



G-Cloud 15

Safe Transition to Cloud

January 2026

Contents

Transforming Business using the Cloud 3

Safe Transition to Cloud..... 5

 G-Cloud Safe Transition to Cloud Service Description..... 5

 Our cloud experience – how can we help? 6

 1. Security and privacy 7

 2. Regulatory, governance and control 8

 3. Resilience 11

 4. Cloud strategy and business case.....13

 5. Operating model.....15

 6. Vendor management..... 16

Transforming Business using the Cloud

Enabling business and enterprise transformation using the Cloud is a complex, strategic consideration facing many private and public sector organisations. We have worked with many Central and Local Government clients to support the implementation of their business objectives using Cloud technology.

Cloud technology and services have the potential to reduce cost, remove technology bottlenecks, and facilitate rapid business innovation. As a result, for most organisations globally, adopting Cloud technology has become a question of “when and how” rather than “if”.

Opportunities for enterprises generally include a combination of one or more of the following:

- Implementing private and/or hybrid clouds for infrastructure and applications
- Smarter use of public cloud infrastructure for optimising existing business functions
- Using the Cloud for implementing new business services or digital operations
- Reducing cost by moving to consumption-based pricing models that only charge for the actual IT capacity and services used.

Cloud migration or adoption must be properly choreographed for success. We understand the realities and the business and technical risks that need to be fully considered, understood and mitigated before such a move. Critical considerations include:

Alignment of business and technology objectives. This is essential to fully realise the targeted benefits of any cloud transformation or any refinement of existing cloud services. There can be a tendency to adopt cloud systems to fit current ways of working, rather than adopt and standardise processes where possible. The trade-offs between business, customer and technology requirements must be considered to make informed design decisions

Availability and reliability of services. The avoidance of operational downtime to mitigate lost revenue, unnecessary operational cost or reputational damage that can disrupt business operations

Decentralised support structures. The need to tailor and revise the approach to operational security to cover the support structures employed by cloud service providers that will have a different risk profile for sensitive information

Data handling practices. Data classification and data-handling practices that reflect the data flow within a cloud environment must be understood and tailored accordingly to protect customer data

Data privacy. Compliance with GDPR to understand where and how information can be stored or processed. The Cloud model enables data to bounce swiftly around the world by using available server capacity in various geographic locations, but this must be within the bounds of what is permissible. This is ever more of a concern as organisations review their front office, back office and out-of-office experiences

Future Technology Trends. Cloud applications are the stated direction of travel for the major application vendors, but any upgrade path must also cater for the future technology needs of the organisation and seek to minimise technical debt where possible.

A careful assessment of an organisation's needs and different cloud service provider's controls is required, enabling concerns to be addressed and the correct path to the Cloud to be selected.

As a trusted advisor PwC provides the framework, and the wealth of private and public sector experience, to consider the combination of Business, customer experience and Technology activities outlined above. There is no single answer that covers each and every client organisation; we tailor our frameworks to client circumstances to support them:

- As a partner through the complete lifecycle of strategy to execution
- With point business issues encountered during implementation or running the business.

Safe Transition to Cloud

This section describes the service features and benefits included in this service definition document in more detail.

G-Cloud Safe Transition to Cloud Service Description

Our research shows that more than half of organisations that have adopted Cloud have not realised the outcomes they were expecting¹. Whether needing to cut costs, improve resilience, enable new business processes or change business models, tangible value is elusive for many.

So, why is this? The big issue when moving to the Cloud or running parts of your business in the Cloud is not the same as being cloud-powered.

Cloud-powered companies and organisations have reinvented their businesses through Cloud. They report fewer barriers to realising value and they're doing so at a rate twice that of other businesses. They consider the specific, potential risks that the Cloud poses throughout all stages of their transformation journey and react accordingly to be more resilient and confident in their decision-making.

We help our clients become cloud-powered through navigating uncertainty and changing the way they respond to the risks that the Cloud poses. We call this "Safe Transition to Cloud".

