University of South Australia

Information Security Policy

Appendix B: Cloud IT Services Risk Assessment

Responsible Officer:	Chief Information Officer
Last Updated:	July 2021
Date of Review:	July 2024
Audience/Application:	Staff
Related Documents	– Acceptable Use of Information Technology (C-22) – Information Security Policy – Risk Management (C-24)

1. PURPOSE AND SCOPE

All cloud IT services must undergo a formal risk assessment prior to procurement and implementation. This formal risk assessment must be approved by the Chief Information Officer. Cloud based services that are not approved by the Chief Information Officer and/or do not meet minimum standards will be "disconnected" from the University's IT environment.

2. BACKGROUND

2.1 ***Cloud IT services*** are those where the IT service (including the application and/or the data) reside on hardware that the University does not own. There are three main off-variants of cloud IT services: ***hosting***, ***software as a service*** (SaaS) and **cloud computing.**

2.2 In the ***hosting*** scenario IT resources are allocated exclusively by the Provider to the University and there is minimal or no sharing of capabilities or costs among the multiple user organisations.

2.3 In the ***cloud computing*** scenario IT resources are allocated to applications and/or user organisations with elasticity: just-in-time with on-demand and metered quantity and quality (advanced capability).

2.4 In the ***software as a service*** (SaaS) scenario IT resources are offered to 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.

3. RISKS PRESENTED BY CLOUD IT SERVICES

Clous IT services can appear attractive however their use can introduce a number of 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.

These risks must be evaluated and mitigated to an acceptable level before the cloud IT service is procured and implemented.

3.1 Performance and Reliability

Given Cloud IT services are hosted offsite their 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 and reliability are the responsibility of the Provider.

3.2 Data Security

The use of cloud IT services increases the University's information security risk profile due to the data residing outside of the University infrastructure and security controls. The contract with the Provider must impose a contractual obligation to provide the level of security and privacy required by the University and the implementation of that obligation must be monitored and audited by the system owner.

3.3 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. Providing this access requires external data transfer processes to be setup and maintained cooperatively by both the Provider and ISTS.

3.4 Identity and University Credentials

Cloud IT services should utilise University based credentials, providing a single sign on experience through a secure authentication process. Alternatively, if the system maintains unique identity credentials then at a minimum multi factor authentication should be invoked.

3.5 End to End Service Management

For cloud IT services the co-ordination of technical and end user support is more complex. For a cloud 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 cloud IT service 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 cloud IT services:

- 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 is not straightforward.

3.6 Availability and Disaster Recovery

For cloud IT services availability is controlled by the Provider and is 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 that 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 relevant business owner needs to satisfy themselves, both initially and then via regular audit that the Provider's disaster recovery processes and procedures are adequate.

3.7 Long Term Viability

For cloud IT services 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. To mitigate this risk business system owners must maintain a suitable business continuity plan.

The long-term viability of any external service provider is a live risk. 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 if we could get access to the data it was in a form that we could not import into a replacement application.

4. ADVANTAGES OF CLOUD IT SERVICES

Despite the presence of significant risks there are situations where cloud IT services may be appropriate for the University. These situations are likely to be where the risks are outweighed by access to functionality, capacity, or technology that cannot be replicated internally or where the cloud IT service offers significant cost benefits.

Cloud IT services must not be used for systems which process restricted (moderately to highly sensitive) data, or data, which is protected by Federal and/or State legislation.

5. MANDATORY RISK ASSESSMENT

A detailed risk assessment must be undertaken by ISTS and approved by the Chief Information Officer before a cloud IT service is procured or implemented.

A risk identification checklist is available at Annexure A: Risk Checklist for Cloud IT Services.

This checklist must be used to identify risks prior to implementation of a cloud IT service and an assessment of those risks (including appropriate management actions and mitigations) must be included in any business case.

For the life of the cloud IT service, risks associated with the ongoing use of that system must be included in ISTS and the business owners risk management plan. Specific risks should be included to cover upgrades, additions and new versions of the system (whether initiated by the University or by the vendor), and also to monitor assurance reports provided by vendors.

University of South Australia

Annexure A: Risk Checklist for Cloud IT Services

Introduction

This risk checklist supports the development of a detailed risk assessment for a cloud IT service. ISTS have a more detailed template incorporating this checklist along with other details.

This checklist ensures that consideration is given to all aspects of risks associated with cloud IT services. A risk assessment which addresses the risks identified by this checklist should be included as part of the business case for any cloud IT service.

Restricted data

Systems which hold restricted data (refer to the University's Information Security Policy) are unsuitable for hosting in an off campus environment.

Business critical

Systems which are critical to the business of the University may not be suitable for hosting in an off campus environment.

The questions below are intended to assist in the identification of business critical systems. Answering 'YES' to any of the questions below would indicate a business critical system:

	YES	NO
If this system (or its data) was unavailable for more than 1 hour per year, would this have a significant impact on the reputation of the University?		
If this system (or its data) was unavailable for more than 1 hour per year, would this have a significant impact on the revenue of the University?		
If this system (or its data) was unavailable for more than 1 hour per year, would this have a significant impact on the productivity of the University's staff?		
If this system (or its data) was unavailable for more than 1 hour per year, would this have a significant impact on the satisfaction of the University's customers?		

