



National Audit Office

Digital and transformation

Guidance for audit committees on cloud services



APRIL 2021

We are the UK's independent public spending watchdog.

We support Parliament in holding government to account and we help improve public services through our high-quality audits.

The National Audit Office (NAO) scrutinises public spending for Parliament and is independent of government and the civil service. We help Parliament hold government to account and we use our insights to help people who manage and govern public bodies improve public services.

The Comptroller and Auditor General (C&AG), Gareth Davies, is an Officer of the House of Commons and leads the NAO. We audit the financial accounts of departments and other public bodies. We also examine and report on the value for money of how public money has been spent.

In 2019, the NAO's work led to a positive financial impact through reduced costs, improved service delivery, or other benefits to citizens, of £1.1 billion.

Contents



Foreword 4



Introduction 5



An overview of cloud services 10



Part One

Assessment of cloud services 16



Part Two

Implementation of cloud services 22



Part Three

Management and optimisation
of cloud services 26



Appendix One

National Cyber Security
Centre guidance 30



Appendix Two

Assurance arrangements:
Service Organisation Controls
(SOC) reports, Cyber Essentials
and ISO 27001 33

Links to external websites were valid at the time of publication of this report. The National Audit Office is not responsible for the future validity of the links.


This report can be found on the National Audit Office website at www.nao.org.uk


If you need a version of this report in an alternative format for accessibility reasons, or any of the figures in a different format, contact the NAO at enquiries@nao.org.uk

For further information about the National Audit Office please contact:

National Audit Office
Press Office
157-197 Buckingham Palace Road
Victoria
London
SW1W 9SP

 020 7798 7400

 www.nao.org.uk

 @NAOorguk



Foreword

In April 2019, we published the first version of our *Guidance for audit committees on cloud services*. Gaining appropriate assurance can be difficult and our aim is to help audit committees understand the kinds of questions they might ask of management where organisations are contemplating introducing or moving to cloud services.

Since we published that guide, we have seen more of the public sector turn to cloud services. Government spending with the major cloud providers has increased in the past five years. Our previous guidance was well received with a clear appetite from our stakeholders to keep it updated.

Government's digital and commercial functions also instigated a One Government Cloud Strategy, which resulted in additional guidance including the *Cloud Playbook* issued in March 2020.

This guidance has been updated to reflect the above and to recognise wider developments and evolution of cloud services more generally.



Introduction

1 The 'cloud' is a term for using the internet to access systems and data stored outside an organisation's own premises. Cloud can be thought of as an evolution of IT outsourcing as programs and data are held on physical IT equipment owned and managed by the cloud service provider.

2 Cloud introduces new financial and operating models which move away from capital costs 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 possibility to flex demand to only pay for what is required.

3 Public and private sector organisations are increasingly adopting cloud services with the aims of increasing efficiency and transforming their operations. Organisations may also be seeking to reduce costs. The One Government Cloud Strategy has an expectation that, in the long run, cloud services should produce lifetime cost savings. However, this is conditional on cloud services being designed and implemented correctly.

4 Detailed cloud guidance is available, as outlined below. Our guide provides a short summary and complements other resources by setting out specific questions for audit committees to consider when engaging with their management. Other related support for audit committees includes *Cyber security and information risk guidance for audit committees* and *Transformation guidance for audit committees*.

5 This guide aims to help audit committee members to ask informed questions at three stages:

- **Assessment of cloud services** – this section considers cloud services as part of organisational and digital strategies; the business case process; and due diligence.
- **Implementation of cloud services** – this section covers system configuration, data migration and service risk and security.
- **Management and optimisation of cloud services** – this section covers operational considerations, the need for assurance from third parties, and the capability needed to manage live running.

Why this requires attention

6 Government digital policy supports the move to cloud and the prevalence of cloud services continues to increase in both the public and private sectors. Some organisations may, however, lack the capacity and expertise to select the right services for their needs, implement them securely, and manage and optimise them effectively. In particular, the cost and effort of moving to cloud solutions and the investment needed in skill sets and processes required to manage and optimise them effectively should not be underestimated – particularly where multiple suppliers are involved. The skills required are not exclusively technical; additional commercial skills are likely to be needed within digital teams to understand and manage the cloud services the organisation has contracted for.

