SUPC
Southern Universities
Purchasing Consortium

Navigating the Cloudscape: Unleashing the Power of SaaS

By

Mark Lewis, ICT Category Manager, SUPC

Navigating the cloudscape: Unleashing the power of SaaS

As more businesses embrace cloud technology, businesses are leveraging the numerous advantages offered by Cloud Software as a Service (SaaS) providers. This shift not only offers potentially a better optimisation of IT resources but also allows access to the virtually limitless flexibility inherent in cloud solutions.

Engaging with these providers strategically is essential. When meeting a cloud SaaS provider, it's important to ask specific questions to ensure their service aligns with your business needs.

This guide is designed to help you navigate the cloudscape by reviewing some key challenges of migration to cloud technology including:

SUMS Consulting, Procurement Shared Service and SUPC are operating units of Southern Universities Management Services a company limited by guarantee. Registered in England and Wales No. 02732244 Charity Number 1042175 Registered office: Reading Enterprise Centre University of Reading, Earley Gate, Whiteknights Road, Reading, RG6 6BU

1.0 Pivotal considerations

For some time now, data privacy and compliance have been pivotal considerations for organisations. This includes a focus on the importance of safeguarding your storage and taking a more holistic view of security measures.

1.1 Safeguarding your storage

GDPR mandates that data collected on citizens must be stored in the EU or in jurisdictions with comparable privacy protection. This regulation applies to both data controllers and processors, directly impacting organisations utilising or offering cloud services that process data of EU residents.

The primary public cloud giants, namely Microsoft, AWS, and Google, have built European data centres to manage concerns and ensure compliance. In contrast, many secondary and tertiary SaaS cloud vendors may either provide a limited number of data centres or, if relying on major cloud providers, utilise only a limited number of their data centres.

In addition, it's worth noting that certain countries, such as Germany and France, have stringent mandates, requiring their citizens' data to be stored exclusively on physical servers within their national borders. This can lead to issues where data is regularly transferred between locations and therefore makes it difficult to ensure adherence to applicable local laws.

Another consideration in terms of data privacy is that organisations may, in addition to legal and regulatory compliance, offer an additional layer of assurance and/or safeguards to the privacy of personal data. There will naturally be an expectation that that such privacy commitments will continue. However, this may not be the case and especially if the provider operates in numerous jurisdictions.

1.2 A holistic approach to security

Nevertheless, it is crucial to acknowledge the significance of the entire supply chain, necessitating a comprehensive approach to the security of partners at every level. Partners should be asked to evidence their commitment by:

1.2.1 Business continuity and information security plan

Ensuring they (the vendor business Software as a Service (SaaS)) have a continuity plan in place to ensure the resilience and reliability of services in the face of unforeseen disruptions. There are a number of critical considerations to consider when evaluating a SaaS business continuity plan.

1.2.2 Adherence to global standards

Adhering to the globally recognised standards, ISO22301 (Business Continuity) ISO27001 (Information Security Management System) and ISO27017, (information security controls applicable to the use of cloud services), that set rigorous standards for operating within a secure environment.

Organisations can find assurance in the knowledge that the vendor, if adhering to the standards, is complying with established security protocols and has validated their adherence through regular assessment.

1.2.3 Risk management strategy

Implementing a robust risk management strategy, that extends beyond the organisational level to encompass the entire supply chain will ensure proactive oversight at the Board level. This will enable a thorough examination of risk controls and their alignment with business operations throughout the supply chain.

1.2.4 Location understanding

Evidencing a clear understanding of the locations where data is stored within the supply chain, ensuring transparency and accountability in data management.

1.2.5 Regular testing:

Undertaking regular testing, facilitated by third-party auditors, including:

- Regular vulnerability and penetration testing, including assessments of supply chain partners.
- Operational testing to evaluate the effectiveness of security measures.
- Incorporation of lessons learned and continuous improvement mechanisms to adapt to evolving business environments and emerging threats.

By recognising the pivotal role of the entire supply chain, organisations can foster a holistic approach to security. This approach goes beyond immediate operations, ensuring that security considerations are integrated into every facet of the extensive network of entities involved in the supply chain.

2.0 Exit planning

This may seem out of place here as the expectation is that there will be a long and fruitful relationship between all parties, but consideration should be given to what happens when the relationship ends.

Creating an exit plan for SaaS (Software as a Service) software is a crucial aspect of managing technology transitions, vendor changes, or unforeseen circumstances. An exit plan helps ensure a smooth transition out of the current SaaS arrangement.

An initial review of the current contractual terms is always a good starting point. As this allows understanding of termination clauses, notice periods, and any financial obligations tied to termination, although typically most clauses are boiler plate and will only have a general requirement to provide support to between the parties.

2.1 A good exit plan – What's included?

A good exit plan should always be relatively up to date. And should include:

2.1.1 Defined roles and responsibilities

Understanding who is responsible for what and how.

2.1.2 Data migration strategy

Developing a comprehensive Data Migration Strategy is a pivotal step in orchestrating the seamless transfer of data from the existing Software as a Service (SaaS) platform to a new environment. It is about creating a clear plan for moving data from the current SaaS platform to a new one. This involves figuring out of where the data is located, which data is essential, making sure it stays accurate, and using the right tools for the move.

2.1.3 Costs identification

Identifying and categorising all potential costs related to the exit plan is frequently overlooked. It can come a bit of a surprise when the outgoing supplier sends a quote of £000's to cover their costs for supporting the transition of data from their system to the new supplier. Costs should include direct costs such as termination fees, data migration expenses and unexpected technical issues.

