Committee and Date	Item
Audit Committee 15th September 2022	Public

Assurance on the Internal Controls and Risk Management of the Council's Cloud Services

Responsible Officer James Walton
e-mail: james.walton@shropshire.gov.uk Tel: 01743 258915

1. Synopsis

The Council uses cloud-based services in a range of ways. This report is a survey of the current position regarding internal controls and risk management for cloud-based systems.

2. Executive Summary

2.1. This report identifies the current use of cloud-based services by the Council and considers its use of these systems (including wider networks and data centres) to house its data and network systems. It focuses on the approach to assurance for internal controls and risk management for these services.

2.2. This is increasingly important in the context of the rise of cyber security threats and the need to safeguard our data and systems and ensure their ongoing operation.

2.3. The report also considers the current position in terms of consistency of approach across different types of use of the cloud, and invites the committee to comment on the desirability of increased controls and risk management and consistency how these are being applied.

3. Recommendations

3.1. That Members of the committee consider the treatment of different systems and services accessed by the Council and the extent to

which they are 'cloud-based', and the approach to risk management and system security that is in place for them.

3.2. That Members of the committee consider further measures that may be appropriate, or areas for further measures that they may which officers to look into.

REPORT

4. Risk Assessment and Opportunities Appraisal

4.1. No new risks or opportunities arise directly from this report.

5. Financial Implications

5.1. None arising directly from this report.

6. Climate Change Appraisal

6.1. None arising directly from this report.

7. Background

7.1. Shropshire council utilises many cloud-based systems to provide services internally and externally to our citizens and partners.

7.2. The Council has a mix of cloud service types in use:
a) **public cloud** such as the Councils investment in Microsoft Office, Azure and Power platform products.
b) **private cloud** such as the social care Liquid Logic system.
c) **community cloud** such as the Integrated Care Record that operates with health partners and councils across Shropshire, Staffordshire and West Midlands.

7.3. Hybrid cloud which is the current in house provided ICT services model and is a mix of local Infrastructure and software services that operate like a private cloud but also integrate with external cloud-based elements to provide a unified service. So, the hybrid cloud service is a service delivered with some service aspects being in a private cloud, other aspects being in a community cloud, and some elements being delivered from within local, on-premise hardware (so not in the cloud).

8. Additional Information

8.1. In recent years, we have collectively talked about use of 'the cloud' in relation to ICT activity. The cloud can be defined as "the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. Large clouds often have functions distributed over multiple locations, each location being a data centre."[1] Another definition highlights the link to 'real world' data centres: "The cloud is made up of servers in data centres all over the world. Moving to the cloud can save companies money and add convenience for users."[2]

8.2. The Council operates a variety of combinations of cloud-based and premises based solutions for different data systems. These are set out in more detail in the appendix to this report, together with the risk management approach in place for each.

9. Conclusions

9.1. The Council has an integrated approach to systems management that does not differentiate between cloud based and premises-based systems. Risk management approaches have due regard to the different way IT services are delivered but aim for the same standards of governance in all cases.

9.2. In the context of increasing risks around cyber and interconnected networks, it is timely to consider our approach and whether it may in some areas benefit from increased levels of attention and assurance, considering costs and benefits together.

[1] Cloud computing - Wikipedia
[2] What is the cloud? | Cloud definition | Cloudflare

List of Background Papers (This MUST be completed for all reports, but does not include items containing exempt or confidential information)

NA

Cabinet Member (Portfolio Holder)
Cllr Rob Gittings

Local Member
NA

Appendices

Appendix 1 – detailed report (plus attachment)

Appendix 1 – detailed report regarding Assurance on the Internal Controls and Risk Management of the Council's Cloud Services

1 Shropshire Council – current position

Approach

1.1 The Council adopts a 'Cloud where appropriate' approach. This means that on- premise and cloud options should be considered equally to find the best value and efficiency at the time of procurement. Cloud pricing models have altered significantly in recent years.

1.2 For specialist lines of business applications, hosted or cloud solutions increasingly offer both best value and optimum feature sets against on non-cloud/on-premise options. Many recent cloud offerings have also not been mature enough or have had unrealistic pricing models when compared with on premise hybrid provision. We continue to select options based on best value, but review options as well given the pace of change in this area.

1.3 As business systems (including legacy systems) are reviewed, often software and system vendors can now offer cost effective cloud solutions that - only a few years ago - were not available or too expensive compared to the local alternative. With the passage of the procurement cycle more and more systems are organically and naturally transitioning to the cloud.

2 Risk management

2.1 The council has always endeavoured to ensure its ICT systems are secure and compliant. In recent years the growing risk of cyber attack has led to increased focus on this area and increased the level of assurance we have sought.

