Cloud computing governance

Audit leaders have a role to ensure their audit committee maintains pace with important issues and key developments. Cloud computing has been around a while but do our boards understand the risks and assurance needed?

Cloud computing is an area where internal audit can offer a blend of consultancy and assurance services. The trusted advisor position enables audit leaders to engage and educate board members at the same time as constructing an assurance programme that protects and informs.

Statistics published by Eurostat in 2018 suggest over 41.9% of UK business uses some form of cloud service, against an EU average of 26.2% with usage more common in large organisations.

Audit committee guidance published by the National Audit Office suggests questions to consider asking at all stages: assessment, implementation and management. Auditors can also use these as part of audit engagement planning.

We draw on the NAO insights and consider actions for audit leaders.

Competent governance

The word ‘cloud’ creates a sense of mystery yet it refers quite simply to a centralised data centre operated remotely by a third party and accessed via the internet. Cloud computing undoubtedly sounds slicker than outsourced hardware, software and storage but adds to its ambiguity.

Although cloud computing is now commonplace in many organisations, can the same be said for the governance surrounding it? Has it kept pace?

Bruce Schneier, security expert, said "*the internet is no longer a web that we connect to. Instead, it's a computerised, networked, and interconnected world that we live in*." Organisations that engage in cloud computing epitomise this; it is a dependent relationship.

Governance leaders need sufficient knowledge to appreciate the opportunities/threats that cloud technology delivers and most importantly the required oversight. The IT function is no longer the gatekeeper for all technology.

How well informed is your audit committee?

Do they know which questions to ask?

Are assurance gaps understood and challenged?

Every audit committee should know…

Those with oversight accountability, the audit committee, should know the basics before getting caught up in the promises of agile, innovation and efficiency.

- Generic benefits are financial, operational and strategic. Cloud computing provides the means to lease rather than invest in rapidly depreciating technology assets.
- Generic disadvantages are loss of control and flexibility over system functionality, system downtime, data location and security concerns.
- Capabilities to manage cloud computing are a complex blend of supplier relationship management, procurement disciplines and technical expertise.
- Realisation of benefits is not straightforward. Commonly issues relating to ways of working, skills, culture, and legacy systems need to be addressed

The **three types of cloud service** in order of increasing risk

1. Cloud Hosting/Infrastructure as a Service (IaaS): External hosting of only the hardware and servers, the operating systems and applications themselves remain internal to the organisation
2. Cloud Hosting/Platform as a Service (PaaS): External hosting of everything except the software itself which the organisation runs itself
3. Cloud Software/Software as a Service (SaaS): External hosting of everything, the organisation operates nothing itself

Other terminology may also be used adding to the confusion such as cloud support which could apply to any of the services.

The **four types of cloud** in order of increasing risk

1. Private Cloud where the provider gives sole use to resources to one organisation
2. Community Cloud a private cloud shared with selected partners
3. Hybrid Cloud a combination of public and private
4. Public Cloud where multiple organisations share common hardware, storage etc

According to 2018 Eurostat statistics, the rate of adoption of public cloud services at 40% is higher than private at just 31%; Office 365 and DropBox are examples of public cloud.

Are these things your audit committee understands?

Do they understand the risks associated with the different options?

Assessment of cloud services

Cloud services are a highly competitive marketplace and differentiation tactics can add to the complexity of decision making. Organisations should define their digital strategy, including policy on the use of cloud services. This should be based on the needs of the organisation and the boards risk appetite.

Selecting the right cloud services is critical. Business cases often focus too heavily on the positives, the audit/risk committee should be sufficiently challenging to recognise threats/opportunities and gain assurance over their management.

Public sector organisations must also consider compliance with requirements of the G Cloud Framework for procuring cloud services. Audit leaders in other sectors may also find this useful.

Some questions audit committees could ask of management….or expect assurance to cover		
Cloud Strategy	**Business Case**	**Due Diligence**
Are operational realities clearly understood?	How sensitive are costings to future scenarios in respect of change, volume etc?	How is accountability allocated between our organisation and provider, particularly re GDPR?
How does the strategy/policy sit with our appetite for risk?	What does the skills gap look like for managing and using the proposed service? And how will it be closed?	Have features been verified, reference site/user group visits taken up or are we early adopters?
Has the complexity of migration away from legacy systems been thoroughly evaluated?	How long are we intending to commit to? Do we have break clause options?	What are the legalities of where the data will be physically held? Where is the infrastructure located?
Can all the technical requirements be met? Is our internet speed fast enough?	What operational contingency costs are included? Transfer to another provider, returning to in-house.	What aspects of the infrastructure have been tested?
To what extent has non-system change been considered – ways of working, people, culture?	Going forward can the organisation influence the prioritisation of developments?	Will the provider use independent auditors to provide their Service Organisation Controls reports?
What are the implications for our data security?		What are the exit options, including any penalty clauses?

Implementation of cloud services

Governance leaders can take comfort that the challenges associated with implementing on-site systems are

relatively similar for cloud services. Consideration must also be given to vendor management and cultural change. Culture is important as cloud services are often an enabler for changing how people work; empowerment, location, agility and collaboration.

