cmc Cyber Monitoring Centre | parametrix

The Cost of Downtime:

UK Exposure to Cloud Infrastructure Failure

Cyber Monitoring Centre

July 2026

Contents

Foreword

This paper has been developed at an important stage in the UK's adoption of cloud computing. Nearly 80% of the 9,000 companies in the UK with more than £50 million of revenue are reliant on cloud infrastructure and many of these use the cloud for business critical operations. In 2025 there were outages at data centres belonging to Google Cloud, Amazon Web Services and Microsoft Azure. While these cloud failure events were contained, they show that the risk of failure exists, and that there is the potential for longer outages resulting in greater economic impact. The events also led to downtime across cloud hosted platforms and showed that recovery can be delayed due to service dependencies and system backlogs.

The Cyber Monitoring Centre (CMC) was set up to analyse the impact of major UK cyber events. To inform future analysis we wanted to gain a more complete understanding of UK cloud usage and the potential financial impact of cloud outage events, and so partnered with Parametrix, a specialist in cloud analytics and monitoring, to carry out this analysis.

This collaboration reflects a shared commitment to improving the understanding of cloud usage and the potential impact of cloud failure. The insights provide a valuable resource for the CMC to use when assessing future cloud failure events and by releasing this paper we also hope that it can be useful for policymakers, businesses, and the insurance sector as they navigate cloud risk and strengthen digital resilience. Anyone using the analysis should note the limitations that are captured in the methodology section, in particular that the losses only cover directly impacted companies and not any downstream impact. This downstream impact could significantly increase losses during a cloud failure event.

Will Mayes
CEO, Cyber Monitoring Centre

Executive Summary

This paper quantifies the UK economy's exposure to cloud infrastructure outages and identifies critical aggregation points where failures could trigger widespread economic disruption. Using a representative portfolio of 2,100 UK companies spanning micro businesses to FTSE 100 firms, the analysis maps cloud dependencies across providers and regions, then models direct financial losses under various outage scenarios.

Key Findings

Cloud dependency is more concentrated among economically significant firms. While only 11% of UK companies by count are cloud-dependent, this figure rises to 64% when weighted by revenue. Among FTSE 100 companies, 84% rely on cloud services for critical operations, and for Large companies the figure is 66%. This concentration means that cloud outages disproportionately affect the most economically important parts of the UK economy.

Provider concentration varies by market segment. AWS maintains a strong presence across all segments (34% overall dependency), while Azure dominates among larger firms (70% of FTSE 100, 46% of Large companies). Regional providers like Ionos, OVH, and DigitalOcean serve 11%, 5%, and 3% of the market respectively, concentrated among smaller businesses.

Larger firms have a more global cloud footprint. The UK/Ireland region hosts 55% of UK cloud dependencies, with European regions (excluding UK/Ireland) hosting 25% and North American regions 18%. Larger firms distribute their footprint more globally, while smaller companies concentrate more heavily in UK/Ireland regions. Notably, significant UK economic activity still depends on US-based infrastructure, particularly AWS us-east-1, creating cross-border dependency risk.

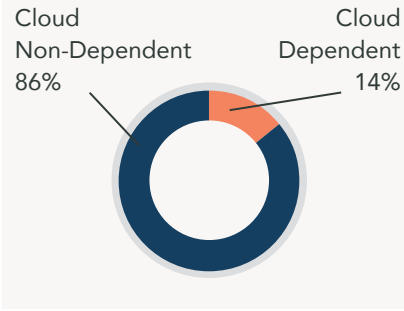
Cloud dependency varies by industry. Among Large and FTSE 100 companies, cloud dependency is highest in Health (91%) and Software & IT Services (90%), followed by Finance and Transportation (both 76%). Manufacturing, Retail/Wholesale, and Other sectors show lower cloud dependency (57% to 66%), but still represent significant absolute exposure given their economic weight.

Redundancy remains the exception, not the rule. 34% of the revenue exposure of cloud-dependent companies employ multi-region redundancy. This figure rises to 71% among FTSE 100 companies but falls to just 4% for Micro and Small businesses. Even among Large and FTSE 100 firms, redundancy adoption varies significantly by industry: Software & IT Services lead with 41%, while Finance and Manufacturing companies lag with 16%.

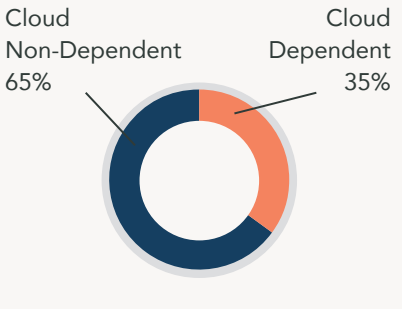
Total economic losses are understated. Direct impact analyses omit downstream effects on dependent firms and supply chains, meaning actual losses from major outages will be substantially higher as disruptions propagate through the economy. This cascading impact was clearly seen in the CMC's analysis of the Jaguar Land Rover (JLR) cyber incident in September 2025.