7 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 offer a level of security that would be economically or operationally difficult for many organisations to provide on their own. Cloud providers invest heavily in security, as otherwise their businesses are at risk. Nevertheless, customers should not assume that the cloud provider is taking care of all aspects of security on their behalf. This point cannot be over-emphasised. There have been well-publicised data breaches arising from customers failing to understand their role in securing cloud services properly, leaving data open to a wider audience than intended. The key to a successful security implementation in a cloud environment is understanding where the cloud provider’s responsibility ends, and where the customer’s responsibilities begin.

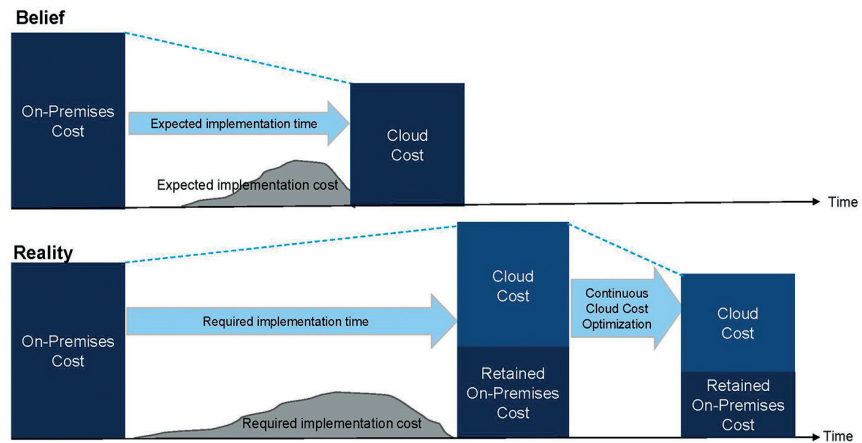
8 Implementation of cloud services is not a ‘once and done’ endeavour. While cloud may sometimes save money, organisations should not assume this will always be the case without undertaking a detailed analysis of their total cost of operation and examining the opportunities for optimisation. For example, a ‘lift and shift’ migration of existing applications to cloud hosting is likely to require further work to ensure they are optimised to take maximum advantage of the benefits that a cloud environment can offer (**Figure 1**).

Figure 1

Possible impact of the move to cloud on an organisation's costs

Without optimisation, there is a risk that cloud services can be more expensive than on-premises

Question Cost Reduction as a Main Driver for Cloud Adoption



RESTRICTED DISTRIBUTION
 1 © 2020 Gartner, Inc. and/or its affiliates. All rights reserved.



Note

- 1 Retained cost represents the in-house capability and expertise an organisation needs to maintain in order to manage cloud services securely and effectively.

Source: Gartner, *7 Elements for Creating a Pragmatic Enterprise Cloud Strategy*. Reproduced with Gartner's permission

What is government policy on cloud services?

9 Government supports the move towards cloud services. It encourages public sector organisations to adopt cloud systems where they offer better services or value for money. It has developed its policy over time:

- Cloud first, May 2013: expresses an explicit preference for public cloud over private, community or hybrid deployment models. Departments are free to choose alternatives to cloud services if they can demonstrate that they are better value for money.
- Cloud native, February 2017: expresses a preference for software-as-a-service (SaaS) applications and encourages organisations to move towards using a range of cloud-based tools.
- Use of G-Cloud: all cloud purchases must be made through the G-Cloud procurement framework available through the Digital Marketplace. The framework is refreshed on a regular basis.
- Technology Code of Practice: the Government Digital Service reassessed the Cloud-first policy in 2019 and it remains a key technology policy, although in stating “consider using public cloud solutions first” it acknowledges that cloud solutions may not be right in all situations.
- Cloud guide for the public sector, March 2020: provides guidance on how organisations can make informed decisions about their cloud strategy. It recognises that cloud services are not “one size fits all” and provides advice on lock-in, commercial, technical, security, operations, people and related issues.

10 Guidance continues to evolve and organisations should ensure they are aware of the latest developments. The One Government Cloud Strategy (OGCS) is an ongoing initiative which has already delivered several cloud-related outputs including the *Cloud Playbook*, Cloud Memorandum of Understanding (MoU) and an Online Shared Workspace. Public sector organisations can contact the Cabinet Office to find out more.¹

¹ Contactable at ogcs@cabinetoffice.gov.uk (correct as at 17 March 2021).

