

Off-campus computing models

Purpose

This paper is a guide to business owners to assess the viability of using Off-Campus Computing Models. The guide provides a decision making model and aims to prevent unnecessary completion of risk assessments or associated work in determining feasibility.

Background

Off-campus computing models are those where the IT service (including the application and the data) resides on hardware that the University does not own. Not owning the resources implies that there is no upfront acquisition cost, but rather, that the Provider is paid for the service on a recurring (subscription) basis. In the off-campus IT scenario, there are always two parties involved: the one that provides the resources (**the Provider**) and the one that “rents” them (**the University**).

There are three main off-campus computing models. These models are defined by Gartner as **hosting**, **software as a service** (SaaS) and **cloud computing**.

In the **hosting** scenario off-campus computing resources are allocated exclusively by the Provider to the University. If a provider has such an arrangement with multiple user organisations (eg. other Universities) then each will have its own exclusive computing resources from the hardware up. There is minimal or no sharing of capabilities or costs among the multiple user organisations.

In the **cloud computing** scenario off-campus computing resources are allocated to applications and/or user organisations with elasticity: just-in-time with on-demand and metered quantity and quality (advanced capability). To fulfil this requirement, the Provider must have resources that substantially exceed the average use patterns and therefore mature cloud environments are characterised by massive scalability.

In the **software as a service** (SaaS) scenario off-campus resources are offered in a one-to-many manner: multiple user organisations using the same application, but in a manner such that each user organisation experiences it as if it were the only entity using the application. The one-to-many model can be implemented through multitenancy or isolated tenancy. Multitenancy implies elasticity and therefore, multitenant SaaS is part of cloud computing. Isolated tenancy allocates fixed isolated resources to each user organisation and therefore is a form of hosting.

Issues/Risks Presented by Off-Campus Computing Models

Off-campus computing models can appear attractive however their use can introduce a number of issues/risks including performance and reliability, data integration, data security, end to end service management, availability and disaster recovery, and commercial risk. The independent location of the service and the possibility of the Provider “subcontracting” aspects of the service can result in additional IT risks, legal and compliance issues.

The presence of these risks means that it is important for UniSA to develop a set of decision making principles for the controlled and secure use of off-campus computing models, so that business systems owners know when they are appropriate to use and have a recognised approval process to follow.

Performance and Reliability

Generally speaking the systems that would be considered for running off-campus would be web based, and hence users will have access to it via a web address (URL). To the end user, the product should function from a look and feel perspective the same regardless of where the solution is hosted however if the system is hosted offsite overall performance and reliability cannot be guaranteed. While Service Level Agreements (SLAs) can be put in place between the hosting organisation and the University, performance issues, particularly those that relate to data transmission (network latency, packet loss and routing abnormalities), and the impact of bottlenecks on the internet could be difficult to troubleshoot and resolve.

Data Security

An externally hosted system increases the University's information security risk profile due to the data residing outside of the University infrastructure and security controls. The hosting organisation would have a contractual obligation to provide the level of security required by the University however the implementation of that obligation would need to be monitored and audited by the University.

With off-campus computing models it is not always possible to know where the University's data is kept. With hosting services this is easier to determine than with either SaaS or cloud computing however in an increasingly global environment it might be difficult or even impossible to determine what country the data is kept in. This could have significant ramifications with respect to complying with privacy regulations.

Data Integration

It is likely that at some stage during the life cycle of the system that the University will require access to the application data for integration with other University systems, including into the data warehouse. To provide this access an externally hosted solution would require external data transfer processes to be setup and maintained cooperatively by both the hosting organisation and ISTS.

End to End Service Management

If the system is externally hosted then the co-ordination of technical and end user support is more complex. In an externally hosted implementation incidents or changes affecting either the hosting organisation or the UniSA ICT infrastructure may well affect the operation of the system as far as the end user is concerned. Technical support for the externally hosted implementation would be provided by the hosting organisation with ISTS staff becoming involved in the management and resolution of support incidents only if the University's local ICT infrastructure was a contributing factor.

Generally speaking for most off-campus computing models:

- change management is the responsibility of the Provider and the University may have little control over how changes are managed, including down time windows for changes and maintenance

- access to test and training environments is generally limited and in any case is likely to incur an additional fee
- integration with the University's (Single Sign-On or Same Sign-On) authentication schemes will not be straightforward. This could mean users will need to remember multiple username/password combinations thereby decreasing overall system security and increasing forgotten password queries to the IT help desk.

Availability and Disaster Recovery

If the system is externally hosted, availability is controlled by the Provider and would be governed by contractual Service Level Agreements. Whilst the Provider would endeavour to provide a high level of service, there will be times when UniSA would need to 'fit in' with other customer requirements who are hosted on the same infrastructure. In the case of unplanned outages the University would be reliant on the performance of the Provider to rectify the issue. In terms of disaster recovery the University would need to satisfy itself, both initially and then via regular audit that the Provider's disaster recovery processes and procedures were adequate.

Long Term Viability

If the system is hosted externally, there are further issues to be considered around the ongoing commercial viability of the Provider. Whilst there may be nothing to suggest this is a risk initially there is always a possibility that the Provider could find itself in a situation where the service the University has contracted for is withdrawn at short notice. It would be prudent therefore in the case of an externally hosted implementation for the relevant business owner to maintain a business continuity plan to manage this possibility.

The long-term viability of any external service provider is clearly a key concern. If the Provider went out of business or was acquired it may leave the University in a situation where there was no access to our data or possibly worse even if we could get access to the data it wasn't in a form that we could import into a replacement application hosted internally.

Advantages of Off-Campus Computing Models

Despite the presence of significant risks there are situations where off-campus computing models may be appropriate for the University. These situations are likely to be where the risks are outweighed by access to either functionality, capacity, or technology that cannot be replicated internally or where the model offers significant cost benefits. It is likely that this would not be the case for systems which process core student, staff and finance data.

Decision Making Principles

Based on the foregoing analysis it is recommended that off-campus computing models:

- (a) are not suitable for:
- systems which process core¹ student data,
 - systems which process core¹ staff data, or
 - systems which process core¹ finance data
- (b) are not likely to be suitable for:

¹ Core data is considered to be data central to that particular process/function that has privacy or security implications. Ultimately that judgment will be made by the responsible SMG member.

- systems which are critical to the operation of the University
- (c) may be suitable for situations where the model :
- provides access to either functionality, capacity, or technology that cannot be replicated internally
 - offers significant cost benefits.

In cases falling under (b) and (c) above a detailed risk assessment would need to be undertaken, with input from ISTS, before a recommendation is made to IMG for final approval.

The decision logic is summarised in the following flow chart.