Snapshot of Cloud Service Dependence: Weighted by Annual Company Revenue

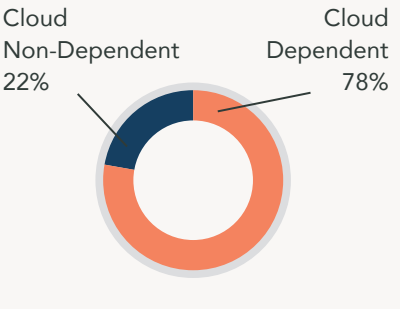
Micro and Small
≤ £10m revenue



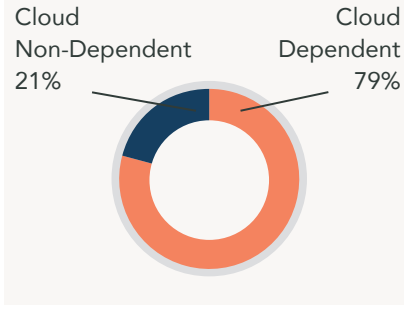
Medium
£10m – £50m revenue



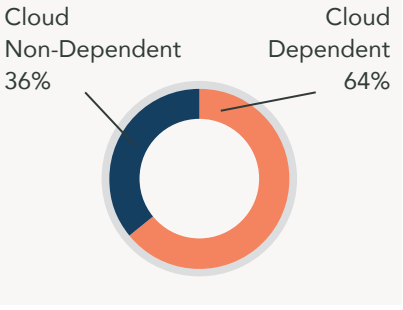
Large (exlcuding FTSE 100)
> £50m revenue



FTSE 100



Total UK Market



A small number of cloud regions support disproportionate economic activity. The analysis reveals critical aggregation points where relatively few cloud regions account for substantial UK revenue:

- AWS us-east-1 (N. Virginia): 20,000 companies exposed, representing £857 billion in revenue (12% of UK economy)
- AWS eu-west-1 (Dublin): 30,000 companies exposed, representing £801 billion in revenue (11% of UK economy)
- Azure northeurope/westeurope (Dublin/Amsterdam): 30,000 companies exposed, representing £1.2 trillion (17% of UK economy)

These three aggregation points account for 40% of UK economic revenue exposure, despite supporting just 3.5% of UK companies.

Outage scenarios can lead to losses exceeding £1 billion not including any downstream impacts. A 12-hour outage at AWS eu-west-1 would generate estimated direct losses of £402 million, rising to £1.7 billion for a 48-hour event. For the AWS us-east-1 aggregation point, a 24-hour outage would produce £647 million in direct losses. A 24-hour event in Azure uksouth, would produce £352 million in direct loss. These estimates exclude downstream impacts on dependent firms and supply chains, meaning actual economic losses could be substantially higher.

For the AWS us-east-1 aggregation point, a 24hr outage would produce **£647M direct losses**

Implications

Companies must quantify their cloud exposure and potential financial impact. Many firms lack visibility into their cloud dependencies and potential financial exposure. With 71% of revenue exposure of FTSE 100 companies employing redundancy but only 4% of smaller (Micro and Small) businesses doing so, vulnerability is unevenly distributed across the economy.

Critical infrastructure dependency raises sovereignty and regulatory questions. Health, Finance, and Transportation sectors show cloud dependency rates of 76% to 91%, with significant exposure in regions outside UK jurisdiction. This creates challenges for regulatory reach and the UK's ability to ensure resilience in critical sectors.

Effective risk management requires coordinated action across stakeholders. Cloud resilience is not solely a technical challenge for individual companies to solve. The systemic nature of cloud dependencies means that outages at key aggregation points cascade across industries and affect the broader economy. Managing this risk effectively requires companies to build robust architectures, insurers to price and cover these risks appropriately, and policymakers to ensure regulatory frameworks keep pace with cloud-dependent critical infrastructure.

The analysis presented in this paper reflects a snapshot in time. Cloud adoption continues to expand rapidly, and the technological landscape is evolving, introducing new exposures, shifting dependencies, and emerging risks. As digital infrastructure architectures change, the strategies used to manage and mitigate these risks must also evolve. This reality underscores the importance of updating such analysis to ensure that risk assessments, mitigation strategies, and insurance solutions remain aligned with the current and future state of cloud dependency.

Methodology

Modelling Process

The modelling process involved the following steps:

1 Building a representative portfolio of companies
Companies were selected from the UK Companies House business register using a stratified sampling methodology to create a representative portfolio of UK companies. The portfolio includes all FTSE 100 companies and a sample of Large, Medium, Small, and Micro companies across the full range of industries.

Companies' segments were determined based on annual revenue:

- **Micro:** companies with annual revenue of £1 million or less
- **Small:** companies with annual revenue between £1 million and £10 million
- **Medium:** companies with annual revenue between £10 million and £50 million
- **Large:** companies with annual revenue exceeding £50 million, excluding FTSE 100 constituents; and
- **FTSE 100:** companies included in the FTSE 100 index, with analysis focused on UK operations only

Demographic data from the UK Office for National Statistics on UK business turnover by industry and size band was used to determine scaling factors that were used to aggregate up the sample results to the overall UK economy.

