INSIGHT

Guidance for audit committees on cloud services

National Audit Office

Good practice guide

September 2024

This guide provides insights and sets out questions for those responsible for overseeing cloud services to ask at each stage of assessment, implementation, management and optimisation

We are the UK's independent public spending watchdog

Communications Team
DP Ref 015434

About our guide

Who is the guide for?

We published the original edition of our *Guidance for audit committees on cloud services* in 2019, with an updated version issued in 2021. Gaining suitable assurance is complex and difficult, and our aim is to help audit committees understand the cloud-related questions they might need to ask of management.

Since we last published this guidance, more of the public sector has adopted cloud services, with a matching increase in government spending with the big cloud providers. Government's digital and commercial functions have also continued to develop their cloud strategy and associated guidance for the public sector.

Our audience found our previous guide to be valuable, so we have updated it to reflect the growing adoption and evolution of cloud services and to keep it relevant.

What does the guide cover?

Our guide sets out specific questions for audit committees to consider when engaging with their management. Our other related support for audit committees includes *Cyber security and information risk guidance for audit committees* and *Transformation guidance for audit committees*. In addition, we have published a guide to *Digital transformation in government* and a report on the *Use of artificial intelligence in government*.

This guide takes a lifecycle approach and poses informed questions at three key stages.

- **Strategic assessment of cloud services:** This section covers both first-time adoption and continuing re-appraisal and re-evaluation of cloud services as part of early lifecycle organisational and digital strategies, the business case process, and due diligence.
- **Implementation of cloud services:** This section covers mid-lifecycle implementation and considers system configuration, data migration, and service risk and security issues when moving from one cloud provider to another, or from on-premises to cloud for the first time.
- **Management and optimisation of cloud services:** This later lifecycle section covers operational considerations, the need for assurance from third parties, the capabilities needed to manage live running, and how to continue to control costs.

Why does this need attention?

Government has developed digital policy to support moving to the cloud for over a decade, and the number of cloud services continues to increase. But some organisations may lack the capacity and expertise to choose the right services for their needs, implement them securely, and continue to use them effectively. In particular, organisations should not under-estimate the cost and effort of moving to cloud solutions and the investment needed in skills and processes to manage and optimise them. These challenges are most likely where multiple suppliers are involved. The skills needed are not just technical ones. Commercial skills will also be needed to understand and manage cloud services. Also, senior management needs to understand the risks involved.

Well-managed cloud services can be more secure than local or on-premises technology. The threat levels for both are broadly the same, but cloud providers can use economies of scale and concentration of expertise to their advantage. This strength of scale offers a level of security that would be difficult for many organisations to provide on their own. Cloud providers invest heavily in security because otherwise their businesses are at risk. However, customers should not assume that the cloud provider is taking care of all aspects of security on their behalf. Some services have differently priced options with different levels of security features available. All cloud services require users to ensure that the security set-up is in line with their needs, including that data is not left open to a wider audience than intended. This point cannot be over-emphasised: the key to a successful security implementation in a cloud environment is understanding where the cloud provider's responsibilities end and where the customer's responsibilities begin. This is called the 'shared responsibility model'.

Implementation of cloud services is not a 'once and done' endeavour. While the cloud may sometimes save money, organisations should not assume this will always be the case without a detailed analysis of their total cost of operation and the opportunities for optimisation. For example, a 'lift and shift' migration of existing applications to cloud hosting is likely to require further work to take maximum advantage of the benefits that a cloud environment can offer. It does not automatically improve the data or applications themselves.

Introduction

An overview of cloud services

Cloud services are a combination of systems and data hosted by third parties and accessed by users over the internet. This is in contrast with traditional systems where hardware and software are maintained on an organisation's own premises and accessed over a traditional corporate local or wide area network. Cloud services are not a new concept and have been available in one form or another for over 25 years. Today many organisations invest heavily in the cloud and well-established offerings are now available to meet a wide range of organisational needs, including business and financial systems.

Cloud services are heavily promoted as providing a wide range of benefits, including efficiency, flexibility and security. These benefits may be achieved through the cloud provider's access to resources, expertise and economies of scale.

Cloud financial and operating models have moved away from capital investment funding and fixed utilisation arrangements to more flexible models such as 'pay as you go', which transfer more costs to operating expenditure. This gives organisations the opportunity to flex demand to pay only for what is required, provided that arrangements are suitably optimised to take advantage of this flexibility.

The National Cyber Security Centre (NCSC) provides a useful overview of the main cloud service and deployment models.[1] Illustrative pricing models for cloud services can be found in Appendix One of this guidance. Broadly speaking, cloud offerings can be thought of in two main categories.

- **Cloud services and software:** Pre-built software applications that are accessed over the internet, such as finance and human resources systems and productivity suites.
- **Cloud hosting and platforms:** Cloud-based components such as servers and platforms (infrastructure) that an organisation can use to build a customised service.

Moving to the cloud is often not straightforward. Appendix One contains a brief overview of dealing with legacy technology in the context of contemplating a move to cloud services.

What is government policy on cloud services?

Government encourages public sector organisations to adopt cloud solutions where they offer better quality of service or value for money. It has developed its policy since 2013, when it expressed an explicit preference for public cloud over other deployment models. This 'cloud first' policy was re-assessed in 2019 and, although the policy remains "consider using public cloud solutions first" it is acknowledged that cloud solutions may not be right in all situations.

Government guidance continues to evolve, and organisations should ensure they are aware of the latest developments published in the *Cloud guide for the public sector*.[2]

[1] National Cyber Security Centre, Cloud security guidance: Service and deployment models, accessed 18 July 2024.

[2] Central Digital and Data Office and Government Commercial Function, Cloud guide for the public sector, accessed 18 July 2024.

Strategic assessment of cloud services

What does this section cover?

This section covers strategic choices for both first-time adoption and ongoing evaluation of cloud services as part of organisational and digital strategies, the business case process, due diligence assessments and lock-in and exit considerations.

Why is this important?

Management should set clear criteria for success so that it can properly evaluate the options available. Organisations need to strategically evaluate what is most suitable for their needs and keep this under review as the cloud market continues to evolve and mature. This includes issues related to supplier lock-in and related exit strategies from cloud service providers.

Strategic assessment of cloud services

1 Digital strategy

A successful digital strategy should be central to the wider organisational vision and strategy, taking due account of government's aim to move towards a more streamlined and consistent set of services over time. Management should guard against technology-led decision making. It should first develop robust organisational and digital strategies that meet the business need, and then establish a clear view of technological requirements to support the needs of the business. Smaller bodies may find it beneficial to engage external expertise to help them understand and navigate the various options.