Other guidance available

11 Our cloud guidance is highly summarised and there are other complementary, more detailed guides on offer.

- The National Cyber Security Centre (NCSC) provides guidance on security specific to cloud services. This includes *Making a decision*, which sets out eight steps to work through when assessing which services are suitably secure, and *Cloud security principles*, which outlines specific considerations to help underpin this assessment (see Appendix One).
- The Chartered Institute of Public Finance and Accountancy (CIPFA) provides a guide to the accounting questions raised by buying software and technology as a service. Compared with traditional technology procurement, this may move expenditure from capital to revenue.
- The Financial Conduct Authority (FCA) provides a guide for firms outsourcing to the cloud and other third-party IT services. This guidance helps firms to oversee the life-cycle 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.
- More specific guides and advice are available through subscription to research services such as Gartner.



An overview of cloud services

12 Cloud services are systems and data accessed over the internet.

This contrasts with traditional systems where hardware and software are maintained on an organisation's own premises and accessed via dedicated connections. Cloud services are not a new concept and have been available in one form or another for more than 20 years. An early example was email accessed through a web browser (Hotmail, launched in 1996). More recently, better and faster internet connections create new opportunities for cloud services, which are available in a wide range of areas, including business and financial systems.

13 Cloud services are being 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.

14 There are three basic cloud service models (**Figure 2**):

- **Infrastructure as a service (IaaS)** – provides the base layer of computing infrastructure. It is suited to users who need access to high levels of capacity for their own systems, for example computationally intensive data analytics processing. The customer has control over operating systems, applications and many security options. Examples include Microsoft Azure, Google Cloud Platform and Amazon Web Services (AWS).
- **Platform as a service (PaaS)** – provides the computing infrastructure plus the operating system and databases. This option works for organisations who want to run their own software on a cloud platform. The customer has some control over the configuration settings for the environment the software runs in. Examples include Microsoft, Google and AWS as above as well as smaller specialist providers such as UKCloud.
- **Software as a service (SaaS)** – this delivers fully featured applications over the internet. Customers do not need to install or maintain software or have their own hardware, other than the devices (such as laptops and tablets) that they will use to access the internet. However it gives the least amount of control over updates and changes to features. Examples include productivity and communication suites such as Microsoft 365 (formerly Office 365) and Google Workspace (formerly G Suite), and finance and planning systems such as Oracle Fusion Cloud, SAP S/4HANA Cloud and Workday.

Figure 2
Comparison between on-premises and different cloud service models

On premises	Infrastructure as a service	Platform as a service	Software as a service
Data content/ security	Data content/ security	Data content/ security	Data content/ security
Applications	Applications	Applications	Applications
Database	Database	Database	Database
Operating system	Operating system	Operating system	Operating system
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Network	Network	Network	Network

You manage
 Others manage

Source: National Audit Office, based on National Institute of Standards and Technology technical guidance

15 Not all cloud services are necessarily described in the above manner. For example, the G-Cloud framework categorises services as **cloud hosting** (infrastructure and/or platforms), **cloud software** and **cloud support** (that is, to help set up and maintain a service). There are offerings which are a hybrid of platform and infrastructure as a service, and specific features can be described “as a service” in their own right, for example desktop, containers, security, and many others. However, these involve a level of more detailed technical explanation which goes beyond the scope of this general guide.

16 The three levels of cloud service outlined above may be provided on the following types of cloud deployment (**Figure 3**):

- **Public cloud** – the cloud provider owns and runs cloud systems which provide services over the internet to anyone who wishes to sign up to them. Many customers (known as ‘tenants’) share the same underlying hardware, storage and network devices and there are technical measures in place to maintain the separation of data belonging to different tenants.
- **Private cloud** – the cloud provider gives a single customer dedicated use of specific cloud systems. This provides enhanced control over the environment as the resources are not shared with others. While this model has security advantages, it is more expensive than public cloud.
- **Community cloud** – this is where a dedicated service is shared between a limited community of organisations with common requirements around security, privacy, performance and compliance and who bear the costs of the service. It is generally the responsibility of the community itself to determine its requirements and whom it wishes to admit.
- **Hybrid cloud** – this involves a combination where some applications and services are run in one cloud and others in a different cloud (or on-premises). These can be complex and challenging to create where there is a requirement to exchange data.