2 Identifying cloud dependencies
Each company in the sample was scanned using Parametrix's proprietary cloud scanning platform to identify its technological footprint and to model cloud service dependencies. This identified:

a The cloud service providers (CSPs) and cloud regions used
b Whether cloud services support mission-critical functions
c Whether regional redundancy is employed

The individual company insights were then aggregated by the five company size segments to understand the cloud exposure profile:

a Dependence on cloud services
b Dependence on specific cloud service providers
c Dependence on specific cloud regions
d Dependence by industry
e Redundancy measures deployed

3 Quantifying the economic impact of cloud outages
For each company in the sample, the financial loss of outages was modelled across relevant CSP cloud regions (aggregation points) for a range of outage durations using Parametrix's proprietary cloud scanning platform. The model uses a proprietary approach to carry out the following analysis for each company:

a Estimate the proportion of revenue and associated profit dependent on cloud services
b Estimate the profit at risk in the event of a cloud outage event
c Where a company depends on multiple aggregation points, assign a profit at risk estimate across the aggregation points
d Model the percentage of the profit at risk that is lost based on outages of various durations

The individual company estimates are then aggregated to estimate the total financial losses at each aggregation point for cloud outages of different durations.

[1] Parametrix's proprietary cloud scanning platform integrates five years of data from companies purchasing Parametrix Cloud Outage Insurance with technology scanning data

Model Limitations

The analysis provides valuable insights into UK cloud exposure and potential outage impacts, but readers should interpret the findings with awareness of the following limitations:

Geographic scope varies by company segment. For FTSE 100 companies, the analysis focuses exclusively on UK operations and UK-based revenue. This approach provides a clearer picture of UK-specific exposure. For all other company segments (Large, Medium, Small, and Micro), the analysis includes their full global operations, which may result in cloud dependencies that reflect worldwide rather than UK-only activity.

Loss estimates capture direct impacts only. The modelled financial losses reflect direct revenue and profit losses for companies whose cloud services are disrupted. The analysis does not quantify downstream or cascading effects, including:

- Impacts on companies that depend on the disrupted firms' outputs (e.g. retailers relying on a logistics provider whose systems go down)
- Supply chain disruptions that propagate through multiple tiers of dependent businesses
- Impacts on end consumers or users of SaaS platforms hosted on affected infrastructure
- Broader economic multiplier effects

As a result, the true economic impact of major cloud outages is likely substantially higher than the figures presented in this paper. The Cyber Monitoring Centre's ongoing work seeks to capture these downstream impacts when assessing actual cyber and cloud events.

Cloud dependencies are modelled, not directly observed. The identification of cloud service providers, regions, and dependencies relies on Parametrix's scanning technology and modelling rather than direct reporting from companies. While this approach enables comprehensive coverage across thousands of firms, it introduces potential model error and may not capture all nuances of individual companies' cloud architectures.

Redundancy assessment reflects a point in time. Companies continuously evolve their cloud architectures, and redundancy measures identified in this analysis represent a snapshot. Actual redundancy effectiveness during an outage depends on implementation quality, testing rigour, and operational response, factors not fully captured in the analysis.

Outage scenarios assume complete regional failure. The loss models assume total unavailability of affected cloud regions for the specified duration. Real-world outages often involve partial degradation, affecting some services while others remain operational, or impact specific availability zones within a region rather than the entire region. Actual losses may therefore vary significantly from modelled scenarios depending on the specific nature and scope of the disruption.

Sample-based estimates involve uncertainty. While the representative portfolio methodology uses stratified sampling and scaling factors derived from ONS data, the aggregated UK-wide figures are estimates subject to sampling error, particularly for smaller company segments where fewer firms were included in the sample.

These limitations do not diminish the value of the analysis for understanding relative risk concentrations and identifying key aggregation points. However, they demonstrate the importance of treating the quantitative findings as indicative rather than definitive, and of updating the analysis periodically as cloud adoption patterns and infrastructure architectures continue to evolve.

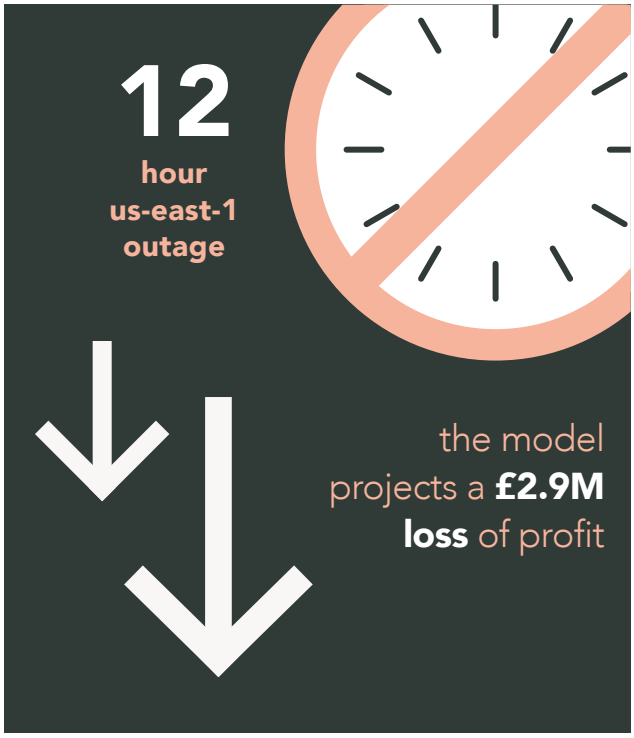
Case Study: Impact on a large, UK-based international restaurant chain

We examined the economic impact of a sustained outage in one of the world's largest cloud regions, AWS's us-east-1 (North Virginia, US), resulting in a complete disruption of cloud-dependent systems.