Question	Further points to consider		
Are the priorities for the digital strategy set out?	● Does it start with the organisation's needs, rather than being retrofitted to a high-level arbitrary decision to use a particular technology?	● Does it align with wider cross-government initiatives, such as any moves to standardise on specific technologies or platforms?	● Is it being actively maintained and kept relevant to reflect both changing organisational needs and the evolution of technology and cloud services?
Does the cloud strategy have an appropriate range of input?	● Does it address commercial aspects, such as planning, negotiating and managing contractual relationships? ● Does it address resourcing aspects such as recruitment, skills and development, both for an initial migration and for maintaining and optimising cloud services thereafter?	● Does it include provision for upskilling teams where a multi-cloud or hybrid approach is being taken? ● Does it envisage establishing a centre of excellence that combines technical and commercial knowledge?	● Does it reflect other essential aspects, such as the organisation's needs for resilience and business continuity? ● While thinking about moving to the cloud, has the business considered all aspects of the service end-to-end to determine how to implement the cloud-based service in a smarter, more secure and cost efficient manner, rather than just 'lifting and shifting' the existing service?
Have technical requirements been articulated?	● Has the organisation considered the most appropriate type of service and deployment model for each of its main activities? ● Have technical lock-in considerations been factored into thinking around requirements?	● Has integration between cloud hosting and customer 'on premise' environments been evaluated and planned for?	● Will connectivity be sufficiently fast and resilient for all users and locations from which cloud services will be accessed, especially with hybrid working?
Have any specific features or legislative requirements been considered and identified?	● Are issues of both data sovereignty (UK-only data hosting) and data separation (isolation of organisation-held data to avoid its exposure to other customers) fully understood?	● As suppliers increasingly incorporate new technologies such as artificial intelligence (AI) into their products and services, are the risks and benefits fully understood, including whether the organisation's data might be accessed and used for AI training?	● Does the provider offer opt-outs from the incorporation of new features, such as AI, or does the customer have no such choice?
Is there a strategy for dealing with legacy?	● Has a plan for handling legacy systems been agreed?	● Has the organisation thoroughly investigated the challenges involved in migration and configuration, such as moving a bespoke system onto a shared platform?	● Where legacy or unsupported technology is to remain on-premises or move to alternative hosting (such as Crown Hosting), has consideration been given to how it will connect and interact with services moving to the cloud?
Will best practice be followed in respect of security?	● Has the organisation set out how assurance will be gained in respect of the NCSC's 14 cloud security principles (see Appendix Two)?	● Is there an in-depth plan for how cloud services will interface securely with existing services, systems and processes?	

Strategic assessment of cloud services

2 Business case

Cloud service providers advertise a range of potential benefits. These include cost efficiencies, adaptability, scalability, and security. However, the cost of cloud services can vary significantly depending on uncertain factors like user numbers and data volumes, as well as currency exchange fluctuations. Different suppliers have different elements to their pricing. Some features may not be included in base level services, and upgrade costs to obtain such features need to be fully understood. The benefits of adaptability and flexibility depend on the complexity of implementation and the extent to which services are provided 'as is' or need to be tailored. The advantages of cloud technology can be significant enough to justify the extra effort needed for accurate forecasting. However, the skills to implement cloud services are different from those required to implement and maintain more traditional on-premises or outsourcing arrangements. Moving from a single prime supplier to an environment involving multiple suppliers will call for a service integration and management skillset, which must be developed and maintained. Users will need to adapt to a culture of more frequent changes and improvement to the systems they work with, and not feel threatened by it.

Question	Further points to consider		
Have costing models been considered to an appropriate level of detail?	● Have the different pricing models (pre-committing to guaranteed availability levels, pay as you go, excess capacity arrangements, etc.) been considered? ● Are the implications of the move towards revenue expenditure rather than capital expenditure properly understood and reflected in the business case and budget profile?	● Is there clarity about which options and features are included with the different levels on offer? (For example, some basic plans may not offer the same security features as higher tier plans). ● Is the frequency and volume of data storage, access and extraction understood in order to model and understand ongoing cost implications and avoid unexpected charges?	● Does this include copying or extracting data from the cloud provider to alternative (provider independent) storage or between cloud providers (known as "data egress")? ● Is the contractual basis for potential future increases in cloud provider charges understood, including those caused by currency exchange fluctuations, and the impact they could have on anticipated costs/benefits?
Have planned costs been subject to suitable scenario testing?	● Does the organisation have a clear understanding of current service usage and how this is changing, or might change in the future? ● Has the organisation considered whether everyone needs the same licence, or are higher tiers and associated functionality only required by a subset of 'power' users?	● Has the organisation factored in any pan-government volume discounts that may be available? ● Has it analysed the baseline (fixed) and potential variable costs in each of the different options and bundled packages? Does the expected usage include development and test environments as well as live services?	● Has the organisation considered the costs of a multi-zone architecture for resilience, from both a technical and commercial perspective? ● For multi-cloud deployments, has the organisation considered in detail the relative costs and benefits of running workloads on different services, considering the impact of committed spend discounts?
Will extra skills and capacity be needed?	● Can the in-house team manage business case development, commercial negotiation, implementation, operations and assurance?	● If consultants or contractors are required to implement systems, will in-house staff be able to build knowledge and capability alongside them (knowledge transfer)?	● Has the organisation considered the use of mixed skills teams for new functions such as cloud cost optimisation? ● What is the wider impact on the workforce and the cost of training and roll-out?
Has an appropriate time horizon been considered in the commercial model?	● Has management ensured the inclusion of break clauses to prevent lock-in?	● If implementation costs are high with highly tailored services, has management considered how this might weaken the negotiating position when the contracted term approaches expiry?	● Has an assessment been made of the longer-term costs of such tailoring, and would a more standard implementation be a better option?

Strategic assessment of cloud services

3 Due diligence

There is a wide variety of cloud service providers, and many are global suppliers. The providers on G-Cloud are pre-screened **only** to check they are suitable to work with government, and not to provide assurance on their specific services. Selection criteria should, therefore, cover the specific needs of the organisation. The organisation should conduct due diligence on shortlisted suppliers to check they meet all security requirements, relevant standards, regulations, and business-specific needs. It should continue to perform periodic due diligence once a service is implemented. Organisations have a responsibility both to ensure security **'of'** the cloud (provider responsibility) and security **'in'** the cloud (customer responsibility).

Organisations not only need to gain assurance over cloud providers but also their own organisation's security and associated accreditations, and to ensure nothing can 'fall between the gaps' due to a misunderstanding of their own responsibilities relative to those of their cloud providers.

Organisations should be clear that they are responsible for the security of their own data in the cloud. The supplier may provide a secure technical environment but identifying and addressing data breaches remains the responsibility of the client organisation. It is not sufficient to be a passive consumer of cloud services.