Figure 3
Types of cloud deployment model



Note

1 Hybrid is a combination of different deployments and is not shown separately.

Source: National Audit Office, based on National Institute of Standards and Technology technical guidance

Pricing of cloud services

17 Cloud services have different pricing models to reflect the degree of certainty or flexibility organisations require or are willing to accept. To get the best value out of cloud services, organisations should understand their requirements and select the model or combination of models which have the best fit with their needs:

- **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.
- **On-demand** – this is a ‘pay as you go’ option that charges for capacity on a metered basis as and when an organisation needs to use it, such as to support peaks in workload. By only paying for what is used, and only using what is needed, this 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** – this is where 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 is sometimes also known as excess capacity and best suits activities that are not critical or time-sensitive and which can be paused (for example, development environments). It is not well suited to services that need to run continuously.

Legacy systems

18 We define legacy as “systems and applications that have been operationally embedded within a business function, but have been overtaken by newer technologies or no longer meet changed business needs”. Public and private sector organisations alike have legacy challenges to manage to some degree. This is because it would not be 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, 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.

19 Options for dealing with legacy technology in the context of contemplating a move to cloud services are set out below. These should be considered on a system by system basis rather than a strict policy for all legacy technology:

- **Retain** (do nothing) – for example 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** – for situations where the system’s functions are either no longer required or can be incorporated into other applications.
- **Repurchase** (‘shop and drop’) – this involves decommissioning the existing application and replacing it with its equivalent cloud-based version. In effect it is little more than a change in licensing arrangements.
- **Rehost** (‘lift and shift’) – this involves 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 customers 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’) – this involves modification and optimisation of 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.

20 The last four of these options will require the organisation to perform extensive testing to confirm that the system operates satisfactorily in its new environment and that the migration has not introduced a lower quality of service overall. For example, whereas all expected functionality 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 in order to stand still in terms of overall user experience.

Lock-in and exit strategy

21 Lock-in arises where an organisation becomes dependent on the products and services from a particular supplier. It can also arise where an organisation uses more than one cloud provider but is dependent on each for the particular services that they offer. Switching to a different technology or provider becomes difficult, time-consuming and disproportionately expensive. There are two main types:

- **Commercial lock-in** – this arises where long and inflexible contracts with providers can prevent organisations from changing their technology strategy when circumstances change. Commercial lock-in is discouraged. Government advice is that it can be reduced by agreeing shorter-length contracts, and organisations ensuring that they retain the intellectual property of their products and services as well as access rights to their data. However, shorter-length contracts can bring their own particular considerations. Organisations will have to run procurement and evaluation exercises at more frequent intervals. Vendors may also be less inclined to offer incentives for a longer-term relationship.
- **Technical lock-in** – this arises where there are no commercial barriers to moving from one provider to another, for example an organisation is approaching the end of its contracted term or is on a pay-as-you-go pricing model, but to do so represents 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. 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 make use of, and could ultimately compromise the value to be obtained from moving to cloud. In most cases a trade-off is involved and each organisation needs to determine its own approach and make a judgement on the degree of lock-in that it is willing to accept.

22 While at the moment non-cloud versions of software may still be available, organisations may find that over time they become less well supported by the vendors, or become more expensive. Therefore, the viability of maintaining an on-premises alternative may diminish over time, particularly for organisations expected to meet common standards set for government as a whole.

23 One of the most important components of a cloud strategy is an exit strategy, even if it is never used. An exit strategy 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 take into account other points of lock-in, such as skills and capability.



Part One: Assessment of cloud services

1.1 Before selecting a cloud solution, organisations need to evaluate what is suitable for their needs and objectives. Cloud providers are promoting their services very strongly in the market. It can be challenging for decision-makers to form a clear view of the relative merits and potential pitfalls of various cloud services. Management needs to set clear criteria for success so that it can properly evaluate the options available. This is particularly important when using G-Cloud because of the requirement to evaluate all suppliers which meet the organisation's stated requirements and choose the best fit including whole-life cost.