2.2 Importantly, many of the same safeguards are applicable for both cloud and non-cloud systems, such as standards of good practice and data safety applies.

3 Safeguarding and securing Cloud systems.

3.1 With the increasing risk of cyber-attack the council has implemented extra protection activity including the creation of a new decision making and actions group (Safety and resilience) to address review and address identified weaknesses in council systems.

3.2 This group helps coordinate safeguarding activity such as audit recommendations, supplier advisories, proposed service

improvements to ensure a focussed approach to securing council systems.

3.3 The council also undertakes a number of activities to safeguard its systems such as identifying and managing service area and strategic risks via the council's risk management system. Additionally, our internal audit service undertakes frequent audit activity to identify areas of weakness or possible improvement to cloud and on-premise service provision.

3.4 The council is now implementing enhanced, detailed vulnerability testing, which is replacing our existing capability to identify new or existing system vulnerabilities that can be patched or mitigated. Further, a 24/7 external security response service is being engaged (currently at trial stage) to monitor council systems and alert for signs of cyber-attack.

3.5 Lastly, the council continues to have a specialist in-house security team monitoring and managing the security of our systems. The team also provide advice and support for new and existing cloud-based system provision.

4 Data protection

4.1 The council has a dedicated data protection team who consult and advise business areas around data protection obligations for new and existing systems.

4.2 All systems must meet legislative requirements around data security including the data protection bill. It is advised that business areas complete Data privacy Impact assessments (DPIA) before undertaking procurements to understand the implications to sensitive data. It is a requirement that a DPIA is completed before new system go live so that all proper data protection activity is undertaken.

4.3 As cloud based or other ICT systems are created then they can become new data assets and there is a central register of such assets that is overseen by the data protection team.

4.4 Information asset owners and system administrators are required to ensure their data assets are protected and secured by their suppliers in line with contractual obligations.

4.5 For ICT provided systems a business case for a new modern backup solution is being created to safeguard the hybrid model council systems operated by ICT.

5 ICT Security

5.1 Vendors' products should meet best practice security controls, NCSC cloud principals and be ISO 27001 accredited in relation to their delivered services. ICT provide expert advice on the security of cloud-based systems being able to assess the detailed security capabilities of each vendors solution. The team also can assess adherence to NCSC cloud principals and other guidance against a vendor's provision.

5.2 It is strongly advised that all new internet facing systems have an independent external penetration test carried out to confirm that systems are secure before they go live. These often highlight issues with a vendor's solution that require attention before a system can fully go live in a compliant manner.

6 Legislative compliance

6.1 By law all council provided ICT systems must comply with the equalities act of 2010 and cloud-based solutions are no exception. In some cases, this element of solutions delivery is not well understood in the industry and so the council works with providers who are not compliant to advise on the required changes before systems are procured or implemented.

6.2 The council has in house expertise within the Digital services team who frequently undertake disability access assessments and advise on any issues to business areas and vendors.

6.3 As mentioned under data protection council systems must adhere to UK legislation such as the data protection bill and it is the responsibility of the system owners to ensure this, and disability access are adhered to.

7 New system procurements.

7.1 Whenever a new ICT system is procured it is required that the council's procurement rules are followed and the council's procurement team advise on suitable evaluation and procurement methods.

7.2 The team are aware of the other requirements of ICT systems delivery and will direct business areas to ICT and data protection teams to help ensure solutions meet policy and legislative requirements.

7.3 When a business area proposes a new system it should engage with the ICT security, data protection and digital services teams who can help the system owners ensure their systems meet corporate policy, best practice and legislative requirements.

7.4 Potential suppliers are assessed against the NCSC cloud principals, PSN code of connection, disability access, data protection, best practice and corporate policy.

7.5 The key elements of delivery are examined such as secure connection, rights and access management, patching schedules, data storage and protection, cost models, location of the datacentres, security accreditations, legislative compliance

7.6 The on-going management and administration of the system and contract should also be considered for the elements of supplier support, incident handling, service levels, exit arrangements, business continuity and disaster arrangements, dispute handling and assurance activities such as penetration testing or audits.

8 Information governance process

8.1 The council has an information governance process that can be required to provide a governance input when issues or concerns arise with a new ICT systems procurement.

8.2 Sometimes issues exist with a systems implementation such as disability access non-compliance or technical security concerns that must be considered against business benefit.

8.3 Such concerns when framed as a business risk allow a mature discussion at the appropriate managerial or executive level balancing business gains versus potential risks.