Annual revenue: £1.6B
Annual gross profit: £800M

An international restaurant chain relies heavily on AWS's public cloud infrastructure to support both their in-store ordering systems and online mobile application. Cloud services play a critical role in sustaining business continuity, with approximately 60% of the company's gross profit dependent on cloud availability. The company's operations are distributed between two cloud regions: us-east-1 (N. Virginia) and eu-west-1 (Ireland).

For an event where us-east-1 goes down, suffering 12 hours of outage, the model projects a £2.9M loss of profit.



Results

This section examines cloud dependency across the UK economy, from the overall level of reliance on cloud services through to the specific providers, regions and aggregation points where exposure is concentrated. It then quantifies the direct financial impact of outages at these key aggregation points.

1 The Representative Portfolio

The representative portfolio consists of 2,100 UK companies sampled across all size segments and industries. The distribution of the sample portfolio is shown in Exhibit 1.

84% of FTSE 100 companies and **66%** of Large companies rely on the cloud for critical operations

2 Dependence on Cloud Services

The UK dependency of cloud services varies by size of company. In general, larger companies are more dependent on the cloud. The Parametrix model estimates that 84% of FTSE 100 companies and 66% of large companies rely on the cloud for critical operations. In contrast, cloud dependency is less prevalent among Small and Micro companies with only 11% of these companies being cloud dependent.

When weighting cloud dependency by company count (Exhibit 2), Micro businesses drive the results. Their low level of cloud dependency reduces the total percentage of companies that are cloud dependent and could create the impression of low cloud reliance across the economy.

Weighting cloud dependency by revenue (Exhibit 3) provides a more accurate view of the overall economy's reliance on the cloud. This approach places greater emphasis on larger, economically significant companies that are more likely to depend on cloud services, offering a clearer picture of how much UK economic output relies on the cloud.

Exhibit 1 The representative portfolio by segment

Sampling group	Number of companies in sample	Average annual revenue (£M)	Average scaling factor	Scaled revenue in £B
Micro	583	0.3	2,902	482
Small	450	4	362	718
Medium	340	20	96	664
Large (excl. FTSE 100)	627	292	27	4,871
FTSE 100	100	5,347	1	535
Total	**2,100**			**7,270**

Exhibit 2 Cloud service dependence: Weighted by number of companies

	Micro and Small	Medium	Large excluding FTSE 100	FTSE 100	Total
					
Cloud dependent	**11%**	**34%**	**66%**	**84%**	**11%**
Cloud non-dependent	**89%**	**66%**	**34%**	**16%**	**89%**
Number of companies in UK	2,681,960	32,345	10,254	98*	**2,724,659**

*This is less than 100 because some companies are registered overseas

Exhibit 3 Cloud service dependence: Weighted by company annual revenue

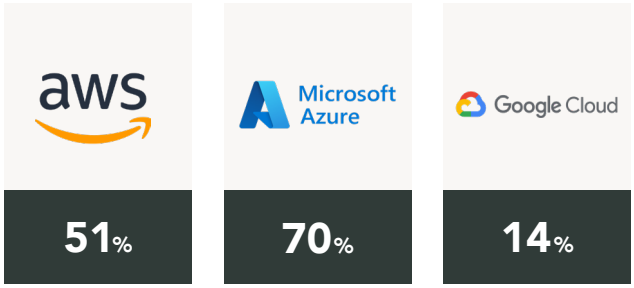
	Micro and Small	Medium	Large excluding FTSE 100	FTSE 100	Total
					
Cloud dependent	**14%**	**35%**	**78%**	**79%**	**64%**
Cloud non-dependent	**86%**	**65%**	**22%**	**21%**	**36%**
Total UK market revenue (£M)	1,200,103	664,402	4,871,552	534,653	**7,270,710**
Average UK market revenue (£M)	0.4	21	475	5,347	**2.7**

3 Dependence on Specific Cloud Service Providers

Use of CSPs varies by market segment (Exhibit 4). AWS has a strong presence across all size segments. Azure has high penetration among larger companies, with its strongest presence in the FTSE 100. Google Cloud Platform (GCP) sees its highest relative adoption among Micro and Small businesses.

Smaller, regional CSPs (Ionos, OVH, and DigitalOcean) have relatively high adoption among Micro, Small, and Medium businesses and provide viable alternatives for businesses with more focused or localised needs.