1: PwC Cloud Business Survey (2023): <https://www.pwc.com/us/en/tech-effect/cloud/cloud-business-survey.html>

Safe Transition to Cloud Services Features	Safe Transition to Cloud Services Benefits
• Cloud strategy and business case: Financial Case and TCO confidence • Governance, controls and regulatory: programme oversight, compliance, risk management • Security, privacy and data protection design and assurance, ecosystem security • Cost & commercial excellence: FinOps, cost optimisation, supplier management, consumption forecasting • Resilience architecture design and assurance, technology stability, recovery and testing • Operating model - shared responsibility model and people skills/competencies.	• Reduced risk and increased confidence in Cloud benefits • Verifiable Cloud Cost Assurance, TCO confidence and functional FinOps • Reduce the risks of contract disaggregation and improve service delivery • Increased management decision effectiveness relating to transformational change • Improved business outcomes, benefits realisation and business engagement • ALB development plans and controls which support integration and independence.

- Data & analytics strategy, architecture, design, assurance. Data migration & engineering.
- Sustainability designed for net zero, transparency and reporting.
- AI by design.
- Support to evaluate hyperscale migration and end-to-end sovereignty.

- Business Cases that deliver value for money and strategic change.
- Improved value for money from digital, technology and transformation investments.
- Increase engagement between the business and digital / technology functions.
- Reduce cloud integration risks while improving legacy and removing obsolescence.

Our Cloud experience – how can we help?

In recent years, leaders have pushed their organisations and themselves beyond their comfort zones:

- Out of the office to remote workplaces (and back towards hybrid)
- Into the Cloud both through migration of existing environments and by adoption of cloud-native platforms into supply chains that are almost completely digital
- Into increasingly product-oriented delivery ecosystems.

Cloud transformation provides a significant challenge. Moving to new world technology with a backdrop of ageing, legacy or obsolete IT, systems and processes and has been done successfully, but requires a robust and highly focused programme of work.

With each new venture has come new risks. Leaders are recognising that their bold moves have increased their organisations' risk exposure, and that to work differently, they must think about risk differently. We use the **Safe Transition to Cloud Framework** to guide our support for organisations before, during and post their cloud transformation.

For all the service features, benefits and scope areas discussed in this service description document, we can help you to understand your risk landscape by:

- Reviewing your performance against industry standard frameworks and vendor good practice as well as our own experience
- Identifying risk, assessing the planned mitigations you've considered, and the gaps you haven't
- Support you to define your improvement plan, as you become cloud-powered.

We can also support you implement your improvement plan through a variety of support models, all of which seek to upskill your team during delivery to leave you more capable and resilient than before we started.

Our view on the service features and benefits in this service definition document are presented below.

1. Security and privacy

According to our 2023 Global Digital Trust Insights survey, cloud management interfaces are the third most common threat that organisations worry about (following business email and ransomware). 49% of IT decision makers rated improved security and compliance as one of the most important outcomes of migrating to the Cloud in a study conducted by Forrester Consulting in 2022.

We have set out the security and privacy themes we can support you with here.

Secure platform: It is imperative that organisations give appropriate focus and consideration to securing the foundations of cloud environments.

Failing to implement foundational controls to appropriately secure the Cloud platform can lead to an increased attack surface and risk posture, and appropriately managing technical debt as part of a cloud migration programme (especially for lift and shift) is key to managing residual risk.

Examples of how we can support you include:

- Support to leverage your Cloud Service Provider's (CSP's) 'well-architected' frameworks to help accelerate your securing of foundations and landing zones
- Assistance in defining, implementing and assessing cloud native controls and principles based on good practice and our experience to help you achieve an expected and effective level of security and protect the business value of your Cloud investment.

Security ecosystem: Organisations that adopt a hybrid or multi-cloud strategy need to ensure they take an enterprise-wide view of technology, people and process.

If an enterprise-wide view is not established before starting a cloud transformation programme, organisations are typically left with a fragmented architecture, duplication of effort and gaps in visibility leading to an increased risk profile. This needs to be considered across people, process, technology, governance and reporting lenses to achieve the transparency, efficiency and security needed.

Examples of how we can support you include:

- Support to develop your focus on key cross platform enterprise controls, such as Identity and Access Management, Visibility and Data Security
- Assistance to achieve cloud principles (e.g. cloud first, future fit, simplicity and zero trust).

Data protection and data residency: Moving sensitive data into cloud environments requires careful consideration in relation to the protection of data; both in terms of security and privacy controls.

