Chartered Institute of Internal Auditors

21 September 2020

Cloud computing

Chartered Institute of Internal Auditors

Get an overview of cloud computing: the likely benefits, significant risks and the ways that internal audit can provide assurance.

What is 'the Cloud ?

The Cloud is a set of on demand computing resources and services, accessed over the internet via third parties. This allows faster innovation and rapid deployment rather than developing, building, hosting and maintaining IT systems and applications ‘in house’ which increases the total cost of ownership.

Cloud is not a new concept anymore – an early example most people will be familiar with is using Hotmail in the 1990s, or more recently Facebook or applications such as OneDrive and iCloud. Common business applications which are based on Cloud technology include Salesforce, Microsoft Office 365 and Google GSuite. Cloud technology is everywhere.

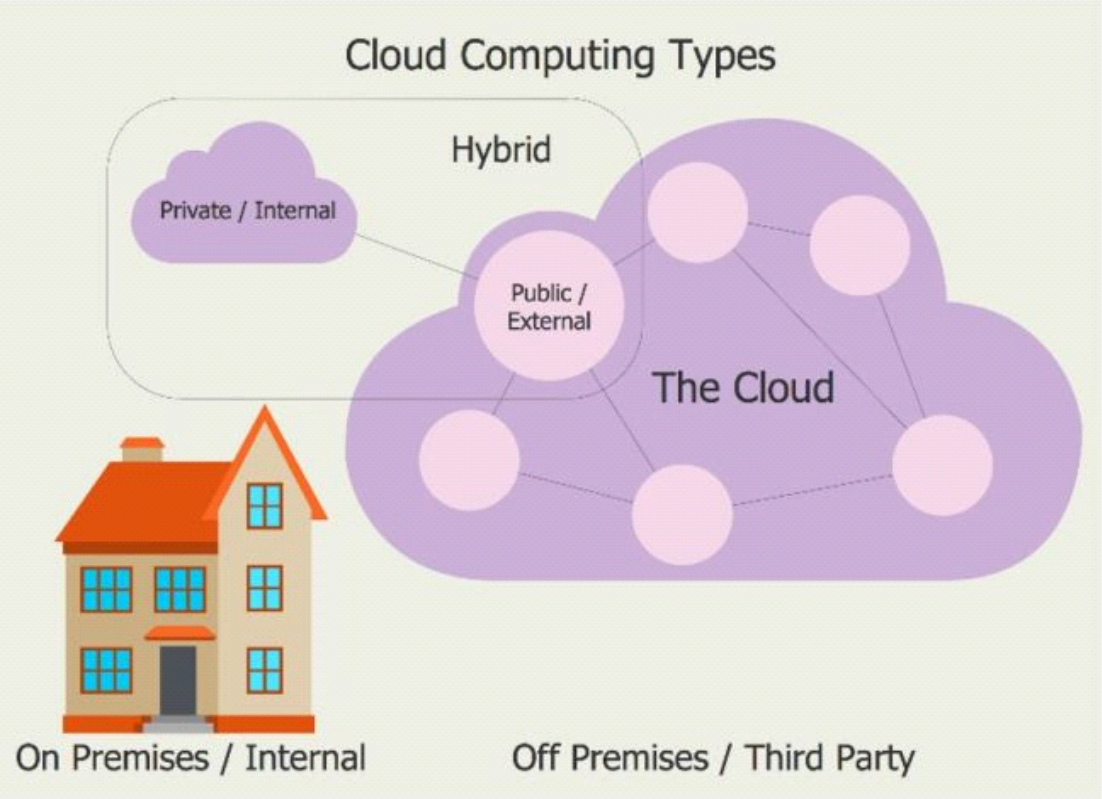
Benefits

The benefits of migrating to the Cloud can be substantial for organisations:

- operating and maintenance costs are reduced
- scalability can be achieved quickly to meet spikes in demand
- organisations only pay for what they use so at times of low transactions costs are lower
- there are greater options for flexibility and accessibility as users can access applications from their own devices and from any location with access to the Internet
- enhanced security capabilities can be achieved by leveraging readily available sets of policies, controls and technologies to protect data and infrastructure
- providing a reliable third party is used; organisations can achieve much greater resilience in system availability.