Question	Further points to consider		
Will there be clear accountability between the organisation and the cloud provider?	● What oversight regime will the organisation have in regard to the cloud provider?	● Does the cloud provider subcontract and, if so, how does it manage risks?	● Has the organisation undertaken sufficient due diligence? Will it mitigate the risk that, in the event of a data breach, it will be held liable as the data controller alongside the cloud provider as the data processor?
Have the service features being promoted by the provider been verified?	● Has the organisation obtained views from other customers on how easy it is to configure and use the cloud service?	● How easily will the new service integrate with other systems?	● Are some features listed as 'beta', meaning they could potentially be modified or withdrawn with little or no notice?
Are the terms of service well understood?	● Is there scope for negotiation to meet organisation-specific needs, or are the terms of service provided 'as is' and therefore non-negotiable? ● Does the organisation have access to guidance and expertise on how to obtain the best out of terms that are negotiable? ● Are the capacity and availability guaranteed by the cloud provider sufficient for the organisation's needs?	● Does the organisation understand that negotiating an improved service level agreement (SLA) does not improve resilience if the solution is not engineered in a meaningfully different way to achieve that resilience? ● Are the SLA and business continuity arrangements fully understood, including how quickly service is guaranteed to resume after an outage?	● Does the service come with inbuilt backup options, or are these paid extras? Would a third-party backup solution provide a better fit for the organisation? ● Does the organisation understand the provider's liability cap (particularly for smaller contracts) and the extent to which it is sufficient to cover the cost of any damage the organisation may suffer?
Is there clarity regarding where the provider's infrastructure is physically situated, and in what jurisdiction(s) the organisation's data is being held and accessed?	● What assurances and guarantees are there on data residency and sovereignty? ● Are security or sovereignty constraints imposed by a parent department or other important stakeholders? (Cloud services are generally organised by region and not every service is necessarily available in every region.)	● If the provider has a UK data centre, what assurances does the organisation have that it will be used for the organisation's own data, and/or covers all services that the organisation plans to use? Will this incur additional cost?	● Will UK resident data be accessed from offshore locations?

Strategic assessment of cloud services

3 Due diligence *continued*

Question	Further points to consider		
Will the cloud service contract be governed by the law, and subject to the jurisdiction, of the UK?	● Where is the service hosted and where is data stored? ● Does data flow across borders and therefore into different jurisdictions?	● How does the provider support compliance with data protection legislation? ● Does the service rely on other third parties or 'sub-processors' and who therefore represent a supply chain risk?	● Will they support requests such as subject access requests under the Data Protection Act 2018?
Does the provider have appropriate security accreditation and protocols?	● What information security standards does the provider meet?	● What measures are there to ensure strong security, including preventing unauthorised access? Are these measures part of the base licence, are they additional paid-for options, or are they left to the organisation to implement separately?	● What is the provider's approach to proactive testing, and is there historical evidence of how they have responded to security issues?
Is there an understanding of what assurances are available from the provider?	● Do they cover all areas identified by the organisation as important (such as the NCSC's 14 cloud security principles)? (See Appendix Two)	● Are assurances based on self-certification or are independent validation reports available? (See Appendices Two and Three for further information)	
Does the organisation understand what security information will be supplied by the provider as part of the service?	● Does the provider undergo regular, independent assurance activities (such as penetration tests, external audits, Service Organisation Controls reports etc – see Appendix Three) and make the results readily available to customers? ● Does the contract exclude any rights of access and audit?	● Does the service provide sufficient logs or alerts to support how the organisation detects and responds to security incidents? ● Are there sufficient in-house resources to understand and interpret the information and alerts being fed back in a timely and responsive way?	● Does the provider operate their own security functions with whom the organisation can collaborate when investigating security incidents or seeking assurance? ● Does the organisation regularly validate its own security through penetration tests, external audits, etc, to provide independent assurance and to flag/fix any issues identified, both internal and related to its external providers?

Strategic assessment of cloud services

4 Lock-in and exit strategy

Lock-in arises where an organisation depends heavily on products and services from a particular supplier. It can also arise where an organisation uses more than one cloud provider but depends on each for a specific service. Switching to a different technology or provider can be difficult, time-consuming and expensive. There are two main types of lock-in.

- **Commercial:** Long and inflexible contracts can prevent organisations from changing their technology strategy when circumstances change. Commercial lock-in is to be avoided. Government advice is that it can be reduced by agreeing shorter contracts, with organisations ensuring that they retain the intellectual property of their products and services as well as access rights to their data. However, shorter contracts can bring their own problems. Organisations will have to run procurement and evaluation exercises more frequently. Vendors may be less inclined to offer incentives than they would be for a longer-term relationship.

- **Technical:** While there may be no commercial barriers to moving from one provider to another (for instance, an organisation is approaching the end of its contracted term or is on a pay-as-you-go pricing model), doing so may represent a significant technical and cost challenge. Technical lock-in cannot be avoided entirely, and trying to do so at all costs has its own downsides. Deep integration with a specific cloud provider's service may provide significant technical or business benefits, but may simultaneously increase the risk of technical lock-in. If an organisation only uses cloud providers in such a way as to be able to migrate off them again easily, this can severely restrict the features and functionality it is able to use. Doing so could compromise the value of moving to the cloud. In most cases a trade-off is involved, and each organisation needs to determine its own approach and judge the degree of lock-in it is willing to accept. Organisations should explore ways to mitigate technical lock-in risks by using approaches such as open standards.

An exit strategy is one of the most important components of a cloud strategy, even if it is never called upon. It should weigh the impact of changing provider against the benefits of staying. Organisations may find it useful to be in a position where they can give an indication of the costs and timescales for exiting from each of their cloud providers, the specific circumstances which might give rise to the need to do so, and the most probable potential alternative solutions. Estimates of time, effort and cost should include other aspects of lock-in, such as skills and capability. Strategies should consider the merits and drawbacks of different timeframes, for instance, a two-year planned exit versus an emergency exit. It is also advisable for such a strategy to be developed in conjunction with a third party expert rather than the provider of the service.

The Cabinet Office is placing an increased emphasis on exit planning as part of the One Government Cloud Strategy.

