

Questions for Decision Makers: Outsourcing Cloud and Managed Services

Take a moment to reflect on your higher education provider's frameworks, policies and practices in relation to identifying and mitigating business risks associated with outsourcing cloud services and managed services.

Note: These self-reflection questions are suggestions only and are provided for decision makers to consider where areas for improvement may be needed in the provider's approach to managing its cyber security risks.

Area	Questions	Notes
Cyber supply chain risk management activities	Have the components and services relevant to the security of systems that are to be outsourced been clearly identified and understood ?	
	Has a review of suppliers and service providers (including their country of origin) been performed to assess the potential increase to systems' security risk profile, including by identifying those that are high risk?	
	Have those suppliers and service providers that have been identified as high risk been declared ineligible to be used?	
	Have components and services relevant to the security of systems been chosen from suppliers and service providers that have made a commitment to secure-by-design principles , secure programming practices and maintaining the security of their products?	
	Have components and services relevant to the security of systems been chosen from suppliers and service providers that have a strong track record of transparency and maintaining the security of their own systems and cyber supply chains?	
	Has a shared responsibility model been created, documented and shared between suppliers, service providers and the higher education provider in order to articulate the security responsibilities of each party?	

Area	Questions	Notes
Managed services	Is a managed service register maintained and verified on a regular basis?	
	Does the managed service register contain all necessary information for each of the higher education provider's managed services?	
Outsourced cloud services	Is an outsourced cloud service register maintained and verified on a regular basis?	
	Does the outsourced cloud service register contain all necessary information for each outsourced cloud service?	
	Are only community or private clouds used for outsourced SECRET and TOP SECRET cloud services?	
	Do outsourced cloud service providers and their cloud services undergo a security assessment by an IRAP assessor at least every 24 months?	
Contractual security requirements	Do service providers provide an appropriate level of protection for any data entrusted to them or their services?	
	Are security requirements associated with the confidentiality, integrity and availability of data entrusted to a service provider documented in contractual arrangements?	
	Is the right to verify compliance with security requirements documented in contractual arrangements? And is this right exercised by the higher education provider on a regular and ongoing basis?	
	Are types of data and their ownership documented in contractual arrangements?	
	Are the regions or availability zones where data will be processed, stored and communicated documented in contractual arrangements?	
	Is access to all logs relating to the higher education provider's data and services documented in contractual arrangements?	

Area	Questions	Notes
	Is the storage of data in a portable manner that allows for backups, service migration and service decommissioning without any loss of data documented in contractual arrangements?	
	Is a minimum notification period of one month for the cessation of any services by a service provider documented in contractual arrangements?	
Access to systems and data by service providers	The higher education provider's systems and data are not accessed or administered by a service provider unless a contractual arrangement exists between the higher education provider and the service provider to do so?	
	If the higher education provider's systems or data are accessed or administered by a service provider in an unauthorised manner, is the higher education provider immediately notified?	

(Source: Adapted from Australian Cyber Security Centre, *Guidelines for Outsourcing*, <https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-outsourcing>)