Service Level Requirements

If a system is identified as business critical, a judgement must be made as to whether the external service provider can meet the service requirements. The following questions will assist in making this judgement:

	YES	NO
Has the University been assured of the vendors track record in meeting its SLA? (Has evidence been provided?)		
Are the vendors scheduled outages acceptable by the University, both in duration and time of day?		
Does the SLA guarantee adequate system availability?		
Will the University receive adequate compensation for a breach of the SLA or contract?		

If the system is business critical and the external service provider can meet the service requirements, a business continuity plan must be developed and tested.

University of South Australia

Risk Identification

Prior to proposing the implementation of an off campus solution, the following checklist should be completed. Any items which are flagged as NO in the list below must be included in a risk assessment and management actions for those items must be identified to mitigate those risks. Additional risks may be identified by business units which should also be incorporated into the risk assessment.

	YES	NO
System Reliability		
If the University accidentally deletes a file or other data, will the vendor be able to restore it quickly?		
Is the network connection between the University and the vendors network adequate?		
Do scheduled outages affect the guaranteed percentage of system availability?		
Can the University easily integrate the off campus solution into the University infrastructure?		

If the answer to any of the questions above are 'NO', consider developing some of these measures to manage or mitigate the risk:

- redundancy mechanisms and off site backups are in place to prevent data corruption or loss
- maintain an up to date back up copy of data held off campus in the proposed system
- plan for how any downtime in the system will be managed
- plan for how the University can move its data or standardised application to another vendor or in-house

	YES	NO
Vendor Management		
Can the University retrieve the data if the vendor goes out of business?		
Will the University receive sufficient notice and access to retrieve data if the vendor discontinues the service?		

If the answer to any of the questions above are 'NO', consider developing some of these measures to manage or mitigate the risk:

- maintain an up to date back up copy of data held off campus in the proposed system

	YES	NO
Disaster Recovery/Business Continuity		
Are disaster recovery / business continuity plans produced by the vendor?		
Are University specific disaster recovery/business continuity plans produced by the vendor?		

If the answer to any of the questions above are 'NO', consider developing some of these measures to manage or mitigate the risk:

- Ensure that University's disaster recovery and business continuity plans cover on campus and off campus systems

	YES	NO
Data Integrity & Security		

University of South Australia

	YES	NO
Will the University retain legal ownership of any data stored off campus by the vendor?		
Will the data be strongly encrypted as part of the proposed off campus solution?		
Will systems used to process University data, be securely monitored by the vendor?		
Can the University use its existing tools to monitor its use of the vendors' services?		
Is data transmitted in a secure manner?		
Does the system manage user identity in a secure manner?		
Does the vendor have a secure gateway environment which is certified by an authoritative third party?		
Does the vendor use endorsed physical security products and devices?		
Is the vendors procurement process for software and hardware trustworthy?		
Is the vendors security posture supported by policies/processes/direct technical controls?		
Can the University access reputable third party audit reports or is it able to audit the vendors security itself?		
Does the vendor support the identity and access management system in use by the University?		
Are users able to access and store sensitive data only via trusted operating environments?		
Does the vendor adequately separate University data from other customers' data?		
Does the University have the option of using systems that are dedicated to it?		
Is the encryption password or key held only by the University and NOT the vendor?		
Does the vendor perform appropriate personnel vetting and employment checks?		
Are actions performed by the vendors employees logged and reviewed?		
Are visitors to the vendors data centres positively identified and escorted?		
Do the vendors data centres have cable management practices to identify tampering?		
Do the vendors security considerations apply equally to the vendors subcontractors?		

If the answer to any of the questions above are 'NO' or the vendor is unwilling to respond to specific questions on this subject, it should be possible for the University to access reputable third party audit reports. This will provide a level of assurance about the vendor without the detail. Discussions with ISTS should also consider whether the University's network security posture is weakened by the vendors cloud.

	YES	NO
System Security		
Is the vendor contactable and do they provide timely responses and support?		
Are the vendors employees trained to detect and handle security incidents?		
Will the University be notified of security incidents by the vendor?		
Will the vendor assist the University with security investigations and legal discovery?		
Will the University receive adequate compensation for a security breach caused by the vendor?		
Will the data storage devices used by the vendor to store University data, be sanitised at the end of life or before being reused?		
Can storage media which stores sensitive data be adequately sanitised?		

If the answer to any of the questions above are 'NO', consider developing some of these measures to manage or mitigate the risk:

- Review the vendor's security incident response plan
- Audit logs and other evidence to perform a forensic investigation

	YES	NO
Legislative Compliance		
Will the proposed system allow the University to meet its legal, moral or contractual obligations?		
Are the privacy laws of countries that have access to University data known and accepted?		
Will the proposed system meet requirements for the EU's General Data Protection Regulation (GDPR)?		
Will the proposed system meet requirements for Australia's Notifiable Data Breaches Scheme (NDB)?		
Are the privacy laws of countries that have access to the University known and accepted?		
*		

If the answer to any of the questions above are 'NO', consider developing plans to manage or mitigate the risk associated with any legislation which may impact on this solution. This may include:

- The Privacy Act 1988
- Tax File Number Guidelines 2011
- Higher Education Support Act 2003
- Education Services for Overseas Students Act 2000