Strategic assessment of cloud services

4 Lock-in and exit strategy *continued*

Question	Further points to consider		
Has the organisation addressed technical lock-in considerations?	● Does the strategy set expectations for how the trade-offs between value and portability will be assessed for each cloud service to determine the degree of lock-in considered acceptable? (The Central Digital & Data Office (CDDO) advises that many, although not all, of the cloud services that provide the most value are also the least portable.)	● Has the organisation set baseline expectations for what a disproportionately large switching cost might be for each service and overall collection of services with a particular provider?	
Has the organisation considered cloud concentration risk?	● Have alternative cloud providers been considered? ● Are the advantages and disadvantages of multi-cloud versus single-provider provision fully understood?	● Is there a clear articulation of the benefits of using a single provider where this is judged to outweigh concentration risk? ● Have the risks of cloud provider errors or failures been modelled and mitigated?	● Is the cloud service optimised to meet the organisation's required levels of resilience? ● Has the Cabinet Office been consulted, especially where services form part of the Critical National Infrastructure?
Is there a well-defined approach to data access and retrieval?	● Has the organisation undertaken an assessment of the costs and barriers to retrieving its data in a format suitable for migration to another service? (The degree of effort and expense to move to a new provider should not be underestimated, and the risk is most acute with software as a service.)	● Are there contractual mechanisms to ensure the provider will supply the organisation's data in an agreed electronic format for alternative back-up arrangements, or migration to another provider?	● Are the actual mechanics of how the data will be extracted sufficiently clear from the outset (particularly in the case of short contract lengths)?
Is there an exit strategy?	● Have issues of potential lock-in as a consequence of deep integration with the native capabilities of a specific provider been considered? What impact would exiting have on the skills required when moving from one cloud provider's technology to another? ● Is there a good analysis and understanding of the trade-offs between regulatory, commercial and technical considerations of exiting from one cloud provider to another? And is there a more detailed exit plan that assesses the specific steps needed to exit, the risks to be mitigated, the time it would take and how it would be managed on an orderly service-by-service basis?	● Has a plan been developed for exiting from the cloud, whether to another cloud provider, on-premises, or just discontinuation of the service? Is it costed and validated so it can stand the test of time? ● If the plan is to switch to an alternative provider, has an assessment been made of the need to operate multiple cloud services in parallel, with a period of dual running, while the migration takes place? ● How mature are the standards, tools and techniques involved in moving services from one cloud provider to another?	● What experience does the organisation have internally with managing a migration from one provider to another? ● Will such a migration ensure that the organisation can continue to meet its obligations under the Public Records Act to preserve and make records available?

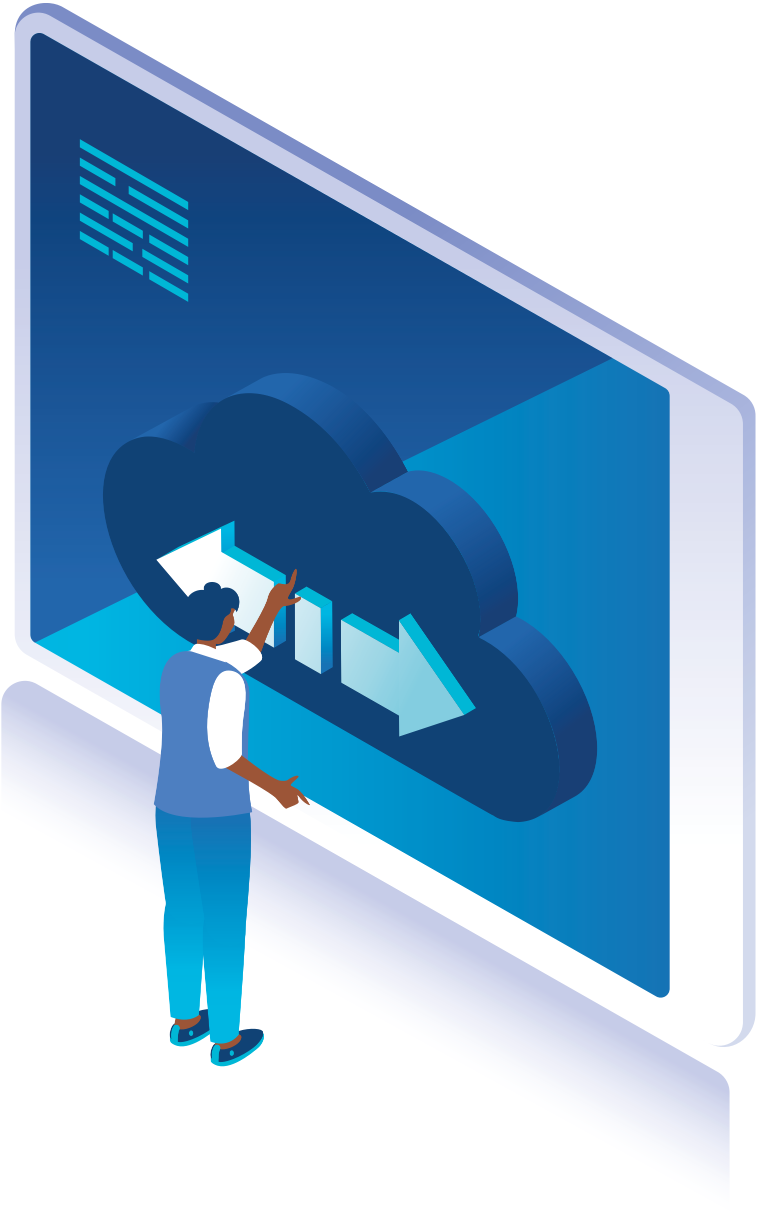
Implementation of cloud services

What does this section cover?

This section focuses primarily on utilising cloud components such as platform infrastructure to develop and deploy a customised service. Some elements discussed here will also apply to the consumption of pre-built cloud. There is a notable difference between the issues involved with these two approaches.

Why is this important?

Management needs to address the risks associated with cloud service implementation. Failing to configure and utilise cloud services correctly can severely hamper the achievement of financial benefits and expose organisations to the risk of a data breach. When organisations are moving from one cloud provider to another, or from on-premises to cloud for the first-time, issues to be considered include system configuration, data migration, service risk and security. Most of the challenges in implementing cloud services are common to on-premises systems. The broader challenges of change management and stakeholder engagement also apply to the introduction and use of cloud systems. However, cloud services and providers can vary in their levels of maturity and the configuration of systems can be complex. Organisations should consider their approach to multi-cloud solutions and whether alternative cloud providers will be considered only at initial implementation or for all new needs. They should assess the initial and ongoing impact of multi-cloud implementation on the costs, capabilities and resources required.



Implementation of cloud services

1 System configuration

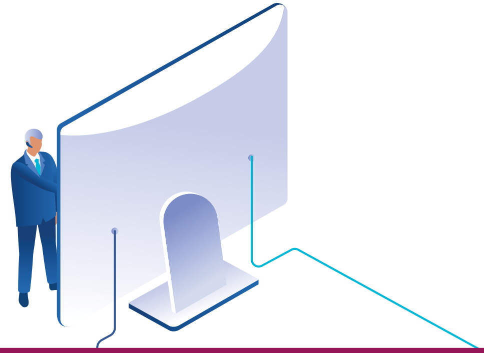
Outside of the use of pre-built cloud applications, such as productivity or finance software operating in a user's browser, the potential variation and continuous innovation in the cloud environment can make configuration more challenging than for an on-premises network. Correct configuration is essential for a hybrid arrangement of cloud and legacy systems to inter-operate and communicate efficiently and securely. Smaller organisations are less likely to have sufficient expertise and capacity to manage the configuration of new systems. Such organisations will need a robust plan in place to manage business as usual at the same time as managing the change while drawing on external help.