2.1.4 Deletion of data

Implementing procedures for the secure deletion of data from the current SaaS platform, adhering to data protection regulations. Incorporate security measures to safeguard sensitive information. It is important to ensure that local laws and rules regarding deletion are fully understood and complied with. After deleting data, thoroughly check to make sure all identified data is gone securely.

2.1.5 Escalation procedures

Developing an Escalation Procedure to provide a structured framework for addressing and resolving issues that arise during the exit process, ensuring timely and effective escalation to the appropriate levels of authority.

2.1.6 Support for the new supplier

Ensuring robust contractual support with the both the outgoing and new supplier is crucial for a smooth and secure transition.

3.0 Service Level Agreements

It is important to have in place clear Service Level Agreements (SLAs) that outline the standards that will be applied for the services provided. Having clear and simplified SLAs ensures everyone is on the same page and helps maintain a reliable partnership with the SaaS provider.

3.1 Key service levels to include within an agreement

3.1.1 Uptime and availability

Specify when the system should be operational, to help ensure minimal disruptions to your work. For critical business functions, a high uptime percentage is typically required to minimise disruptions.

3.1.2 Response times

Set a maximum time for the provider to acknowledge and respond to your inquiries., to ensure quick assistance and the prompt addressing of concerns related or user inquiries.

3.1.3 Resolution times

Set a maximum time for the resolution of issues, to help ensure that the SaaS provider will adheres to industry standards and legal requirements, safeguarding sensitive data against unauthorised access or breaches.

3.1.4 Scalability and performance

Outline expectations for the system's performance, especially during high-demand periods, to help ensure that the system maintains optimal performance even during periods of high demand.

3.1.5 Data security and compliance

Clearly state expectations for data security, encryption, and compliance with regulations. This SLA is crucial for minimising downtime and disruptions to business operations.

3.1.6 Backup and disaster recovery

Specify how often data will be backed up and the time it takes to recover data in case of a disaster, to ensure that data is consistently backed up, and there are robust measures in place to recover data in the event of an unforeseen incident.

3.1.7 Software updates and maintenance

Clarify the schedule for software updates and routine maintenance to manage expectations. This SLA helps manage expectations regarding system downtimes during maintenance activities and ensures that the SaaS provider keeps the solution up-to-date.

3.1.8 Customer support and communication

Define expectations for customer support responsiveness and communication during issue resolution. This ensures a transparent and responsive support process.

3.1.9 Data ownership and portability

State terms for data ownership, portability, and data retrieval upon termination of the agreement. This is essential for ensuring that your organisation retains control over its data and can transition seamlessly if needed.

3.1.10 Service termination and transition

Outline conditions for ending the service, notice periods, and support during the transition to a new solution. This SLA facilitates a smooth exit strategy if required.

Engaging with providers requires a meticulous approach, marked by careful considerations and specific inquiries to ensure a seamless alignment with business needs.

4.0 The cloud's the limit, but at what cost?

Implementing SaaS can have a significant impact on costs and the organisation's financial position. An organisation will need to determine whether SaaS associated costs should be expensed as incurred (through the recurrent budget) or be capitalised, and thereafter consider affordability given the organisation's financial position and challenges.

Cloud-based software ranges from simple application software to complex solutions like ERP systems that usually involve significant implementation costs. Accounting for implementation costs depends on whether the cloud-based software classifies as a software intangible asset or a service contract. Potentially many implementation costs for cloud service contracts will need to be expensed as incurred.

The total (implementation and recurrent) associated costs of cloud migration need to be compared to the capital expenditure required for investing in new hardware, software, or infrastructure. SaaS adoption can give more flexibility to the balance sheet.

Cloud computing can be perceived as the advantageous "pay-as-you-go" model where you do not have to pay for resources that you have not consumed. Cloud services are also typically able to scale-up quickly by upgrading to a plan, with less up-front costs.
An organisation needs to understand the holistic impact of moving to SaaS on its financial position.

5.0 Navigating the complexities of a modern technological landscape

The landscape of data privacy and compliance introduces an additional layer of complexity, demanding strict adherence to regulations such as GDPR and navigating the nuances of in-country data storage requirements. Recognising the critical role of the entire supply chain becomes imperative, urging businesses to adopt a comprehensive security approach substantiated by unwavering adherence to stringent standards.

Business continuity planning emerges as a linchpin for ensuring resilience and reliability, where globally recognised ISO standards serve as tangible evidence of a commitment to maintaining rigorous operational standards within a secure environment. This commitment is further reinforced by robust risk management strategies, board-level oversight, transparent location practices, and regular testing, collectively contributing to a holistic security framework.

Exit planning, often underestimated, takes centre stage in the realm of technology transitions. A well-defined exit plan, inclusive of delineated roles and responsibilities, a resilient data migration strategy, cost identification, secure data deletion procedures, escalation protocols, and seamless support for the new supplier, ensures a smooth and well-managed transition.

In the realm of Service Level Agreements (SLAs), clarity reigns supreme. Essential SLAs covering various aspects, including uptime, response and resolution times, scalability, data security, backup procedures, software maintenance, customer support, data ownership, and termination processes, serve as the bedrock for establishing and maintaining a reliable and mutually beneficial partnership with SaaS providers.

Simultaneously, obtaining direct feedback from current customers enriches the decision-making process, providing invaluable insights into the real-world applications, challenges, and benefits of the technology. While vendor references offer a starting point, tapping into the collective wisdom of institutions connected through networks like SUMS and SUPC can contribute to more informed and well-rounded decision-making, ultimately contributing to the success and effectiveness of the investment. Adopting this holistic approach will position businesses to navigate the complexities of the modern technological landscape with resilience, security, and strategic foresight.