8.4 Often at times appropriate mitigations or the risk profile of the system is low such that an element of risk can be accepted where a system fails to meet the required levels of assurance.

9 Systems Implementation

9.1 Once a system has passed the assessment and procurement activities the system can be implemented. Cloud based systems fundamentally rely heavily on the supplier to guide and direct the implementation process. Depending on the type and scale of the system various stakeholders and activities must be undertaken.

d) Detailed design
e) Data upload
f) System integration
g) Connectivity
h) User management
i) System administration
j) Incident handling process

k) Security configuration
l) System and user testing

10 Management of existing systems

10.1 As indicated the Council has a mix of cloud-based systems and each requires suitable controls to be in place for the efficient on going management of that system.

10.2 The attachment to this report sets out indicative examples of the requirements of managing each type of service delivery.

10.3 Members are invited to comment on areas where they consider that additional controls may be appropriate, or further review work merited.

Attachment – summary of key systems, on/off cloud location, and risk management

1 Enterprise Public cloud: Microsoft Office, Azure and Power Platform products.

1.1 This type of service provides a very largescale multiuser set of vendor defined services capable of servicing thousands of customers simultaneously. The vendor provides these defined services in accordance with their own business and technology development plan.

1.2 Customer's data is protected but the overall system delivery is shared by the general user base.

1.3 Performance of the cloud system is not guaranteed and at times overall performance can be degraded. This delivery is heavily reliant on the vendors expertise and competence. The relationship is fundamentally in the vendors favour as there is no scope to alter or challenge contract terms. Only high reputation firms are considered as the scale of risk to the organisation is potentially so high.

1.4 To further reduce potential risk the Council has invested in extended support with Microsoft which provides enhanced troubleshooting and support above the normal public support level.

1.5 Public cloud offerings have major business benefits but also bring increased challenges as the vendor can alter service capabilities without regard for the council's use of those services. To mitigate this where possible ICT manage the relationship with the supplier maintaining a close dialogue is essential to understand and prepare for the service impacting changes.

1.6 As we leverage the ever-increasing capabilities of the Microsoft product set 'lock in' is a fundamental risk due to the scope nature and adoption of their technology within the council. This is not a Microsoft issue as other public cloud vendors such as Googles product sets also inevitably lead to a reliance on your chosen partner of choice.

Enterprise Public cloud: Responsibility and accountability

- Supplier contract management: ICT
- Supplier relationship: ICT
- System Management and administration: ICT
- Connectivity: Vendor, ICT
- Data safeguarding: Vendor, ICT
- Data asset responsibility: Information Asset owners relevant to the information

- System integrity: Vendor

2 Private cloud: Social care Liquid Logic, Planning IDOX system

2.1 In this model the vendor creates a specific environment for the customer to deliver the application, both the data and the application are segregated from other customers.

2.2 Performance of the system is more predictable as the service is designed for the capacity of the customer.

2.3 This model provides most control and flexibility around the delivery of services and systems and allows only high level of risk management.

Private cloud: Responsibility and accountability

- Supplier contract Management: Business area
- Supplier relationship: Business area
- System Management and administration: Business area system administrators
- Connectivity: Vendor, ICT
- Data safeguarding: Vendor
- Data asset responsibility: Information Asset owners relevant to the information
- System integrity: Vendor

3 Line of business applications via the public cloud: Fix my street, HAF, Registrars system

3.1 In this model the vendor provides a system as a service using a shared cloud rather than a dedicated environment for the customer. Performance can be unpredictable dependent on the service use.

3.2 Customer data is protected but the overall system delivery is shared by the general user base.

3.3 This model provides less control and flexibility around the delivery of services and systems and allows only a low level of risk management.

Line of business applications (public cloud): Responsibility and accountability

- Supplier contract Management: Business area
- Supplier relationship: Business area
- System Management and administration: Business area system administrators
- Connectivity: Vendor
- Data safeguarding: Vendor

- Data asset responsibility: Information Asset owners relevant to the information
- System integrity: Vendor

4 Hybrid cloud: Pensions system, Ivanti service desk system, ICON payments system

4.1 This is the current in house provided ICT services model and is a mix of local infrastructure and software services. It operates like a private cloud but also integrates with external cloud-based elements to provide a unified service.

4.2 This model provides a great deal of control and flexibility around the delivery of services and systems and allows a greater level of risk management.

Hybrid cloud: Responsibility and accountability

- Contracts Management: ICT
- Supplier relationship: ICT
- Infrastructure management: ICT
- System Management and administration: Business area system administrators
- Connectivity: ICT
- Data safeguarding: ICT
- Data asset responsibility: Information Asset owners relevant to the information
- System integrity: ICT