Question	Further points to consider		
Is there a strong governance and project management plan in place?	● Is there an identified owner of the implementation process? ● What commitment is there from the provider to work collaboratively on systems configuration?	● Is there a full range of senior representatives from across the relevant areas of the organisation involved in programme governance?	● Is it clear which roles and responsibilities the organisation has and which roles and responsibilities the provider has?
Have infrastructure, applications and data been prepared for the move?	● If legacy data is poor quality, should it be transferred in its existing state into the new system, or cleansed and improved first?	● Are other systems sufficiently up to date to integrate with the new cloud service?	
Is the organisation following configuration best practice?	● Is the move to the cloud being clearly documented to ensure that any changes, for example, in data categories or business processes, are understood?	● Has pre-implementation testing been completed and documented prior to go-live?	● Are configurations and customisations fully documented in a way that can be understood by someone not involved in the original implementation?
Is the organisation overly reliant on third-party resource?	● Is there sufficient continuity in the in-house team to maintain a robust corporate memory?	● Will the post-implementation in-house team understand how the system has been configured?	● Is there documented guidance in place?

Implementation of cloud services

2 Risk and security

The cloud is not necessarily any more or less secure than on-premises technical architecture. The threats in an on-premises and a public cloud environment are broadly similar. Organisations must take responsibility and accountability for ensuring that data is appropriately secured and not left open to a wider audience than intended.

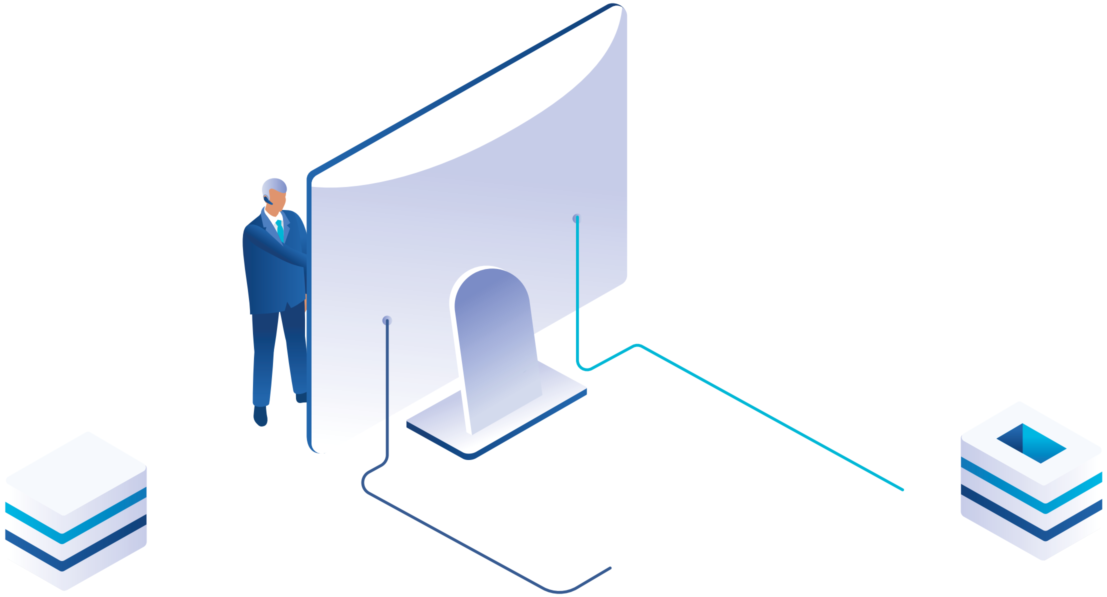


Question	Further points to consider		
Are technical risks covered with clear responsibilities and mitigating actions?	• Has the organisation put an agreement and action plan in place to cover risks such as resource exhaustion, isolation failure, threats from insiders, interface compromise, data interception, data leakage, insecure data deletion, denial of service (DoS) attacks, ransomware, and loss of encryption keys?	• Are key personnel aware of the steps they need to take in the event of different kinds of security breach?	• Have these steps been practised?
Does the organisation have the capacity and capability to analyse security data made available by the cloud provider?	• Is it clear who in the organisation is responsible for reviewing this data and the timeframe within which they should do so? • Do they know how to act on any warnings and alerts contained within the data?	• Are lines of responsibility between digital services/IT teams and information security teams clear? • Have the costs of obtaining any additional skills needed been considered?	• Has the organisation assessed the reputational risk of a data breach arising from a failure to act on warning signs that should have been heeded?
Are the required legal and policy agreements in place?	• Do contracts cover data protection risks, licensing risks and changes of jurisdiction?	• Are the software licensing implications fully understood?	• Are there policies in place to cover key vulnerabilities such as vendor lock-in, governance, compliance, and reputational risks, or supply chain failures?
Have business continuity plans been updated?	• Is the organisation prepared for a range of scenarios for service outage?	• How frequently will plans be tested to ensure they work and to apply any lessons learned?	• Has the organisation considered resilience requirements in case of a failure in one zone/region of the cloud provider and the option to shift to another zone/region?
Are plans in place to cover the event of data loss?	• Is key data covered by a system of point-in-time backups or restore points? • Are the provider's backup arrangements sufficient, or are third-party solutions required?	• Are data backups maintained in a safe location outside of the cloud provider's services to guard against unforeseen failures, and to mitigate risks such as ransomware attacks? • Are there plans in place to support ongoing business operations in the event of data being lost or compromised?	• Are data backups and service continuity or recovery arrangements regularly tested? • Have clear lines of responsibility, management and communication been established for handling the impact of data loss or a data breach?

Implementation of cloud services

2 Risk and security *continued*

Question	Further points to consider		
Are financial controls fully tested and compliant with best practice?	● Particularly for financial software as a service, does the organisation thoroughly understand all the configuration options, and in particular what automated controls can be enabled within the system?	● Has strong segregation of duties been established within the system?	● How robust is identity management and assurance to ensure that financial controls are not undermined?
Have privileged accounts been secured?	● Are administrator and service accounts (that is, accounts used by the system itself rather than individuals) secured appropriately?	● Are privileged accounts properly managed and monitored to avoid the granting of excessive permissions, or granting of power to a single account without adequate governance and technical controls?	● Have service accounts been checked to ensure they do not inadvertently have greater permissions than required, for instance, the ability to delete an entire database when all that is needed is permission to read and write?



Implementation of cloud services

3 Implementation

The realisation of benefits from new software can depend on the acceptance, compliance and engagement of users. Cloud systems often involve significant and more frequent changes to the user interface. While these changes may appear intuitive to technical colleagues, they may not work for everyone. In addition to managing technical implementation, organisations must focus on the importance of change management for all key stakeholders and users.