Different types of Cloud provision – benefits and risks

The main types of Cloud are private, public and hybrid.



Source: https://www.conceptdraw.com/solution-park/computer-networks-cloud-computing-diagrams

Public

- public Cloud is owned by the third party

- typically, all users across different organisations or jurisdictions share the same resources/infrastructure
- the organisations using the public Cloud don't own any of the technology assets.

Benefits

- there is greater ease of interaction/collaboration between multiple people
- ease and efficient management of resources through a web browser
- the organisation can quickly expand or reduce capacity to meet supply and demand which drives cost benefits as the organisation does not need to pay for resources is it not using
- the reliability of the technology services should be improved, particularly when using one of the top tier providers
- maintenance of technology is carried out by the Cloud provider, leading to further cost savings.

Risks

- the organisation has limited control over the public Cloud
- Cloud services are classed as 'multi tenancy' which means that all organisations may share resources or infrastructure while access is managed using different log on credentials; which could lead to concerns over data protection and security
- there is reliance on the Cloud provider's controls to segregate data between the different organisations
- the organisation may assume incorrectly that the Cloud services have been configured correctly when in fact Cloud services need to be configured to an organisation's needs, or additional services need to be paid for.

Private

- the organisation is the single customer and has sole use of resources
- private Cloud can be hosted in the organisation's own data centre or third parties.

Benefits

- the organisation is completely isolated from other organisations therefore there are decreased risks associated with data segregation and control
- the Cloud services are more flexible to the individual needs of the organisation and can be customised.

Risks

- the cost considerations of this option need to be carefully considered as this option is more expensive for example, the organisation is responsible for service management and maintenance
- the organisation needs to consider whether it has the required skills in house to manage private Cloud

Hybrid

- a mix of public and private resources is used by the organisation allowing data and applications to move between both, with generally the more sensitive operations using private Cloud.

Benefits

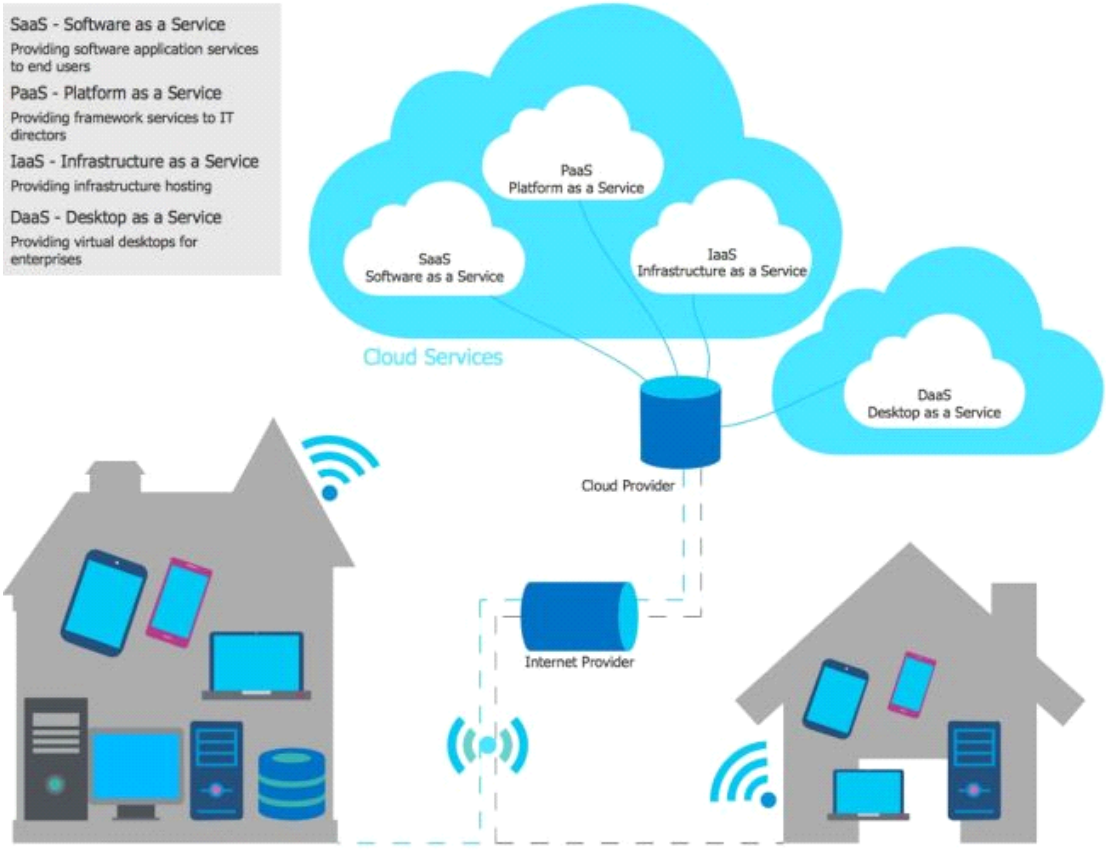
- hybrid Cloud allows efficient management of workloads whilst enhancing control over more sensitive operations by using the private Cloud
- the cost benefits of expanding capacity to meet supply and demand can still be achieved using the public Cloud where possible.