FTSE 100 companies dependence on cloud service providers



Companies may depend on multiple CSPs simultaneously, so provider-level dependency percentages are not mutually exclusive. Each table row in Exhibit shows the share of companies reliant on a given provider, meaning totals across providers can exceed 100% as firms adopt multi-cloud strategies.

4 Dependence on Cloud Regions

As might be expected, all UK company segments have their highest dependence in UK/Ireland cloud regions (Exhibit 5). However, the results show that Small companies rely more heavily on UK/Ireland cloud regions whereas Large companies have a greater distribution of cloud footprint across continents. Across all market segments, dependence on European (non-UK/Ireland) cloud regions typically exceeds reliance on US-based regions, driven by data residency regulations, latency considerations, and a preference for closer geographic proximity of providers.

In most cases, companies select the cloud region to host their data and services, rather than being constrained by auto selection, although this can be the case where there are limited CSPs available. For many UK-based companies operating within or serving EU markets, hosting data and services in the European region supports regulatory compliance (including GDPR), improves performance and reduces legal and operational complexity compared to using US-based infrastructure.

For FTSE 100 companies, the analysis focuses specifically on their UK operations, which increased the level of dependency in the UK/Ireland region. No such adjustment was made to the Large company segment, where cloud dependencies may reflect their global operations.

Exhibit 4 Dependence on cloud service providers

	Micro and small	Medium	Large excluding FTSE 100	FTSE 100	Total
AWS	34%	27%	50%	51%	**34%**
Azure	17%	40%	46%	70%	**18%**
GCP	28%	12%	9%	14%	**27%**
ionos	12%	11%	5%	1%	**11%**
OVH	5%	7%	2%	2%	**5%**
DigitalOcean	3%	10%	5%	2%	**3%**
Other	3%	2%	5%	2%	**3%**

Exhibit 5 Dependence on cloud regions

Region	Micro and Small	Medium	Large excluding FTSE 100	FTSE 100
UK/Ireland	56%	53%	40%	49%
Europe other	25%	23%	25%	27%
North America	17%	24%	31%	20%
Asia	1%	0%	3%	2%
Other	0%	0%	1%	2%