Digital strategy

1.2 A successful digital strategy should be central to the wider organisational vision and strategy. Many organisations are now developing cloud strategies. However, management should guard against its vision being led by a decision to use specific technological solutions. Management should first develop robust organisational and digital strategies and establish a clear view of its technological requirements. Smaller bodies may find it beneficial to engage the expertise of service companies to help them understand and navigate the various options.

Questions audit committees could ask:

- **What are the priorities for the digital strategy?** Does it start with the organisation's needs, rather than being retro-fitted to a high-level decision to use a particular technology? Does the digital team have a clear understanding of the operational realities of the business activities undertaken? Are operational experts committing time to supporting the digital team to develop their strategy?
- **Has the cloud strategy had input from an appropriate range of stakeholders?** Does it address the commercial aspects, such as planning, negotiating and managing the commercial relationship? Does it address resourcing aspects such as recruitment, skills and development, both for the migration and or maintaining and optimising cloud services thereafter? Does the strategy envisage undertaking steps to properly optimise cloud costs, such as the creation of a central cloud team that combines technical and commercial knowledge?

- **Have technical requirements been articulated?** Has the organisation considered what is the most appropriate type of cloud service model (infrastructure, platform or software as a service) and deployment model (public, private, community or hybrid cloud)? Will the organisation's own external internet connections, and those from other locations where users may be accessing cloud services (for example, working from home), be sufficient and reliable for software as a service to be viable, especially with the increased levels of home working seen during the COVID-19 pandemic?
- **Have any specific features or legislative requirements been considered and identified?** Does the organisation have a strategy for the use of cloud services, based on a clear understanding of the implications for personal data, privacy and consent? Are there any specific requirements which need to be accommodated, such as machine learning, advanced data analytics, UK-only data hosting? Is the organisation aware that not every service may be available in every region? Will some services require the use of particular or multiple cloud providers?
- **Is the complexity of legacy system issues fully understood?** Has the organisation thoroughly investigated the challenges involved in migration and configuration, such as moving a bespoke system onto a shared platform? Does the digital strategy include a risk assessment of the degree of change involved, including personnel considerations? Is there a strategy for retiring legacy systems to avoid the costs of supporting old and new systems together for extended periods? 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? Does the strategy include provision for upskilling teams where a hybrid approach is being taken?
- **Will best practice be followed in respect of security?** Does the strategy set out how assurance will be gained in respect of the NCSC's 14 cloud security principles (see Appendix One)? Does it have an in-depth plan for how cloud services will interface securely with existing services, systems and processes?

Business case

1.3 Cloud service providers advertise a range of selling points. These include cost efficiencies, adaptability, scalability and security. However, the cost of cloud services can vary significantly depending on uncertain factors such as user numbers and data volumes in future usage scenarios. Different suppliers have different elements to their pricing. The benefits of adaptability and flexibility depend on the complexity of implementation and the extent to which services are tailored. The advantages of cloud technology can be significant enough to justify the extra effort needed for accurate forecasting.

Questions audit committees could ask:

- **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) been considered? Have any potential additional charges for copying or extracting data from the cloud provider to local storage (known as 'data egress') been taken into account?
- **How sensitive are planned costs to scenario testing?** Does the organisation have a clear understanding of current service usage and how this might change in the future? Has it analysed the fixed, marginal and step costs in each of the different options and bundled packages? Does the expected usage include development and test environments as well as live services?
- **What extra skills and capacity will 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? What is the wider impact on the workforce and the cost of training and roll-out? 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. Users will also need to adapt to a culture of more frequent change and improvement to the systems they use for work, and not feel threatened by it.
- **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 Government Digital Service (GDS) 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?** Is there clear articulation of the benefits of using a single provider where this is judged to outweigh concentration risk? Has the Cabinet Office been consulted, especially where services form part of the Critical National Infrastructure?
- **What time horizon is being considered in the commercial model?** Has management ensured that break clauses are there to prevent lock-in if the provider does not keep pace with requirements such as changes in open standards? If implementation costs are high with highly tailored services, will this weaken the negotiating position when the initial contract expires? Has an assessment been made of the longer-term costs of such tailoring, and would a more 'vanilla' implementation be a better option?
- **Is there an exit strategy?** Has the organisation undertaken an assessment of the costs and barriers to retrieving the organisation's own 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 contract exit arrangements fully documented with a legal commitment for the cloud provider to cooperate with transfer and removal of data? Are there contractual mechanisms to ensure the provider can supply the organisation's data in a reasonable electronic format for migration to another provider? Are the actual mechanics of how the data would be extracted under such a scenario sufficiently clear from the outset (particularly given the current contract lengths on G-Cloud)?

