had an outage in the past year, up from 25 percent the year before. The top three causes of downtime were power outages (at 33 percent), network failures (at 30 percent), and IT or software errors (at 28 percent).

Most importantly, 80 percent of data centre managers said their most recent outage was preventable. Is it hardly surprising then that IT Directors are increasingly concerned, particularly as the commercial impact of IT downtime is on average $5,600 per minute but can be as high as $540,000 per hour, according to Gartner.

Perhaps the real concern however is the brand and reputational impact. In May WhatsApp had to urge all of its 1.5 billion users to update their apps as an added precaution after an advanced cyber threat actor used surveillance software on the end to end encryption,

allowing the attacker to read the messages on the target's device. More recently, Salesforce's 15 hour and eight minutes outage enabled Salesforce users in a company to see all of their company's data, with or without permission.

The fact that some of the biggest technology companies in the world are experiencing this does not instil confidence. One thing for certain is that outages, failures or issues will continue and are likely to have bigger impacts to businesses and society – and even on human life where technology is more widely used to automate services.

There is no doubt that the pace of change and growth within the industry is creating real challenges when it comes to the ability to govern and suitably manage the risks. Looking ahead, both the industry and end users need to be doing more in order to drive the right industry behaviour and recognise that the lack of consistency in the market is having a huge impact.

"The pace of change and growth within the industry is creating real challenges."

As a starting point real consideration needs to be given to the benefits of a common and accessible standard to address design, security and operational management. This needs to be relevant, able to keep pace with the fast moving sector and be accredited both regionally and globally.

In conclusion this research positively shows that the industry recognises its shortcomings and the need to change.

Whilst data centre standards may be one of the less exciting topics of our industry, it is one that will ultimately set the right foundations in which to build the future.

There is work to do and it needs to be done quickly.

APPENDIX

Q1

Do you require any specific data centre standards / accreditations?

Yes	80%	No	20%

Q2

Which data centre standards or accreditations are you aware of? (Tick all that apply)

EU Code of Conduct	48%	ISO9001	48%
ISO27001	46%	Data Centre Alliance	44%
ISO14001	42%	ISO50001	38%
BREEAM	31%	EN50600	27%
Uptime Institute	21%	Unaware of any	3%

Q3

Do you think data centre accreditation will be become a more important consideration in the next 2 years?

Yes	88%	No	6%	Don’t know	6%

Q4

Thinking about security, how much risk do you think you are taking on by having data stored in off-site premises or in co-location facilities?

High risk	20%	Medium risk	60%	Low Risk	20%

Q5

If you were seeking accreditation, which of the following would you want to demonstrate to external and internal audiences? (Tick all that apply)

That security is taken care of	68%
Resilience and up-time	59%
Maintenance and management	57%
To demonstrate a futureproofed estate	47%
Energy efficiency	43%
None of the above	1%

Q6

How often are you asked by internal or external stakeholders what data centre accreditations your business has?

Very Often	31%	Sometimes	42%
Rarely	22%	Never	5%

APPENDIX

...

Q7

What accreditations or standards do you view as value for money? (Tick all that apply)

ISO9001	44%	EU Code of Conduct	41%
ISO50001	30%	ISO27001	26%
EN50600	25%	Data Centre Alliance	24%
ISO14001	24%	Uptime Institute	21%
BREEAM	18%	There's no accreditations or standards I view as value for money	8%

Q7a

Does the cost to obtain and maintain an accreditation influence your decision to gain an accreditation?

Influences my decision strongly	46%
Influences my decision somewhat	42%
Does not influence my decision	12%

Q8

Do you think that the current landscape of data centre accreditations is confusing?

Yes	77%	No	18%	Don’t know	5%

Q9

To ensure clarity of what customers are buying / vendors are selling, do you believe there should be regulated standards for data centre design and operations?

Yes	78%	No	3%	Don’t know	19%

Q10

Edge data centres have been described as the next growth area for the data centre industry, underpinning technology like autonomous vehicles and IOT. In your opinion, are we going to face problems in the future if we don’t have a consistent set of standards for edge data centres?

Yes	72%	No	21%	Don’t know	7%

APPENDIX

Q11

Do you consider the limitations of your data centre infrastructure before deciding to deploy new hardware?

Yes	69%	No	24%
Don’t know	3%	N/A	4%

Q12

Are you concerned about the pressure put on IT to prove its resilience against security breaches and cyber-attacks?

Yes	71%	No	26%	Don’t know	3%

Q13

Do you think the average hacker could outwit the average IT director?

Yes	70%	No	22%	Don’t know	8%

Q14

Do you and your team have enough time to learn about new technologies and develop your skillset?