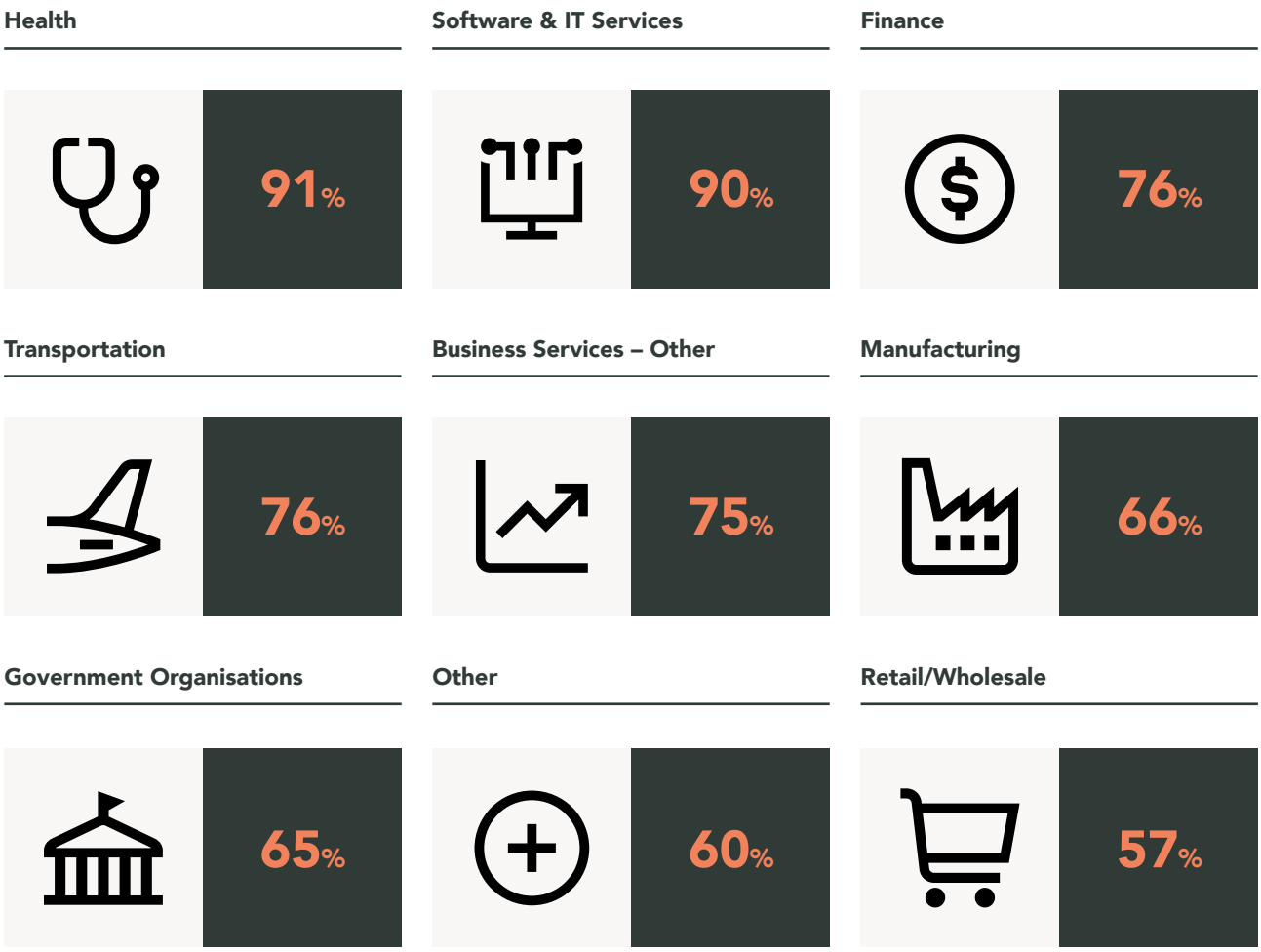
5 Cloud Dependence by Industry

In addition to variation by size of company, cloud dependency also varies by industry. To isolate the industry variation and focus on the most economically significant exposures the industry-level analysis focuses on Large and FTSE 100 companies only. Exhibit 6 shows the rates of cloud service dependency by industry.

Cloud dependency is highest in Health and Software & IT Services and remains relatively high in Finance, Transportation, and Business Services (including sectors like Management and Other Consulting, Human Resources, Accounting, as well as Other Enterprise and Household Services). By contrast, Manufacturing, Retail/Wholesale, and the Other category (including Construction, Mining, and Telecommunications) show lower levels of cloud dependency.

Cloud **dependency is highest** in Health and Software & IT Services

Exhibit 6 Cloud dependence by industry (Large and FTSE 100 companies)



6 Redundancy Measures

Redundancy refers to the duplication or backup of cloud functionality across multiple regions, to maintain business continuity in the event of a cloud region failure. Redundancy ranges from Active-Active, in which systems run concurrently across regions and enable seamless failover, to non-instantaneous solutions approaches such as Backup and Restore where data and systems can be recovered manually in a secondary region if the primary region experiences downtime.

In practice, companies typically apply redundancy to select systems. For example, a retailer may run its customer-facing e-commerce platform in an Active-Active setup across two cloud regions to ensure uptime, while its internal reporting tools or inventory forecasting systems may operate without any redundancy, accepting some risk of downtime. Although CSPs offer tools and infrastructure to enable redundancy, they do not implement them automatically. Companies must design, implement and fund redundancy architectures themselves, making redundancy a function of business priorities, cost tolerance, and risk appetite rather than technology availability alone.

As a result, redundancy appears far more frequently among Large and FTSE 100 companies, which have both the resources and the operational need to minimise downtime (Exhibit 7). Micro and Small businesses are much less likely to invest in redundancy, often due to budget constraints, simpler infrastructure needs, or limited technical capacity.

When assessing redundancy for Large and FTSE 100 companies by industry, redundancy is most prevalent in the Software & IT Services sector, where service uptime is mission-critical and customers expect minimal disruption. It is also relatively common in Business Services, which depend heavily on digital platforms. Redundancy is less prevalent in sectors such as Finance and Manufacturing, potentially reflecting greater reliance on legacy systems, lower cloud integration in certain functions, or risk models that prioritise other forms of continuity planning.

Given the limited number of Large and FTSE 100 companies in some industries, we aggregate smaller sectors into an "Other" category to avoid drawing spurious conclusions from small samples.

Exhibit 7 Redundancy measures by segment, weighted by company anuual revenue

	Micro and small	Medium	large excluding FTSE 100	FTSE 100	Total
Redundancy	4%	7%	33%	71%	**34%**
No Redundancy	96%	93%	67%	29%	**66%**

Exhibit 8 Redundancy measures by industry (Large and FTSE 100 companies)

Industry	Proportion with redundancy
Software & IT Services	41%
Business Services – Other	29%
Finance	16%
Manufacturing	16%
Other	21%
Total	**21%**

71% of FTSE 100 companies operate with redundancy, while only 7% of Medium companies do

7 Aggregation Points

An aggregation point typically represents a single region for a CSP. However, where redundancy is in place, an aggregation point may span multiple cloud regions that would need to fail simultaneously to cause business interruption.

Analysis of the largest aggregation points across different market segments shows that exposure patterns vary significantly by company size (Exhibit 9).

A UK economy-wide analysis of aggregation points (Exhibit 10) provides an understanding of the potential loss due to a major cloud outage event.

For example, the table shows that 12,554 companies are exposed to AWS's eu-central-1 aggregation point in Frankfurt, representing just 0.5% of UK companies, but accounting for a significant 7% of total revenue, highlighting the concentration of economic exposure at specific cloud regions.