Question	Further points to consider		
Have key stakeholders been engaged through a comprehensive change management strategy?	● Does the organisation have adequate plans to provide training, on-going support, and coaching for users before, during and after implementation, appropriate for the service(s) chosen?	● Does the implementation programme have an effective governance structure to prioritise the backlog of requirements?	
Are contingency plans in place to manage implementation issues?	● If the organisation is relying on third parties, will it have sufficient control over them?	● Do the organisation's existing systems represent a "burning platform" and would they be able to continue indefinitely until implementation issues are resolved?	
Are there adequate plans for technical and user acceptance testing?	● Has the organisation identified all relevant business scenarios for inclusion in testing, and defined thresholds for acceptable deviations or other issues with acceptance?	● Has testing been completed, and does it demonstrate that users are able to complete all required tasks without encountering system errors?	● Have non-functional requirements, such as the need to operate under high levels of user demand to an acceptable level of performance, been fully tested?

Management and optimisation of cloud services

What does this section cover?

This section covers operational considerations, the need for assurance from in-house teams and third parties (reflecting the shared responsibility model), the capabilities needed to manage live running, and how to continue to control ongoing costs.

Why is this important?

A move to cloud services has an impact on the skills and resources required in-house to manage live services. Cloud service providers can usually take care of infrastructure management and maintenance. However, this is unlikely to apply if a legacy system has been 'lifted and shifted' into the cloud, with software patches and updates involved at various system levels. In such a case, responsibility remains with the organisation. Cloud providers can also offer a helpdesk and support to users and technical staff depending on the service procured. However, new capability is required to understand, manage and interpret the interface between the cloud service and the organisation. Organisations cannot outsource responsibility for governance of data and controls over financial and other transactions, nor for data security. This includes the interpretation of monitoring information and alerts from the cloud provider. Many organisations also opt to modify the services they use. This can increase the ongoing need for in-house service management, particularly as cloud providers routinely release system updates.

Management and optimisation of cloud services

1 Operations

Immediately after implementation there may be a 'teething' period as it takes time for the requirements backlog to be addressed. Ongoing change management will be important through this period to assure users and to signpost any further changes to system interfaces or configuration. It is important for strong governance to be in place over the cloud provider and the in-house team. Thereafter the cloud environment is likely to be more dynamic, with a greater frequency and volume of changes and updates compared to an on-premises environment. The organisation will have less control over the acceptance of these updates, particularly with software as a service.

Question	Further points to consider		
Is there effective governance to prioritise the removal of any temporary workarounds?	● Are the priorities clear, shared and bought into by all concerned?	● Are there any integration issues still outstanding that expose security weaknesses?	● Is information being manually exported to other systems and are there plans to automate this?
Is there clear oversight over what the cloud providers are planning?	● Is the cloud provider being transparent over their plans to release new features and upgrades to their systems?	● Is the organisation able to influence the cloud provider to prioritise the developments they would value, or the retention of features they would not wish to see discontinued?	● Is the organisation assessing the impact of planned changes on the business, including whether the original business case benefits continue to be achieved?
Are arrangements clear for system changes, upgrades and patches?	● Does the in-house team have the capacity and expertise to manage any changes they will be required to make?	● Will the team have sufficient time to test any changes in a 'sandbox' before being required to release them into the live service?	● Will the team be able to prevent new features, such as artificial intelligence (AI), being deployed by a cloud provider until they have had time to assess their technical, security and legal implications?
Is there sufficient capability to take advantage of the reporting functionality?	● Will the in-house team continue to be dependent on third-party support to manage key reporting and system processes?	● Have relevant logging and auditing functions been turned on to provide tracking information?	● Does the team have the expertise to interpret and act on the data?
Is the organisation monitoring its usage of the cloud to confirm that it is getting the best value?	● Does this monitoring include the development environment as well as live services? ● Does it ensure that new cloud instances and services are only set up where there is a necessary business requirement?	● Are they being set up in the most efficient way, and shut down again when the business need has been satisfied?	● Is there a regular review to ensure that the pricing model continues to be the best fit for the organisation's needs? ● Is the organisation taking advantage of any available free optimisation advice and solutions from the cloud provider?

Management and optimisation of cloud services

2 Assurance

Cloud providers typically offer assurance to their customers in the form of Service Organisation Controls (SOC) reports (see Appendix Three). Cloud providers commission independent auditors to write these reports to provide assurance on their processes and security arrangements. Management needs clarity on the assurance that these reports provide and where there may be controls gaps or areas where further assurance is needed. External auditors will also wish to have sight of these reports as part of the annual audit where they relate to cloud services supporting key systems and processes.

Question	Further points to consider		
Does management understand the general scope and limitations of the different types of SOC reports?	● Is assurance required to cover financial reporting (SOC1) or wider operational controls (SOC2)? Is a publishable public-facing report (SOC3) needed?	● Do available reports provide an assessment of both cloud provider(s) and the organisation itself (to reflect the shared responsibility model and ensure no potential gaps between areas of assurance and accountability)?	
Is management clear on the scope of controls tested, the extent of testing and the assurance given?	● Is the service auditor a recognised firm? ● What additional controls or assurance are needed to cover internal processes and systems?	● If there are weaknesses or gaps in the cloud provider's controls, are there additional steps that management should take to strengthen internal controls?	● Does management need to obtain further assurance on the overall operating model?
Do SOC reports give assurance on the success of operational controls over time?	● Are SOC2 reports available which test the controls over time rather than simply documenting them?	● Does management have a way of monitoring any changes in key controls between reports?	
Are SOC reports frequent enough to keep pace with continuous improvement?	● Is there a mechanism in place to allow management to continuously monitor compliance with key controls?	● Is there a trigger clause to oblige the cloud provider to obtain a new report if it makes significant changes to its systems or controls?	
Does management carefully scrutinise SOC report findings?	● Even if the report gives an 'unqualified opinion', are there any exceptions noted? ● What is the quality of the cloud provider's responses to any exceptions raised?	● Does management acknowledge that, while the organisation may outsource procedures or services, it cannot outsource responsibility for the control environment, and that outsourcing extends the scope of management's responsibilities for gaining assurance over data, transactions and controls operated on their behalf by others?	● How has the organisation checked it has not accidentally exposed document storage to unintended public access?

Management and optimisation of cloud services

3 Capability

Moving functionality into cloud systems does not necessarily mean that there will be any significant efficiencies, and organisations may need more investment in terms of in-house capability. Simple cloud applications may make little difference to capability requirements. However, more complex integration work will need significant upfront resource to configure and implement, with a long tail thereafter to manage ongoing system improvements and updates. Integrating several different cloud services at the same time can be particularly challenging.