Yes	58%	No	42%

Q15

What do you think will be the main challenges facing IT Directors in the next year? (Tick up to three)

Security	66%
Pressure to adopt new tech	45%
Access to skills and talent	42%
Prove the value of applications	32%
More reliance on third parties	30%
Getting internal buy-in for change from the rest of the board	23%
I don't think there will be a main challenge facing IT Directors in the next year	4%

KEY CONTACTS

Jon Healy

Managing Executive - Keysource

With a background in engineering and extensive experience in the data centre and critical environment industry, Jon has led a range of award winning solutions and services for a host of companies from global enterprise to major government organisations.

E: jon.healy@keysource.co.uk

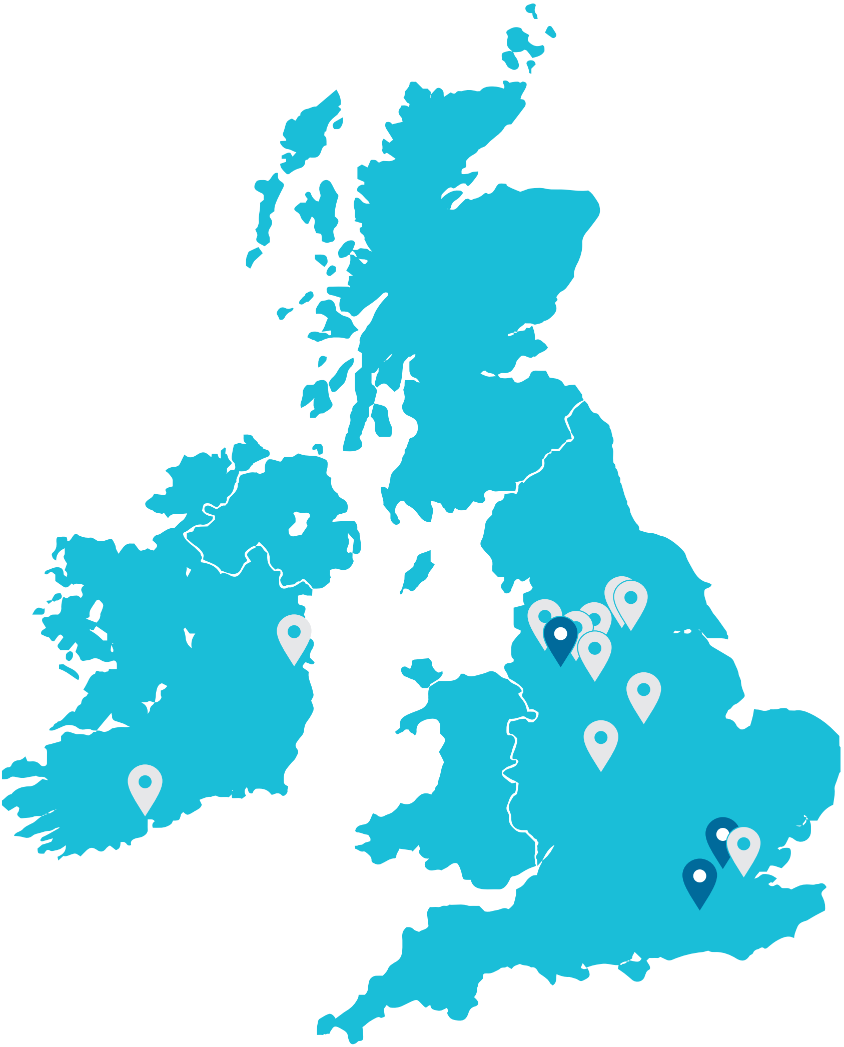
Emma Fryer

Associate Director - techUK

Emma manages the UK Council of Data Centre Operators and techUK's Data Centres Technical Committee and has achieved some major outcomes for the sector, including negotiating and implementing the Climate Change Agreement for Data Centres.

E: emma.fryer@techuk.org

■ Keysource office locations
□ Other Extentia Group office locations



Gatwick - HQ

3 City Place
Beehive Ring Road
Gatwick
RH6 0PA

London

Floor 499
Charterhouse Street
London
EC1M 6HR

Manchester

Cavendish House
Cross Street
Sale
M33 7BU

ABOUT KEYSOURCE

...

Keysource is one of the world's leading specialists in critical environments, helping to ensure business continuity for clients across the globe.

In today's fiercely competitive world, keeping your business up and running is non-negotiable, that's why it's vital to ensure you have the right approach to your critical and technology infrastructure.

Our consultative led approach sees us working closely with major international brands, local and national governments, as well as leading universities and start-ups on cutting edge technologies and innovative critical engineering and infrastructure solutions.

After a deep audit of your technical estate, technology and protocols to gain a thorough insight into your operation, we deliver ultra-robust and future proof solutions to safeguard your business operations and infrastructure, underpinned by cutting edge technology and software.

Then, after project managing the seamless integration and delivery of your new solution to avoid disruption, our operational approach delivers ongoing management, on-site support and maintenance planning of your new asset

.It's this unique approach that enables us to achieve repeat business with clients we've worked with for decades, who trust us to protect their reputations and keep their operations running.

KEYSOURCE

keysource.co.uk