Risks

- Cloud integration is a highly skilled role and therefore the organisation needs to ensure it has the right resource to support this approach
- there can still be security concerns for sensitive data as data management can be a challenge if data is moving between both Cloud types
- it can be hard to find an efficient strategy to derive the maximum benefits from this approach
- the design of the network can be complex.

Different types of Cloud services

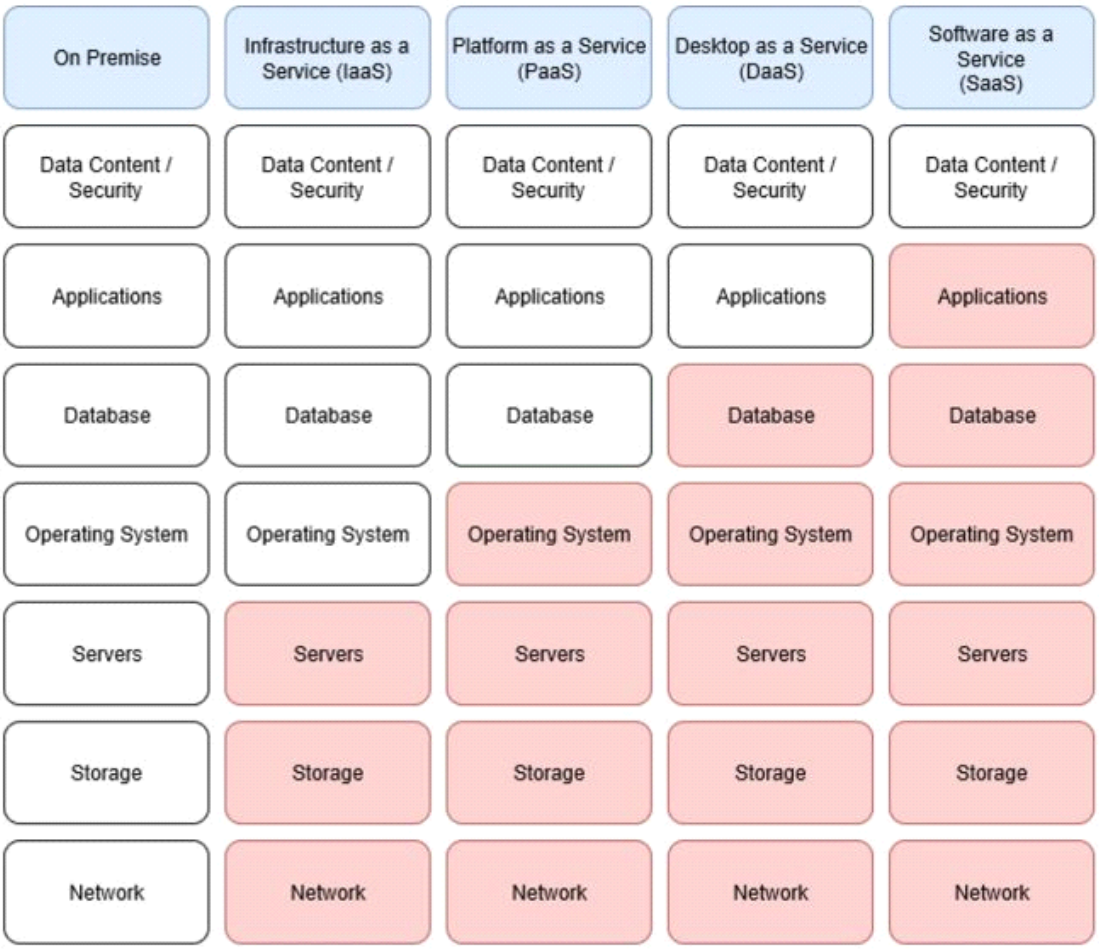
The types of Cloud services are Platform as a Service, Infrastructure as a Service, Software as a Service and Desktop as a Service.