Many organisations experience data fragmentation between multiple different cloud providers leading to a lack of visibility and control over sensitive data. Coupled with legacy applications and historical data, we see significant risk that such environments may not align with current privacy principles (e.g., accuracy and data minimisation). This can lead to requirements for unplanned work impacting both the timeline and cost of a cloud transformation.

While many organisations continue to migrate to the Cloud, poorly configured tenants and a lack of understating of personal (and/or corporate sensitive) data flows and storage out of the UK/ EEA into third countries can mean contractual and/ or technical provisions are not put in place, leading to increased data residency risks, and the potential to expose private UK public sector data to overseas entities.

Examples of how we can support you include:

- Support to analysis, document and implement cloud-native data controls (i.e. data classification, data discovery, data loss prevention, encryption, segmentation and access management) across your environment
- Help to make practical use of assurance reports provided by CSP(s) to help provide clearer visibility over technical privacy controls and reduce the cost/effort for second- and third-line functions
- Review of your data lifecycle management capabilities (i.e data minimisation, data retention) enabling a simplified approach for data migration, and support to define and implement improvements.

2. Regulatory, governance and control

Governance is a key concern for cloud-powered companies with, according to PwC's 2023 Cloud Business Survey, 80% having cloud governance resources in place and 78% stating they have "formal and distinct cloud controls". 33% of IT decision makers rated regulatory and governance concerns as one of the top 3 challenges of migrating to the Cloud in a study conducted by Forrester Consulting in 2022.

Regulatory, governance and control themes we can support you to consider include:

Scrutiny and oversight: UK authorities recognise the potential benefits of Cloud adoption. However, they are concerned about significant associated risks including:

- Over-reliance on a single or small number of CSPs
- Concentration in the CSP market and the potential for systemic disruption to the financial system should a CSP fail

- Failure by regulated firms to properly maintain oversight of functions outsourced to CSPs, in accordance with the provisions of SYSC.

Increasing scrutiny of technology, data and cyber investments is being experienced across the public sector. Organisations need to demonstrate a financial case for investment and be ready to demonstrate compliance with standards issued by central functions like Central Digital and Data Office, Government Digital Service, and Government Security Group such as the HMG Standard for Generative AI. Across industries we have seen authorities exercise powers to halt an organisation's cloud migration if they determine that there is inadequate oversight and accountability from the executive team.

Expectations and requirements are continuously evolving, and there is likely to be continued focus on the use of CSPs. Failures in relation to CSP oversight is a critical risk to government organisations, who need confidence that CSP are acting as expected, to avoid risk of data loss, reputational damage and costly periods of enforced supervision / remedial action.

Examples of how we can support you include:

- Support to define requirements, review compliance and implement technical, data and cyber processes in line with industry standard frameworks including but not limited to ITIL, COBIT, and NIST and our own good practice. Organisations must take a proactive approach and address emerging themes such as resilience, exit planning, concentration risk, hybrid cloud, portability, and data protection
- Help to implement effective risk management strategies, to demonstrate your commitment to the standards expected by government (and where relevant, regulators), and to build trust
- Advisory services to undertake early and through delivery reviews of plans, designs and technical process for cloud migration, to provide confidence that cloud adoption plans are achievable, value for money and support your business strategy.

Policies, Standards, Controls and Risk Management: When adopting the Cloud it is essential to establish clear policies, standards, and controls to align the organisation's cloud usage with its risk management strategy.

We have worked with many organisations who have found updating and implementing risks standards and controls with the Cloud a significant challenge. Example risks include:

- The extent to which the organisation is ready to handle opex charging for services, having historically used capex investment to build services
- Lack of financial controls (such as FinOps) suitable for the environment(s), technology changes including immutable (short-lived) infrastructure
- The risk of increased costs and lack of visibility.

The increasing trend to decentralise IT and enable business teams to manage their own cloud environments can create situations without sufficient governance which can lead to a lack of visibility and control. This may result in operational inefficiencies, increased security risks, and difficulty in maintaining compliance with standards.