Question	Further points to consider		
Will the organisation retain the necessary technical knowledge post-implementation?	● What ongoing knowledge will there be of any legacy systems and how they interface with new cloud systems? ● What plans are there for knowledge transfer from the cloud provider pre- and post-migration?	● How is knowledge sharing operating with the cloud provider? ● Will documentation be routinely maintained and provided to track configuration changes and customisations?	● Is there a learning plan to keep users and administrators up to date with changes and developments?
Does the technical team have the capability to take full advantage of the cloud systems?	● Is specific training arranged for different cloud provider systems (which may have widely varied data structures and technical requirements)?	● Do teams responsible for legacy systems (such as business intelligence reporting, third-party payroll, or fixed asset modules) have the capability to manage the interfaces with the cloud system?	
Will there be sufficient capability to manage updates, downtime, and system changes?	● Will the organisation retain people who understand the cloud system configuration and can manage changes and continuous improvement?	● Will the technical team be able to effectively monitor planned cloud system updates and understand the organisational impacts?	
Will there be sufficient commercial and legal capacity to challenge on value for money and compliance?	● Is there a thorough understanding of providers' pricing structures, including across areas such as compute, storage and retrieval, and data egress (transfer out) as well as the way services may be bundled or tied together?	● Will the commercial team have sight of the usage of cloud systems through monitoring tools? ● Will they be able to understand and interrogate the cost drivers to ensure ongoing value for money?	● Will there be legal capacity to support the technical team if there are breaches of service level agreements (SLAs)?
Is there sufficient base-level stakeholder capability to optimise cloud system usage?	● Are system users taking advantage of the opportunities and features available?	● Is there a training plan in place to keep users up to speed with changes and induct new users?	● Do decision-makers have sufficient understanding of cloud capabilities to engage effectively?
Does the organisation have access to skills and knowledge of a broad range of technical solutions?	● Is this sufficient to maintain a perspective of the cloud market and of technologies becoming available?	● Is external capability needed to support and/or train up internal resources?	● Will recruitment and training cover more general cloud skills as well as specific cloud platforms?

Appendix One

Cloud services – pricing models and legacy systems

Pricing models for cloud services

Cloud services have different pricing models to reflect the degree of certainty or flexibility organisations require or are willing to accept. Cloud providers can offer a variety of models, including one or more combinations of per-user pricing (with charges based on the number of users), tiered pricing (which offers a range of bundled packages with varying functionality), feature-based pricing (based on specific features or modules), pay as you go, freemium (where a basic version is available free with charges for premium features), flat pricing/subscription (with fixed monthly or annual fees), and free (free access with advertising).

To get the best value out of cloud hosting/platforms (as opposed to the consumption of pre-built cloud application services), organisations should understand their requirements and select the model or combination of models which has the best fit with their needs.[3] These include the following.

- **Reserved instance:** Organisations pay for guaranteed access to a defined level of capacity for a set period of time, whether or not they actually use it. This model is best suited to services that are stable and need to run continuously. It can be inefficient where usage is variable or unpredictable, as the lack of flexibility in this model commits an organisation to a level of spend that it cannot reduce. It can be combined with on-demand for handling peak loads.
- **On-demand:** A 'pay as you go' option that charges for capacity as and when an organisation needs to use it, such as to support peaks in workload. It gives organisations the flexibility to start and stop using cloud resources without early termination fees or long-term commitment. To get the best value from this model, it is important for organisations to manage their usage diligently, for example, by not using capacity unnecessarily and by shutting down capacity that is no longer required.
- **Spot instance:** Cloud providers offer high discounts for the use of otherwise idle capacity in exchange for customers accepting that it may be taken away at very short notice (in some cases, less than a minute) if needed by another customer. This option best suits activities that are not critical or time-sensitive and can be paused (for example, development environments). It is not well suited to services that need to run continuously.

Legacy systems

Across the whole of government, ageing IT systems are a key source of inefficiency and create a major constraint to improving and modernising government services. These ageing systems are commonly referred to as 'legacy'. However, it would not provide value for money to constantly replace all systems whenever a new need or a more effective technology is identified. Well-managed legacy systems deliver continuity of service, and there are circumstances where the lives of such systems can safely be extended. By 'well-managed', we mean that the system has been kept up to date and is still supported by the relevant vendors, and there are no significant security or data protection issues that need to be addressed. Having a cloud strategy does not equate to moving everything into the cloud indiscriminately. The Central Digital & Data Office (CDDO) *Guidance on the Legacy IT Risk Assessment Framework* sets out how organisations should assess their legacy technology.[4]

[3] According to the Cabinet Office, selecting the most appropriate approach for an organisation's circumstances could yield discounts of between 60% and 80%.

[4] Central Digital and Data Office, Guidance on the Legacy IT Risk Assessment Framework, accessed 18 July 2024.

Appendix One

There are various options for dealing with legacy technology in the context of contemplating a move to cloud services. These options, which include the following, should be considered on a system-by-system basis rather than as a strict policy for all legacy technology.

- **Retain (do nothing):** Where the system is not cloud-compatible but is otherwise working well and there is no strong business case for the cost and disruption of moving to an alternative.
- **Retire:** Where the system's functions are either no longer required or can be incorporated into other applications.
- **Repurchase ('shop and drop'):** Decommissioning the existing application and replacing it with its equivalent cloud-based version. In effect it is a change in licensing arrangements alongside the work required to move the service into the cloud.
- **Rehost ('lift and shift'):** Moving the application from on-premises to the cloud with no or only minimal modification to adapt to the new environment. It means that the application is unlikely to be able to take advantage of cloud-specific features but may be the only feasible option where organisations do not have the ability to make the necessary changes themselves. This may be the case for commercial off-the-shelf applications or customised applications built using proprietary technology that imposes constraints. This option is sometimes called 'moving without improving'.
- **Replatform ('lift and shape'):** Modifying and optimising the application for moving to the cloud, but not to the extent of significantly changing the core functions.
- **Refactor (rewrite):** This is the most complex option and involves a major overhaul of the application. It is very time-consuming and resource-intensive but offers the greatest opportunity for making extensive use of cloud capabilities.

The last four of these options will require the organisation to perform extensive testing to confirm the system operates satisfactorily in its new environment and that the migration has not introduced a lower quality of service. For example, while all expected functionalities may be present, the migrated system may run more slowly, or there could be an adverse impact on interfaces or other integrations such as robotic process automation. To compensate for this, an organisation may find it needs to pay the cloud provider for a higher level of performance or capability than the on-premises equivalent to stand still in terms of overall user experience.