Source: https://www.conceptdraw.com/solution-park/computer-networks-cloud-computing-diagrams

The table below demonstrates what each Cloud service provides compared to traditional on-premise technology. On-premise refers to the physical kit and infrastructure that an organisation would need to have on-site in order to run the organisation's technology. When using Cloud services, the organisation utilises the Cloud providers infrastructure rather than owning everything themselves on the organisation's own premises.

For all the different types of Cloud services, the responsibility for data security always resides with the organisation rather than the third party – as with responsibility for all risks. The organisation still owns all the risks; however, they may need to be managed in a different way with different means of gaining assurances.



Note: shaded boxes are what 'others manage

There are lots of resources available to explain the different types of Cloud in more detail, including the recently issued guidance from the National Audit Office for Audit Committees.

Potential risks and responses

The risks associated with Cloud are wide ranging and varied, and when auditing Cloud or considering the risks you are effectively assessing the whole range of IT risks because whole sections of IT operations are being outsourced to a third party. Often, in the race to migrate to the Cloud, insufficient consideration is given to the entirety of what is required to move to this new operating model.

Cloud provision is classed as material outsourcing in any organisation, and indeed for organisations regulated by the Financial Conduct Authority FCA Material Outsourcing SYSC 8 regulations need to be applied. As with any outsourcing, the risks are not delegated to the third party and it remains the organisations' responsibility to manage those risks. It will always be the organisation's reputation at stake for any customer service issues, major incidents or breaches.

Internal audit activities are recommended to perform a risk assessment as Cloud risks and scope areas are almost as wide ranging as an IT audit universe. It could be difficult to perform one audit which covers all the risks in enough detail.

One approach for consideration is to always include Cloud consideration in every IT audit so that both on premise and Cloud risks are considered in tandem. This will require the chief audit executive to consider the resource impacts when preparing the annual audit plan as more time will be required.

Below is a summary of the key scope areas to consider, it is not an exhaustive list

Different types of Cloud services need to be audited differently depending on the service agreements and the type of Cloud service, below are generic considerations that should be considered as part of the audit of different types of Cloud services.

1. Service interruptions of Cloud provision

Potential impact

- the organisation's continuity of service is interrupted leading to financial losses, poor customer service and reputational damage.

Potential responses

- enough due diligence has been completed over the Cloud provider to ensure the organisation is satisfied with equipment/site locations, emergency power supply and the level of environmental or other risks which could impact continuity
- the contract in place with the Cloud provider is robust and includes the continuity clauses, service level agreements and monitoring approaches, including setting out availability targets
- the organisation has continuity policies and procedures in place that are aligned with the Cloud provider including ensuring the Cloud provider can meet the recovery point objectives and recovery time objectives set out in the business impact analysis

- the organisation has a robust business continuity and disaster recovery testing approach in conjunction with the Cloud provider which is exercised at least annually.

2. Security of data hosted in the cloud

Potential impact

- data is not appropriately secured or managed leading to loss or breach of company or customer data leading to regulatory censure and reputational damage.

Potential responses

- the organisation has conducted suitable due diligence with the Cloud provider to ensure the required controls are in place surrounding data protection
- suitable clauses are included within the contract surrounding data protection
- the organisation and the Cloud provider agree and align controls according to the end to end processes in place and the data in use including but not limited to:

  a. data classification
  b. data inventories
  c. data flow maps
  d. ownership and stewardship
  e. disposal of data and kit
  f. asset management
  g. privileged user and user access management
  h. archiving
  i. cross border controls
  j. process for managing breaches
  k. secure area authorisation.