Due diligence

1.4 There is a wide variety of cloud service providers and many are global suppliers. The providers on G-Cloud have been pre-screened only to check they are suitable to work with government, and not to provide any 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.

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

Questions audit committees could ask:

- **Will there be clear accountability between the organisation and cloud provider?** What oversight regime will the organisation have over the cloud provider? Does the cloud provider sub-contract and if so how does it manage risks? Has the organisation undertaken sufficient due diligence to mitigate against 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 been verified?** Has the organisation obtained feedback from other customers on how easy it is to configure the cloud service? How easily will the new service integrate with other systems? Are some of the features listed as 'beta', meaning they could potentially be modified or withdrawn with little or no notice?
- **What are the terms of service?** Is the capacity and availability guaranteed by the cloud provider sufficient for the organisation's needs? Is this backed up by the provider's track record to date? Is the service level agreement fully understood? What are the business continuity arrangements? How quickly is service guaranteed to resume after an outage? Is the provider's liability cap likely to be sufficient (particularly for smaller contracts) to cover the cost of any damage the organisation suffers?
- **Where is the provider's infrastructure physically situated, and in what jurisdiction(s) is the organisation's data being held and accessed?** What assurances and guarantees are there on data residency and sovereignty? Are there security or sovereignty constraints imposed by a parent department or other important stakeholders? (There is no government policy which directly prevents departments or services from storing cloud-based data in any specific country and it is the responsibility of each organisation to take risk-based decisions. 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 make use of? Will this incur additional cost? Will UK resident data be accessed from offshore locations?

- **Will the cloud service contract be governed by the law and subject to the jurisdiction of the UK?** Where is the service hosted? 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 therefore represent a supply chain risk? Will the cloud provider allow access to its premises and data by the organisation, its auditors (internal and external) and any relevant regulators without any restrictions? Will it support requests such as subject access requests under the Data Protection Act 2018?
- **What security accreditation and protocols does the provider have?** What information security standards do they meet? What measures are there to prevent unauthorised access, for example encryption or multi-factor user authentication? Are these part of the core offering, are they additional paid-for options, or are they left to the organisation to implement separately? Has the technical architecture of the system been reviewed by appropriate experts? What is the provider's approach to proactive testing, and is there historical evidence of how it has 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*)? Are assurances based on self-certification or are independent validation reports available? See Appendices One and Two 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 (SOC) type 1, 2 or 3 assessments and so on – see Appendix Two) and make the results readily available to customers? Does the service provide sufficient logs or alerts to support how the organisation detects and responds to security incidents? Will there be sufficient in-house resources to understand and interpret the information and alerts being fed back? Will there be the capacity and expertise to respond appropriately when the alerts indicate that action is required on the part of the organisation? Does the provider operate its own security functions with whom the organisation can collaborate when investigating security incidents or seeking assurance?



Part Two: Implementation of cloud services

2.1 The majority of the challenges in introducing cloud services implementation are common to on-premises system implementation. Indeed, the broader challenges of change management and stakeholder engagement also apply to the introduction of cloud systems. However, cloud services and providers can vary in their levels of maturity and configuration can be complex. Management needs to be confident that it has addressed the risks associated with cloud service implementation. Failing to configure cloud services correctly can severely hamper the achievement of financial benefits as well as exposing organisations to the risk of a data breach.

System configuration

2.2 The potential variation and 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 interoperate and communicate efficiently and securely. Smaller organisations are less likely to have sufficient expertise and capacity to manage 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.

Questions audit committees could ask:

- **Is there a strong governance and project management plan in place?**
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 business in the programme governance?
- **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? 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 which can be understood by someone not involved in the original implementation?

- **Is the organisation overly reliant on third-party resource?** Is there sufficient resilience 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?
- **Will people be ready for the new systems?** Have users been engaged throughout? Have there been clear communications about the cut-over dates? Do people know about the systems they should use and their own responsibilities for maximising the chances of a smooth transition?