Appendix Two

National Cyber Security Centre (NCSC) guidance

Working towards your cloud security – four steps

The NCSC advises an approach based on the following four steps. Working through these in order will help organisations identify cloud services that are suitably secure for their intended use.[5]

1 Know your business requirements.

2 Choose a cloud provider that meets your needs.

3 Use the cloud service securely.

4 Continue to monitor and manage the risks.

The NCSC outlines a lightweight approach to cloud security that sets out minimum expectations across data encryption, authentication and access control, security logging and incident management, and governance, but notes the full approach (as below) is still recommended for more sensitive systems.[6]

The 14 cloud security principles

The 14 security principles that NCSC recommends organisations should use are summarised as follows.[7]

1 **Data in transit protection:** User data transiting networks should be adequately protected against tampering and eavesdropping. This can be achieved through a combination of network protection, authentication and encryption.

2 **Asset protection and resilience:** User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure. Considerations include physical location, legal jurisdiction, data centre security, data encryption, data sanitisation, equipment disposal, and physical resilience and availability.

3 **Separation between customers:** A malicious or compromised customer of the service should not be able to affect the service or data of another customer. The factors affecting this include the deployment model (public, private or community cloud), service model (infrastructure, platform or software as a service), and the level of assurance available over the design, implementation and operating effectiveness of the cloud provider's separation controls.

4 **Governance framework:** The service provider should have a security governance framework that coordinates and directs its management of the service and information within it.

5 **Operational security:** The service needs to be operated and managed securely to impede, detect or prevent attacks. The elements to consider are configuration and change management, vulnerability management, protective monitoring and incident management.

6 **Personnel security:** Where service provider personnel have access to data and systems, the customer needs a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, can reduce the likelihood of accidental or malicious compromise by service provider personnel.

7 **Secure development:** Services should be designed and developed in a way that minimises and mitigates threats to their security.

8 **Supply chain security:** The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.

[5] National Cyber Security Centre, Cloud security guidance: Introduction to cloud security, accessed 18 July 2024.

[6] National Cyber Security Centre, Cloud security guidance: Lightweight approach to cloud security, accessed 18 July 2024.

[7] National Cyber Security Centre, Cloud security guidance: The cloud security principles, accessed 18 July 2024.

Appendix Two

9 **Secure user management:** The provider should make tools available for customers to securely manage their use of the service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of resources, applications and data. The key considerations are minimising permissions, a single and coherent access control mechanism, and time-bounded permissions.

10 **Identity and authentication:** All access to service interfaces should be restricted to authenticated and authorised individuals. Authentication should take place over secure channels and employ strong methods such as two-factor authentication, certificates or secure federated identity. User names and passwords alone are weak and susceptible to compromise.

11 **External interface protection:** All external or less trusted interfaces of the service should be identified and appropriately defended. Services that accept connections over the internet from any worldwide location are more exposed to attack.

12 **Secure service administration:** Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data. Customers should understand how the service provider is managing the service.

13 **Audit information and alerting for customers:** Customers should be provided with the audit records needed to monitor access to their service and the data held within it. The type of audit information available will have a direct impact on a customer's ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

14 **Secure use of the service:** The security of cloud services and the data held within them can be undermined if customers use the service poorly. Consequently, customers will have certain responsibilities when using the service in order for their data to be adequately protected, for example, implementing the required services to interpret and act on data highlighting poor usage practices.

Appendix Three

Assurance arrangements: Service Organisation Controls (SOC) reports, Cyber Essentials and ISO 27001

Assurance over cloud providers can vary from self-certifications through to reports prepared by certified, independent assessors.

Where assurance is provided, typically this is in the form of SOC reports.[8] Cloud providers commission independent auditors to write these reports to provide assurance to customers on processes and security arrangements. There are three types.

- **SOC1:** The focus is on transaction processing and IT general controls relevant to financial reporting.
- **SOC2:** This covers wider operational controls over the IT environment and includes the auditor's test procedures and results.
- **SOC3:** A shorter version of the SOC2 report that is placed in the public domain but omits the detail of the test procedures undertaken.

Organisations should understand what assurances they are, and are not getting from such reports and other certifications such as Cyber Essentials or ISO 27001.[9,10] The level of assurance in practice may be less than might be assumed.

- Cyber Essentials focuses on simplicity of approach and aims to help a wide range of organisations assess and mitigate risks to their IT systems from the most common cyber security threats. Cyber Essentials relies on self-certification. While Cyber Essentials Plus is the externally assessed equivalent, it is not specifically targeted at any particular type of organisation and should not be regarded as a comprehensive audit of all technical controls operated by a cloud service provider.
- ISO 27001 is a management standard, rather than a security standard. While it provides an auditable framework for the management of information security, it does not provide a 'gold standard' for security, which, if implemented, would ensure the security of an organisation.

Organisations that fail to appreciate these considerations may in effect be outsourcing unknown levels of risk. In practice it can be difficult to get reports and assurances from cloud providers on a timely basis in order to hold them to account effectively. An approach may be needed that prioritises essential services. This is the approach adopted by GovAssure, which replaces the cyber security element of the Departmental Security Health Check (DSHC).[11] GovAssure was introduced in 2023 to support the aim set out in the *Government Cyber Security Strategy: 2022 to 2030* that all government organisations across the whole public sector should be resilient to known vulnerabilities and attack methods no later than 2030.

[8] The content is prescribed in International Standard on Assurance Engagements (ISAE) 3402: Assurance Reports on Controls at a Service Organization (accessed 18 July 2024), issued by the International Federation of Accountants. This standard has not been adopted formally by the Financial Reporting Council for the UK but can be drawn upon for best practice.

[9] National Cyber Security Centre, About Cyber Essentials, accessed 18 July 2024.

[10] International Organization for Standardization, ISO/IEC 27001:2022, accessed 18 July 2024.

[11] Government Security, GovAssure, accessed 18 July 2024.

Appendix Four

Other available guidance material

Our guidance on cloud is highly summarised and, as well as that from the National Cyber Security Centre (see Appendix Two), there are other complementary, more detailed guides on offer.

1 The Financial Conduct Authority (FCA) provides a guide for firms outsourcing to the cloud and other third-party IT services.[12] This guidance helps firms to oversee the lifecycle of their outsourcing arrangements. This ranges from making the decision to outsource, selecting an outsource provider, and monitoring outsourced activities on an ongoing basis, through to exit.

2 The Competition and Markets Authority (CMA) investigation of the supply of public cloud infrastructure services in the UK has published a competitive landscape working paper that highlights a range of issues relating to cloud services, from a review of the main providers to customer switching and use of multi-cloud.[13]

3 More specific guides and advice are available through subscription to research services such as Gartner.

[12] Financial Conduct Authority, FG16/5: Guidance for firms outsourcing to the 'cloud' and other third party IT services, accessed 18 July 2024.

[13] Competition & Markets Authority, Cloud services market investigation: Competitive landscape working paper, 23 May 2024, accessed 23 July 2024.