Examples of how we can support you include:

- Support to determine your risk appetite and how to apply a risk-based lens to governance and control processes to enable accelerated transformation proceeds and reduce risk
- Reviews to identify gaps in, and deviations from, policies, standards and controls together with remediation plans to enable them to be updated to accommodate the expected business outcomes
- Assistance to define roles and responsibilities across the organisation so that those accountable and responsible for delivering the Cloud (and the products which run on it) are able to properly discharge their responsibilities
- Help to consider how you can ‘codify’ policies and standards as part of your cloud deployments to enable guardrails for cloud deployment, making future implementation of products safer
- Focused support to consider shared responsibilities (e.g. relying on the Cloud Service Providers to provide relevant attestation of controls e.g. SOC Type II, NIST, ISO27001 etc.), including how this could impact the organisation and how and where controls need to be refined as a result.

Programme Oversight: Implementing robust programme management is critical when undergoing significant transformations, with support from both technical expertise in the first line and risk oversight in the second line. This approach helps ensure that transformation initiatives are carried out efficiently and with minimal risk to the organisation.

In our experience it is crucial to establish effective oversight / assurance mechanisms and to have the Executive accountability to mitigate risks and avoid potential disruptions to cloud migration plans. Enterprise Architecture needs to be a key part of the transformation as the link between strategy and execution. This allows the right strategic and design decisions to be made to limit any technical debt and operational inefficiencies.

Examples of how we can support you include:

- **Assistance to establish effective executive oversight:** From a risk perspective this is crucial for successful cloud adoption. We can help you to build the right strategic support from key roles such as the Chief Information Security Officer (CISO), Data Protection Officer (DPO), and Chief Security Officer (CSO)
- **Design and implementation** of secure, resilient, and privacy-focused design governance which should be an integral part of the overall Architecture Governance Framework for cloud adoption

- **Support** to establish a core set of enterprise architecture principles upfront, to guide your cloud adoption strategy. This helps you to align cloud architecture with your long-term goals and requirements.

3. Resilience

The prominence of operational resilience with financial services regulators reflects its importance in maintaining the functioning of, and confidence in, individual and collective UK financial institutions. The UK is intentionally driving a step-change in how firms consider resilience through the lens of customers and markets which traditionally had a narrow focus of business continuity. In practice this also increases expectations from citizens on how they experience and consume services, and from employees on how they expect internal services to be joined up and delivered.

Evolving risks from third-party ecosystems and greater reliance on outsourcing and third-parties brings benefits and opportunities, including in the case of Cloud, the potential for enhanced resilience and security compared to on-premises systems. However, experience has taught us that these need to be designed carefully and specifically for the services in question, to be confident that services will ‘really’ be resilient in the event of a critical incident.

Resilience themes we can support you to consider include:

Operational Resilience: The ever increasing focus on operational resilience from both a regulatory and business perspective is driving increased expectations. This should be considered as early as possible as part of any significant transformation to understand how to build operational resilience into critical operations by design.

Our work across Financial Services shows that organisations seeking to implement operational resilience need to carefully consider how risks faced change during transformation and into the Cloud. For example, in third-party, technology and data, so as to not inadvertently impact the resilience of critical operations.

Examples of how we can support you include:

- Support to build business and external stakeholders’ confidence that your operational resilience plans and practices are robust, effective and value-for-money, through the definition of robust and effective operational resilience practice and processes
- It may be the case that public sector organisations consider using components of the requirements set out in the EU Digital Operational Resilience Act (DORA) as a starting point for defining their own requirements, even if they are not subject to the regulation. We are ideally suited to support your design, implementation, testing, and review of operational resilience processes and controls
- Support to determine the effectiveness of your processes which identify, and drive remediation of, aged, legacy and obsolete technology, services and systems. Help to quantify the extent to which you

are impacted by such systems and services and help to define and execute your remediation programme.

Technology stability: Disaster recovery has a significant impact on an organisation's ability to deliver. Strong ITSM practises and tooling will need to evolve to manage a hybrid IT environment and support new cloud services, including external SaaS providers, alongside existing on-premises systems. Organisations need to put in place the mechanisms to identify, assess and monitor their risks against risk appetite and tolerance.

Our experience is that many organisations don't have a complete, up-to-date and end-to-end view of their estate. Accordingly, their ability to effectively manage the estate and recover from incidents will be compromised.

Robust design, implementation and assurance of both the technical and people activities needed to recover from incidents are needed, together with detailed work instructions for unique use cases where relevant (for example in the case of a suspected ransomware incident). Together these need to be tested before confidence can be placed in their capability and capacity to support the business.