Some questions audit committees could ask of management….or expect assurance to cover		
Configuration	**Risk and Security**	**Implementation**
Have all relevant business experts been involved?	Have technical risks been documented with clear ownership and mitigation?	Have all pre-implementation checks been successfully completed?
What commitment has the provider given to working collaboratively?	Are all legal, regulatory and policy agreements in place?	Have all testing scenarios been executed and issues addressed?
Have legacy systems and data been prepared for the transition?	Are sufficient plans in place to cover a data loss event?	What cultural change does this introduce and are people sufficiently engaged?
Are we over-reliant on the provider or are we enabling corporate memory?	Have financial controls been tested for robustness and compliance?	How will the transition be managed? What contingency exists if implementation issues arise?
How engaged and ready are users/stakeholders?	Have business continuity plans been updated to include new outage scenarios?	Is there sufficient information for a Go/No Go decision to be made?

Management of cloud services

Different skillsets are required to manage cloud services than those traditionally employed to manage in-house services. Organisations retain accountability for governance of data and transactional controls, particularly financial. Risk accountability is always retained never transferred.

Some questions audit committees could ask of management….or expect assurance to cover		
Operation	**Assurance**	**Capability**
What temporary workarounds are still in place that impact data, security or require manual interaction?	Does management have sufficient understanding of the various Service Organisation Controls reports?	How is knowledge-sharing operating in practice with the provider?
Is governance in place to evaluate the impact of new development on the business?	Is the assurance in place able to keep up with the pace of change?	Do our legacy teams have the skills to manage the interface and also leverage new opportunities?

Are responsibilities clear for managing updates, change impact etc?	Is the providers assurance comprehensive or should further assurance be obtained?	Is there adequate legal and commercial expertise to challenge value for money and compliance?
How do we know we are realising the business benefits of the cloud services?	What assurance is needed to cover internal processes and systems?	How will SLA breaches be identified and managed?
	How do we agree, monitor and progress remedial actions with the service provider?	Are decision-makers appropriately informed and engaged about cloud capabilities?

Role of audit leaders

We highlight five potential areas that could help to educate the audit committee and improve governance whilst also providing valuable assurance.

1. Cloud Governance

Few individuals outside of the board have the insights of chief audit executives (CAEs). Thinking about your conversations and observations on the topic, what is your impression of the board's understanding regarding cloud computing?

Would it be useful to share the NAOs guide (or an adaption of) with them?

Could they benefit from an informative session by the head of technology/external trainer?

The cloud computing model disrupts traditional governance. It removes reliance on the IT function and facilitates individual managers to identify needs, negotiate contracts and implement services without safeguards. Cloud governance is wide-ranging, from technical standards and procurement protocols to human resource for changing job profiles.

What governance assurance has been provided to your board in relation to cloud computing?

2. Cloud Strategy/Policy

A governance audit may touch on strategy, particularly recommending one if it is absent.

Where strategy/policy exists, either informally or formally, assurance should be provided over the process used to develop it.

Without having defined clear strategic intent for cloud services, organisations can find themselves inadvertently exposed to risk beyond their appetite.

The Technology Code of Practice is a set of criteria to help government design, build and buy technology but it is a useful document for auditors across all sectors.

3. Vendor Management

It may be necessary to provide the board assurance explicitly for cloud vendors. Processes have to be

sufficiently flexible and robust to manage a wide variety of vendors from niche start-ups to large scale operations. It is relatively straightforward for non-technical managers to deal directly with cloud vendors.

Internal audit could help evaluate the many facets of cloud vendor management (link to short practical summary) including the pros and cons of centralised vs decentralised management, the organisations expertise in managing partners/outsource arrangements and the maturity of processes.

4. Business Resilience

Organisations with a dependency on cloud services for critical activities may value independent assurance on resilience. Short-term continuity planning is different to long-term resilience. Cloud computing may improve an organisation's resilience or create new exposures.

The question of where internet cables are laid becomes much more important when the organisation cannot operate without it. Some countries are at higher risks of intentional national internet shutdown than others which could impact operations. A 2018 report by Freedom House found India at the top of the list with over 100 instances due to riots, terrorism and to prevent the spread of misinformation. Look at the report – do some of the countries your organisation relies on feature in the top 10?

A breach of service level agreement by a cloud vendor for data security or service downtime could be a moot point for lawyers long after the organisation's doors have closed. Has business resilience/continuity assurance adapted with the pace of technological change within your organisation? How meaningful is the assurance you give your board?

5. Third Party Auditing

Audit leaders may want to consider creating an assurance map specifically for cloud services. Clear delineation between the first and second line may help to ensure that amid the complexity all necessary activities are accounted for without duplication. Likewise a RACI for key contracts or governance in general could be useful to ensure responsibility and accountability is clearly understood.

What role should internal audit play?

Is it enough to test and validate the efficiency and effectiveness of risk management activities?

Should internal audit independently audit high risk vendors?

Closing Thoughts

Audit leaders can find themselves caught into the detail of providing assurance on new systems and validating compliance checks. Perhaps now is the time to take a moment to step back, build on your partnership with the audit committee and look at the broader picture of cloud governance.

"Cloud is about how you do computing, not where you do computing"

Paul Maritz, computer scientist