Risk and security

2.3 The cloud is not necessarily any more or less secure than on-premises technical architecture. The threats in an on-premises and public cloud ecosystem are broadly similar. There are entire application ecosystems running in public cloud that have strong cyber defences with multiple layers of security. Equally, there is a plethora of cloud solutions that are deployed with default configurations. Organisations must recognise their own role in ensuring that data is appropriately secured and not left open to a wider audience than intended.

Questions audit committees could ask:

- **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 and loss of encryption keys? Are key personnel aware of the steps they would need to take in the event of different kinds of security breach?
- **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? 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 taken into account? Has the organisation assessed the reputational risk of a data breach arising from failure to act on warning signs which 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? What are the policies covering key issues such as vendor lock-in, governance, compliance, reputation and supply chain failures?

- **Have business continuity plans been updated?** Is the organisation prepared for a range of scenarios for service outage?
- **Are plans in place to cover the event of data loss?** Is key data covered by a system of point-in-time backups? Are there plans in place to support ongoing business in the event of data being lost?
- **Are financial controls fully tested and compliant with best practice?** Particularly for financial systems 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? How robust is identity management to ensure that financial controls are not undermined (for example, segregation of duties)?
- **Have privileged accounts been secured?** Are administrator and service accounts (that is, accounts used by the system itself rather than individuals) also secured appropriately? (Recent studies have suggested that three-quarters of security breaches begin with compromised privileged accounts, of which there can be several thousand across cloud platforms.)

Implementation

2.4 The realisation of benefits from new software can be contingent on user acceptance, compliance and engagement. Cloud systems often involve significant and more frequent changes in the user interface and, while they 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.

Questions audit committees could ask:

- **Have key stakeholders been engaged through a comprehensive change management strategy?** Does the organisation have adequate plans to provide training, ongoing support and coaching for users before, during and after implementation, according to the service 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' (that is, where maintaining the status quo will become prohibitively expensive or even impossible) and would they be able to continue indefinitely until implementation issues are resolved?
- **Are there sufficient 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?
- **Is there sufficient information for a Go / No Go decision?** Has the organisation assessed the impact of any issues outstanding?



Part Three: Management and optimisation of cloud services

3.1 A move to cloud services should reduce the previous type of capability required in-house to manage live services. Cloud service providers can take care of infrastructure management and maintenance and software patching and updates. They can also provide a helpdesk and support to users and technical staff depending on the service in the cloud. However, new capability is required to understand and manage and interpret the interface between the cloud service and the organisation. Organisations cannot outsource responsibility for governance of data and controls operated over financial and other transactions, nor for data security including the interpretation of monitoring information and alerts from the cloud provider. Many organisations also opt to modify the services they use and this can increase the ongoing need for in-house service management.

Operations

3.2 Immediately after go-live there may be a period of teething issues and frustration as it takes time for the requirements backlog to be addressed. Ongoing change management will be important through these stages to assure users and signpost any further changes to system interfaces or configuration. It is important for there to be strong governance 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 with an on-premises environment. The organisation will have a lesser degree of control over the acceptance of these updates, particularly with software as a service.

Questions audit committees could ask:

- **Is there effective governance to prioritise the removal of any temporary workarounds?** Are there any integration issues still outstanding which 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 its plans to release new features and upgrades to its systems? Is the organisation able to influence the cloud provider to prioritise the developments it would value, or the retention of features it would not wish to see discontinued? Is the organisation assessing the impact of planned changes on the business?
- **Are responsibilities 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? How long will the team have to test any changes in a sandbox before being required to release them into the live service?

- **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 logging and auditing functions been turned on to provide tracking information?
- **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 cloud instances and services are only set up where there is a necessary business requirement, that they are done so in the most efficient way, and that they are shut down again when the business need has been satisfied? Is there a regular review to ensure that the pricing model selected continues to be the best fit for the organisation's needs?

Assurance

3.3 Cloud providers typically offer assurance to their customers in the form of Service Organisation Controls (SOC) reports (see Appendix Two). Cloud providers commission independent auditors to write these reports to provide assurance on their processes and security arrangements. Management needs clarity on the assurance 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.