Exhibit 9 Top aggregation points

Micro and Small		Medium		Large excluding FTSE 100		FTSE 100	
CSP	**Aggregation point**	**CSP**	**Aggregation point**	**CSP**	**Aggregation point**	**CSP**	**Aggregation point**
gcp	Europe-west2	azure	UK south	aws	eu-west1	aws	eu-west1

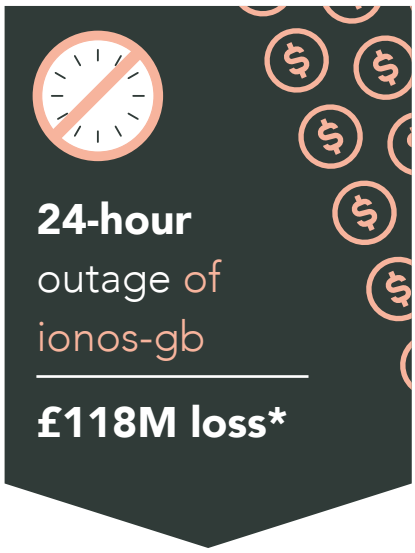
Exhibit 10 Top aggregation points for UK economy

CSP	Aggregation point	Location 1	Location 2	Number of companies exposed	Revenue of companies exposed (£M)	Percent of total companies exposed	Percent of total economy revenue exposed
aws	eu-west-1	Dublin		36,440	801,280	1.3%	11%
aws	eu-central-1	Frankfurt		12,554	542,974	0.5%	7%
aws	us-east-1	N. Virginia		21,606	856,804	0.8%	12%
azure	northeurope westeurope	Dublin	Amsterdam	37,530	1,204,492	1.4%	17%
azure	westeurope	Amsterdam		24,052	570,614	0.9%	8%
azure	uksouth	London		27,709	450,089	1.0%	6%

8 Direct Financial Impact to the UK Economy

The direct financial impact to the UK economy is then modelled based on different outage lengths at each of the aggregation points (Exhibit 11). These estimates capture the losses from businesses that use the cloud services directly. They do not include any downstream impacts on firms that rely on their outputs.

The financial impact of an outage to an aggregation point depends on the size and industry of companies that use the affected regions to support mission critical services. For example, a 24-hour outage of AWS eu-west-1 would generate a modelled loss of £1B, compared with £118M for an equivalent outage for ionos-gb, reflecting differences in the concentration of economically significant users.



*excluding downstream impacts

Exhibit 11 Impact on selected aggregation point

				Projected financial loss (£M)					
CSP	**Aggregation point**	**Location 1**	**Location 2**	**4 hrs**	**8 hrs**	**12 hrs**	**24 hrs**	**48 hrs**	**72 hrs**
aws	eu-west-1	Dublin		79	217	402	1,008	1,714	1,778
azure	uksouth	London		26	70	128	352	718	753
gcp	europe-west2	London		23	55	93	206	350	371
ionos	ionos-gb	London		7	20	38	118	262	274
azure	northeurope westeurope	Dublin	Amsterdam	29	77	142	350	550	569
aws	us-east-1	N. Virginia		42	119	227	647	1,392	1,483

*excluding downstream impacts

A 24-hour outage of AWS eu-west-1 would generate a modelled loss of **£1B** (excluding downstream impacts)

Why this matters

The findings reveal a UK economy which is increasingly dependent on cloud infrastructure, with exposure concentrated at a small number of critical aggregation points. This concentration creates systemic vulnerabilities that require coordinated action from companies, insurers, regulators, and policymakers to manage effectively.

For Companies

Understand their cloud exposure before disruption occurs. Many companies lack visibility into their cloud dependencies: which providers and regions they rely on, what revenue depends on those services, and how failures would cascade through their operations. The analysis shows that a 12-hour outage at a major aggregation point like AWS eu-west-1 could generate £402 million in direct losses across affected firms. Companies should map their dependencies, understand cloud usage of critical suppliers, quantify potential losses, and stress-test their business continuity plans against realistic outage scenarios.

Redundancy is essential but unevenly deployed. While 71% of revenue exposure of FTSE 100 companies employ multi-region redundancy, only 33% of Large companies and 4% of smaller businesses do. This gap reflects resource constraints but also creates disproportionate vulnerability among smaller firms that may lack the capital or expertise to implement resilient architectures. Companies must evaluate whether their redundancy strategies match their actual risk exposure and operational requirements, recognising that CSPs provide the tools but do not implement redundancy automatically.

Multi-cloud strategies alone do not eliminate risk. Even companies using multiple providers often concentrate their critical workloads in a small number of regions. Geographic diversity matters as much as provider diversity. Firms should assess whether their cloud footprint truly distributes risk or simply creates operational complexity without resilience benefits.

For Insurers and Risk Managers

Meaningful risk accumulations can be found at specific aggregation points. Three aggregation points: AWS eu-west-1, Azure northeurope/westeurope, and AWS us-east-1 support 40% of UK economic revenue exposure. A prolonged outage impacting any of these points could trigger simultaneous claims from many policyholders.