Examples of how we can support you include:

- Definition and execution of your business continuity and IT disaster recovery (DR) workstream through your implementation / migration to the Cloud. This includes the opportunity to assess each application migrated or service onboarded against your business impact assessment (BIA) and DR requirements
- Support to develop your BIA and ITDR requirements and processes in line with business needs, including working with suppliers to determine their ability to meet requirements
- Design and implementation of revised BC/ITDR practices and processes across the organisation and your supply chain
- Post incident review
- Support to review, update and implement new ITSM processes for recovery and dependent ITSM components
- Assistance to leverage automation to keep asset repositories (i.e. CMDB) up-to-date.

Concentration risk Concentration risk is a systemic and firm-specific consideration. Organisations need to be mindful of where its' critical operations are delivered from, so they can assess and manage the risks created by concentrating services into locations, suppliers or territories.

While most organisations are using the Cloud in some manner, their consideration of cloud risk is often limited to considering the Cloud as 'the answer' when really it provides a different set of questions. For example, while on-premise system and facility designers are familiar with geographically distributed data

centres and diverse network providers, this level of transparency is not available to cloud customers - so what changes are needed in a cloud environment?

This example of concentration risk shows it should be explicitly considered, including but not limited to:

- How risk is built into your current or planned use of the Cloud
- How it extends to portability and multi-cloud strategies which could impact future decision making.

We can support you to identify concentration risk and plan and design changes which can mitigate the specific concentration risk you face. Amongst other examples, this may include multi-cloud, portability, exit planning strategy and hybrid cloud migration planning. To define an approach which is right for you these need to be carefully considered against the limitations of each approach.

4. Cloud strategy and business case

According to PwC's 2023 US Cloud Business Survey, over half of organisations have yet to realise the benefits they sought from their Cloud migration: cutting costs, improving resilience, driving new revenue, and others. In addition, 58% of organisations overspend their cloud budgets (source: Apptio).

51% of IT budgets will be dedicated to the Cloud by 2025 with spending on public cloud expected to increase by 29% in the next 12 months (source: Flexera State of the Cloud Report, 2022). From a taxpayer and citizen perspective this must be shown to be robustly in the public interest, and to deliver value-for-money.

Cloud strategy and business case themes we can support you to consider include:

Modernising with the Cloud: Managing risks and realising full benefit of Cloud requires a change from legacy on-premise architectures and ways of working. Typical approaches from CSPs consider the most appropriate modernisation approach for applications and services. At first glance, it may seem simpler to complete a 'lift and shift' migration from the data centre, however our view is that this increases risk and the amount of likely rework in the medium-term to enable IT to support business strategy ambitions.

A 'lift and shift' approach also doesn't enable the business transformation often envisaged as part of the move to the Cloud, or the productivity and cost management approaches that the Cloud can enable - eroding business value further.

Examples of how we can support you include:

- Support to increase use of cloud native technologies to increase transparency and efficiency in IT costs
- Assistance to identify, implement and optimise new features and continued resilience and control

- Help to identify, qualify and quantify the risks associated with a planned move to cloud, or those inherent in your cloud strategy together with appropriately designed mitigation strategies.

Business strategy enablement: A streamlined technology strategy aligned to the strategic goals and objectives of the business will increase service and product innovation capabilities whilst increasing margins and adhering to security compliance requirements.

In our experience, misalignment between stakeholder expectations, business needs and technical methodologies for migration to public, private or hybrid cloud can lead to lower stakeholder engagement and lower benefit to the business. Our experience in building value through both back office and customer-facing systems during their move to the Cloud will be beneficial here.

Examples of how we can support you include:

- Design, build or assure your cloud strategy / migration business case
- Identification acceleration opportunities to support you to implement your strategy faster
- Define and plan the “must stop” activities which should no longer take place once you move to cloud, and assistance to move equivalent activities (where relevant) into cloud enabled processes
- Support to review, recommend and implement change across your portfolio design function to assist their adoption of processes which enable cloud success
- Support to develop appropriate metrics, reporting and insights to effectively track and manage your progress through delivery.