- where multi-tenancy is in place with public Cloud provision, suitable controls have been designed to segregate the organisation's assets and protect any data from unauthorised access including implementing intrusion detection and prevention monitoring and alerting, and an agreed and tested incident management plan is in place
- appropriate security and application controls have been implemented to protect all data exchange and ensure transaction security and integrity
- appropriate controls are in place relating to use of data in project/development work particularly testing to ensure that non-production data (data used in the non-production environment ie in testing areas) is appropriately used and secured.

3. Change control and configuration management

Potential impact

- the change control and configuration management in place within the Cloud provider is not of the required standard causing incidents in the live environment impacting service continuity and customer experience.

Potential responses

- as part of due diligence, the organisation confirms that the Cloud provider has suitable change

control and configuration management standards in place
- suitable terms are agreed within the contract and associated schedules detailing the agreed upon processes and standards to be achieved are included
- the organisation and the Cloud provider agree and align controls related to change control and configuration management including but not limited to:

  a. development
  b. outsourced development
  c. quality testing
  d. unauthorised software installations
  e. production changes
  f. service and data integration
  g. implementation management including readiness
  h. emergency changes
  i. change authorisation protocols
  j. project management.

4. Cloud strategy

Potential impact

- an inappropriate, misaligned strategy has been implemented by Technology without suitable buy in from the organisation leading to unnecessary costs and inefficiencies.

Potential responses

- technology have implemented a Cloud strategy in conjunction with the business to meet business needs
- the Cloud strategy is well communicated throughout the organisation and appropriate controls are in place to ensure that future development follows the strategy
- a clear plan has been developed to manage migration to the Cloud and appropriate funding has been secured to facilitate the journey
- the risks of migrating legacy workloads to the Cloud have been assessed and suitable controls put into place to manage these risks
- the risks associated to adding a Cloud service to the existing footprint have been identified, assessed and appropriate controls put into place to manage them
- a 'to-be' target architecture is established for the Cloud strategy
- a clear plan had been developed to establish the required data privacy and security controls associated with the consumption of the different types of Cloud services.

5. Human resources

Potential impact

- the people related impacts surrounding a Cloud strategy are underestimated and lack of control at both the organisation and the Cloud provider leads to risk of inappropriate behaviour such as insider fraud and malicious insider behaviour
- the organisation does not have suitable skills employed to successfully implement and operate a Cloud strategy.

Potential responses

- suitable controls are in place in relation to termination of employment at both the organisation and the Cloud provider to ensure that upon cessation of employment, the necessary action is taken to remove access from the organisation's assets, particularly for colleagues with privileged access
- appropriate policies and procedures are in place within the organisation to manage mobile device usage particularly where Cloud-based applications are used from personal devices; this includes remote wipe facilities
- both within the organisation and the Cloud provider, the necessary colleague training and awareness campaigns are in place. As part of the due diligence and contract, the organisation ensured that the training within the Cloud provider covers key areas including legislation and regulation
- a skills analysis has been performed and suitable recruitment, retention and success planning is in place
- salaries are market rate and in line with competition.

6. Governance

Potential impact

- the organisation has failed to implement suitable governance over Cloud usage.

Potential responses

- there are suitable roles and responsibilities in place within the organisation which have clear accountability and responsibility for Cloud
- the organisational structure has been reviewed in line with introducing Cloud provision and any necessary changes have been made
- management oversight has been extended to cover all necessary elements of Cloud and any existing governance meetings and reporting also encompass Cloud operations
- existing policies and procedures have been reviewed and updated to encompass cloud
- any new cloud specific policies and procedures required have been approved, implemented and communicated to the required parties
- all compliance monitoring activity has been extended to include Cloud
- all risk management activity has been extended to include Cloud at both first and second line (where there is a second line)
- internal audit activity includes cloud within the audit universe and risk assessment processes.

7. Operations

Potential impact

- the existing IT operations (and business operations where required) have not been extended to encompass Cloud and separate processes have been put into place leading to inefficiencies and poor control.