Questions audit committees could ask:

- **Does management understand the general scope and limitations of the different types of Service Organisation Controls reports?** Is assurance required to cover financial reporting (SOC1) or wider operational controls (SOC2)? Is a publishable public-facing report (SOC3) needed? Does the report provide a view on the cloud provider's latest penetration test or vulnerability assessment report?
- **Is management clear on the scope of controls tested and the extent of testing?** Is the service auditor a recognised firm? What additional controls or assurance is needed to cover internal processes and systems? If there are weaknesses or gaps in the cloud provider's controls, are there additional steps which management should take to strengthen internal controls? Should management obtain further assurance on the overall operating model?
- **Do Service Organisation Controls reports give assurance on the success of operational controls over time?** Are Type 2 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 Service Organisation Controls reports frequent enough to keep pace with continuous improvement?** Is there a mechanism 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 Service Organisation Controls 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 outsourcing extends the scope of management's responsibilities for gaining assurance over data, transactions and controls operated on its behalf by others?

Capability

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

Questions audit committees could ask:

- **Will the organisation retain the necessary technical knowledge post-implementation?** What knowledge will there be of any ongoing 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 made available to show what configurations or customisations have been implemented in practice?
- **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 (BI) 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 value for money and compliance?** 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 technologies becoming available?



Appendix One

National Cyber Security Centre guidance

Making a decision - eight steps

NCSC advises that working through the eight steps below will help organisations identify cloud services that are suitably secure for their intended purposes:²

- 1 Know your business requirements.
- 2 Understand your information.
- 3 Determine relevant security principles (see below).
- 4 Understand how the principles are implemented.
- 5 Understand the level of assurance offered.
- 6 Identify additional mitigations you can apply.
- 7 Consider residual risks.
- 8 Continue to monitor and manage the risks.

The 14 cloud security principles

The 14 security principles which NCSC recommends organisations should consider in support of the steps above are summarised as follows:³

- 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 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 at rest protection, data sanitisation, equipment disposal, and physical resilience and availability.

² Available at: www.ncsc.gov.uk/collection/cloud-security (accessed 16 March 2021).

³ Available at: www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles (accessed 16 March 2021).

- 3 Separation between users** – a malicious or compromised user of the service should not be able to affect the service or data of another user. 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 which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.
- 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 to identify and mitigate 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.
- 9 Secure user management** – the provider should make tools available for customers to securely manage their use of its 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 authentication of users, access control and segregation of duties.
- 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 (that is, where a single identity is trusted across multiple systems). 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 which 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 for users** – 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 the configuration and management of devices (PCs, tablets, phones and so on) used to access the service.



Appendix Two

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

1 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 Service Organisation Controls (SOC) reports.⁴ 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; and
- **SOC3** – a shorter version of the SOC2 report which is placed in the public domain but omits the detail of the test procedures undertaken.

2 Organisations should understand what assurances they are and are not getting from such reports and other certifications such as Cyber Essentials⁵ or ISO 27001.⁶ 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 externally assessed, 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.

⁴ The content is prescribed in *International Standard on Assurance Engagements (ISAE) 3402: Assurance Reports on Controls at a Service Organisation*, 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. It is available at: www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isa-3402.pdf (Accessed 16 March 2021).

⁵ Available at: www.ncsc.gov.uk/cyberessentials/overview (Accessed 16 March 2021).

⁶ See: www.iso.org/isoiec-27001-information-security.html (Accessed 16 March 2021).

- 3** Organisations which fail to appreciate these considerations may in effect be outsourcing unknown levels of risk.
- 4** Organisations may find that 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 which prioritises essential contracts and services.

© National Audit Office 2021

The material featured in this document is subject to National Audit Office (NAO) copyright. The material may be copied or reproduced for non-commercial purposes only, namely reproduction for research, private study or for limited internal circulation within an organisation for the purpose of review.

Copying for non-commercial purposes is subject to the material being accompanied by a sufficient acknowledgement, reproduced accurately, and not being used in a misleading context. To reproduce NAO copyright material for any other use, you must contact copyright@nao.org.uk. Please tell us who you are, the organisation you represent (if any) and how and why you wish to use our material. Please include your full contact details: name, address, telephone number and email.

Please note that the material featured in this document may not be reproduced for commercial gain without the NAO's express and direct permission and that the NAO reserves its right to pursue copyright infringement proceedings against individuals or companies who reproduce material for commercial gain without our permission.



National Audit Office