Benefit planning, monitoring and realisation: Organisations should place emphasis on the ongoing monitoring of business benefits, including cost, security, agility and resilience. Focus should be placed on optimising Cloud as an aspect of business value enablement.

Our experience various project types shows that failure to monitor business benefits is likely to result in unachieved business goals and can lead to increased operational costs.

Financial benefits need to be explicitly planned and delivered (including against which budget) so that expected cost savings can be realised. Non-financial benefits need to be designed and expertly managed into reality as too often these can be ‘de-scoped’ resulting in future cost and rework.

Examples of how we can support you include:

- Definition of value-based metrics to demonstrate the business impact and return on investment
- Support to make conscious trade-offs between cost, quality and speed of execution
- Assistance to reimagine your core business and think of cloud as a driver of innovation - identifying and delivering further benefit where this represents value-for-money.

5. Operating model

The people aspects of multi-cloud are often neglected. When organisations need to adopt cloud at pace, they need to establish new, skilled teams to support a new cloud platform, requiring investment and time to recruit and upskill existing teams. Often, resources from existing cloud (or on-premise) teams are transitioned to support the establishment of a new platform, which strains resources overall and can create risks for resilience or change activities.

According to research published by PwC in 2022 including more than 3,000 IT and IT security practitioners, only one in three respondents said protecting data in the Cloud is their responsibility. 35% said CSPs bear the most responsibility for sensitive data in the Cloud and 33% said the responsibility is shared.

Operating model themes we can support you to consider include:

Shared Responsibility Model: Shifting from a traditional, on-premises set-up to a Cloud set-up changes the responsibilities of the customer. This may include SaaS, PaaS or IaaS-based models. Shared responsibility does not mean outsourced responsibility as it is incumbent on organisation to set the responsibility and accountability foundations with their cloud provider.

Cloud introduces additional complexity in security configuration and risk management of certain services, over and above those inherent in systems. Actors in the responsibility model need to be familiar with processes, roles and responsibilities in the Cloud. If shared responsibilities are not defined clearly, it may lead to a lack of risk ownership and service disruptions.

Examples of how we can support you include:

- Design, implement or review your governance framework across the Cloud including how it governs shared responsibilities with the CSP
- Develop and mature your TOM and RACI Model to better articulate ownership for your organisation and the CSP
- Support to consider which type of Shared Responsibility Model will be most effective for your organisation. What do you want to be responsible for, and what risk do you want your CSP and supply chain to support?

People skills and competencies: Successful transition and operation of Cloud-enabled business services requires teams with cloud-specific technical acumen based on the chosen operating model.

Without a team skilled in cloud-related competencies (e.g. cloud engineers and architects, DevSecOps, etc) you may not be able to leverage the Cloud as desired, owing to capacity or capability constraints, or to similar restrictions in your supply chain.

Particular attention needs to be paid to how people will be rewarded and motivated in a shared responsibility operating environment, both to enable you to attract talent, and to avoid the risk of talent loss where in demand skills leave your organisation.

Examples of how we can support you include:

- Understand your cloud TOM and its underlying services
- Identify the skills needed to support your cloud operations
- Develop skills programmes including training and identifying skills gaps for resolution
- Support to develop effective teaming practices with your supply chain partners.

Cloud Centre of Excellence (CCoE): A common CCoE model that delivers Cloud adoption with transformed business and IT operating models, adopting a new, cloud-native business strategy and operating model.

We have seen in many organisations how lack of a Cloud CoE may lead to inconsistent practices which expose organisations to reputational, security and financial risks. In addition to understanding the estate in depth (to enable resilience practices, see above), it is also critical to develop consistent and standardised operating practices across your organisation to deliver standardisation, sustainable development and support practices, and to reduce long-term cost.

Examples of how we can support you include:

- Support to develop your effective policy, process and control set for public, private and hybrid cloud environments
- Rapid assessment and evaluation of control design and performance
- Help to build management information and reporting tools which support you to manage risk in real time
- Develop training, upskilling and real-world events like hackathons which support democratisation of skills and encourage good practice
- As you promote product mindsets and democratise access to technology, we can support you to develop a group of skilled individuals who are able to guide you on striking the right balance between control, agility and empowerment, and to move towards a trust and verify model.