Potential responses

- all existing IT and business operations have been reviewed considering utilisation of Cloud and existing processes and controls have been extended to include Cloud. This includes but is not

limited to:

a. IT operational monitoring
b. incident management and analysis
c. business continuity and disaster recovery
d. supplier management
e. financial management and cost monitoring
f. procurement.

8. Third party management

Potential impact

- utilising Cloud providers is effectively outsourcing elements of IT to varying degrees. Inability to effectively manage key strategic outsourcing relationships damages the commercial proposition of the organisation.

Potential responses

- the organisation's procurement processes are robust to ensure that the right supplier is selected
- suitable due diligence is carried out on all prospective suppliers to ensure that the organisation's required standards can be met
- the legal representatives of the organisation are suitably experienced in dealing with large suppliers such as Amazon and Microsoft
- the contracts in place protect the needs of the organisation
- where the organisation cannot secure like for like contracts across all strategic suppliers due to the larger scale of some of the suppliers, suitable controls are in place to be able to easily collate the different key contractual terms which need to be included in monitoring and supplier management
- relationship managers are in place to manage all strategic supplier relationships both within the organisation and the Cloud provider who are conversant with the details of the contracts and schedules
- regular supplier management meetings are in place, with the frequency prescribed through a risk-based approach
- where 'right to audit' terms cannot be included in contracts or are difficult to exercise, the organisation must regularly receive the outputs of any appropriate certifications such as ISO27001, or receive the results of independent third party audits
- suitable management information/reporting packs should be in place and regularly monitored to ensure the supplier is meeting the service level agreements specified within the contract. Any issues of poor performance should be managed according to the pre-agreed protocols.

Resource skills and expertise

In alignment with Standards 1210 Proficiency and 1220 Due professional care, internal auditors must possess the knowledge, skills and other competencies needed to perform their individual responsibilities.

The internal audit activity collectively must possess or obtain the knowledge, skills and other

competencies needed to perform its responsibilities.

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor.

Whilst some Cloud scope areas are more generalist such as supplier management, some of the more complex areas such as encryption which may require skills to be bought in eg co-sourcing.

Challenges auditing the Cloud

As Cloud services are provided by third parties, there can be challenges auditing areas that are under the control of third parties, particularly for large Cloud providers such as Microsoft and Amazon who have more commercial power than most of their clients. In these instances, internal audit may need to gain assurance from other sources such as external certifications; it may not always be possible to include or exercise 'right to audit' clauses.

If involved in the procurement stages, internal audit can provide recommendations as to the contractual requirements for gaining assurance and can ensure that the first line of defence implement sufficient oversight controls through robust supplier management. In addition, internal audit can work collaboratively with the business to help ensure control by design throughout the process and provide useful impartial expertise and input.

Conclusion

Depending on the stage of the journey each organisation is on, for an organisation where Cloud use is prevalent, internal audit should include Cloud as another infrastructure layer, and should aim to include Cloud and 'on premise' controls for key risk areas in the IT audit universe. Often organisations set up their Cloud capability and controls as separate entities to their on-site activity, which can be inefficient and lead to unnecessary costs. Where organisations are earlier on in the journey, internal audit can focus on ensuring robust assessment and change planning are in place to ensure a smooth transition.

Further reading

Standards

1210 Proficiency

1220 Due professional care

The National Institute of Standards and Technology (NIST)

Definition of Cloud Computing

Cloud Computing: A Review of Features, Benefits, and Risks, and Recommendations for Secure, Efficient Implementations

International Standard

17788 Information technology – Cloud computing - Overview and vocabulary

17789 Information technology – Cloud computing – Reference architecture

ISACA

Controls and assurance in the Cloud: Using COBIT5

Guiding Principles for Cloud Computing Adoption and Use

KPMG

Moving to the Cloud – key considerations

Journey to the Cloud – The creative CIO agenda

Deloitte

Creating a Cloud strategy

Maintaining control in the Cloud

PwC UK

Compliance in the Cloud – embracing the new normal

Contracting effectively for Cloud-based services

Moving to the Cloud: Governance and Planning

Financial Conduct Authority – Senior arrangements, systems and controls – Chapter 8 - Outsourcing

National Audit Office – Guidance for Audit Committees on Cloud Services

Cloud Security Alliance