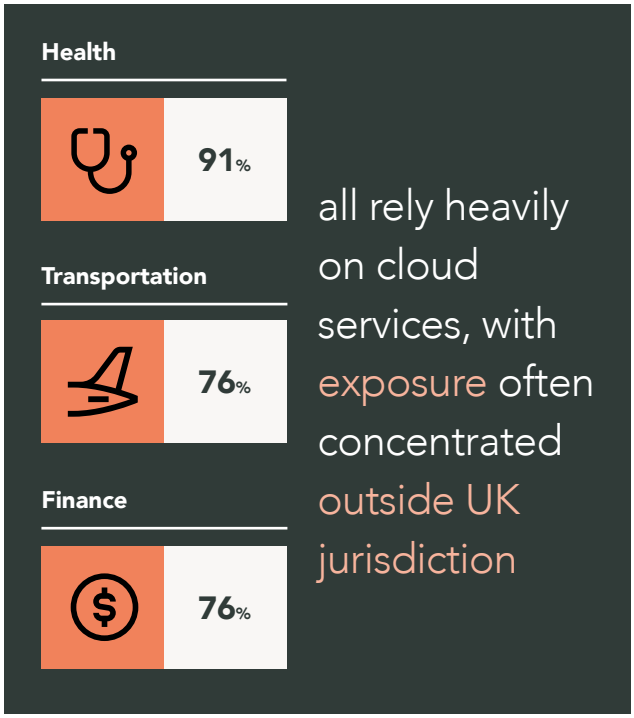
AWS eu-west-1, Azure northeurope/westeurope, and AWS us-east-1 **support 40% of the UK** economic revenue exposure

Direct loss figures substantially understate total economic impact. The modelled losses in this analysis exclude downstream effects on dependent firms and supply chains. Insurers must try to understand the full potential losses, particularly for outages affecting economically significant aggregation points.

For Policymakers and Regulators

Critical national infrastructure now depends on a small number of cloud providers. The analysis shows that Health (91% cloud-dependent), Finance (76%), and Transportation (76%) sectors all rely heavily on cloud services, with exposure concentrated in regions often located outside UK jurisdiction. This creates questions about digital sovereignty, regulatory reach, and the UK's ability to ensure resilience in critical sectors.

Monitoring and transparency are essential for preparedness. The Cyber Monitoring Centre's ability to assess cloud outage impacts in real-time depends on understanding exposure patterns and aggregation points before events occur. Ongoing monitoring of cloud region operational health, dependency shifts, and emerging concentration points should inform both policy development and incident response planning.



A Shared Responsibility

Cloud resilience is not solely a technical challenge or a problem for individual companies to solve in isolation. The systemic nature of cloud dependencies means that outages at key aggregation points can cascade across industries and affect the broader economy. Effective risk management requires companies to build robust architectures, insurers to price and cover these risks appropriately, and policymakers to ensure that regulatory frameworks and support mechanisms keep pace with the reality of cloud-dependent critical infrastructure. As cloud adoption continues to accelerate, the strategies used to manage these dependencies must evolve in parallel.

Cross-border dependencies create regulatory complexity. Significant UK economic activity depends on US-based infrastructure, particularly AWS us-east-1, which supports £857 billion in UK company revenue. Outages in these regions could affect UK businesses while falling outside UK regulatory authority, highlighting the need for international coordination on cloud resilience standards.

Smaller businesses face disproportionate barriers to resilience. Only 4% of revenue exposure of cloud dependant Micro and Small businesses employ redundancy measures, compared to 71% of revenue exposure of FTSE 100 companies. This gap reflects both cost constraints and limited technical capacity. Policymakers should consider whether support programmes, guidance, or incentives could help smaller firms improve resilience without imposing unaffordable compliance burdens.

About CMC and Parametrix

The Cyber Monitoring Centre (CMC) was established to analyse major cyber events affecting the UK economy. Operating as a non-profit, independent entity, the CMC assesses the economic impact of cyber incidents as they unfold, providing timely insights to government, businesses, and the insurance sector.

The CMC's work focuses on quantifying both direct and downstream economic losses from cyber events, including ransomware attacks, data breaches, and infrastructure failures. By developing robust methodologies for impact assessment and maintaining ongoing monitoring capabilities, the CMC helps stakeholders understand the true scale of cyber risks and supports more informed decision-making on resilience and preparedness.

This white paper represents part of the CMC's broader effort to build foundational understanding of UK digital dependencies and vulnerabilities, enabling more effective response when major incidents occur.

Parametrix, the leading provider of digital business interruption solutions, specializes in parametric insurance that protects against the financial cost of technology and digital infrastructure downtime. Leveraging a proprietary network of monitoring systems, they collect and analyze real-time, granular data on the performance and availability of critical infrastructure – including data centers, SaaS providers, and cloud services – to accurately assess risk and deliver fast, transparent claims payments. Their solutions enable businesses, data center stakeholders, and (re)insurers to quantify, manage, and transfer the financial risks of downtime with unmatched precision.

Parametrix provides the Cyber Monitoring Centre with ongoing monitoring of global cloud infrastructure to understand the duration and impact of cloud outage events that have significant UK company exposure.

Parametrix is a Managing General Agent and Lloyd's Coverholder, with policies backed by major A-rated global insurers, and is headquartered in New York. Parametrixinsurance.com

Cyber Monitoring Centre

info@cybermonitoringcentre.com
cybermonitoringcentre.com