6. Vendor management

Cloud technology innovation is disrupting the traditional controls used by organisations to manage IT spend. Many organisations have found themselves ill-equipped to stay on top of escalating consumption-based charges, and sizable contracts which underpin them.

New approaches to controlling cloud spend are being adopted in their organisations to optimise arrangements with the CSPs, however they need to consider the risk in their end-to-end supply chain. For example, only three in ten businesses have undertaken cyber security risk assessments of their supply chains in the last year as per the DCMS 2023 Security Breaches Survey.

Vendor management themes we can support you to consider include:

Third party risk management: Hyperconnectivity via third-party enables extensive optimisation, but it increases their attack surface due to complexity of interconnection of data and supply chain ecosystems. It is incumbent on organisations to identify, protect, detect, respond, and recover from third-party related threat events through robust supply chain risk management and understanding of the shared security risk model.

We have experience in supporting clients to identify, mitigate and manage third party risks. This experience extends to supporting recovery from failure to adequately manage third-party risk where resulting issues have caused critical failures. Failure to manage third-party risks can result in regulatory penalties, financial loss, reputational damage and impact your operational resilience.

Examples of how we can support you include:

- Support to establish a cloud specific third-party risk framework integrated to your enterprise supply chain risk management approach
- Design, implementation and review of practice and tools used to surface risk in your cloud workloads and infrastructure, enabling you to have a rapid and effective means of risk mitigation.

Exit planning: A gradual unwind of the cloud vendor, or sudden loss of a critical third-party requires planning and preparedness to minimise disruption to the business and customer.

While most organisations are discussing moving to the Cloud, we must also consider exit to enable graceful transition between suppliers, and continuity of service. We have seen first generation Cloud contracts and suppliers fail to adequately define exit responsibilities and poor execution of exit plans. This inevitably results in delays, unplanned and unexpected costs.

Unless this is done well, the risks of further disruption to business and customers due to loss of a critical service or an unplanned exit is high. Transition or exit may also pose data security and privacy risks if processes are not in place for the secure transfer and destruction of sensitive data during exit.

Examples of how we can support you include:

- Support to embed exit planning in your procurement process with cloud vendors, that allows you to conduct exit strategy simulations similarly to a BCP test, through a regularly scheduled “lights out” test at both the vendor and your organisation

- Help to review exit plans and / or to independently review your exit activities to build confidence they are well planned, controlled and likely to succeed
- Assistance to establish methods for secure transfer and destruction of your data as part of the exit strategy.

Commercial control and supplier management: A lack of understanding and confidence in how Cloud spending differs from on-premise, including the shift from CapEx to OpEx flows, can prevent businesses from maximising economic efficiencies. That and an inconsistent approach to deployment and optimisation of cloud spend can result in the business case failing to deliver anticipated benefits.

Lack of alignment between contractual commitments and consumption of cloud resources can result in suboptimal commercial arrangements with CSPs, often realised in friction in joint processes and breakdown of communications.

Poor use of tooling to manage complex cloud data, coupled with poor planning and controls across processes can quickly result in higher costs than expected or budgeted.

Examples of how we can support you include:

- Support to develop people, processes and technology to sustain continuous optimisation of cloud spend by choosing the right pricing models, matching capacity with demand, and identifying underutilised resources. These optimisation activities will free up investment for business growth
- Design and implement operating model changes need to be made to enable FinOps function to maximise value by helping IT, finance, commercial and operational teams to collaborate on data-driven spending decisions
- Undertake assessment of your cloud spend, alongside reporting from your CSP supporting you to identify technical, process and responsibility changes which will reduce cost in your cloud services.

We welcome the opportunity for further discuss any of the example support area discussed in this document, together with further examples of how we can support you with Safe Transition to Cloud.



Confidential. This document does not constitute a Call-Off Contract for Services with PricewaterhouseCoopers LLP. Where we are engaged to provide Services, our Services will be governed by a subsequent Call-Off Contract that may be entered into between us. If you receive a request under freedom of information legislation to disclose any information we provided to you, you will consult with us promptly before any disclosure. All information contained in this document or otherwise provided or made available as part of any Award Procedure is confidential and may not be disclosed to anyone else without our prior consent.

© 2026 PricewaterhouseCoopers LLP. All rights reserved. 'PwC' refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.