TX-RAMP Agency Guide:
Cloud Service Identification Template
April 2023

General Information

Texas Government Code 2054.0593 mandates that state agencies as defined by Texas Government Code 2054.003(13) must only enter or renew contracts to receive cloud computing services that comply with Texas Risk and Authorization Management Program (TX-RAMP) requirements beginning January 1, 2022. Cloud service providers requiring TX-RAMP certification can submit their request for certification to the Department of Information Resource (DIR).

The information within this document may be used to develop an agency's own questionnaire to help staff undergo an initial discovery phase and identify if a service is in scope of TX-RAMP. However, it is important to note that some products may have some of the characteristics described but may not be fully cloud-based. Therefore, it's always best to check if necessary.

Resources

Texas Risk and Authorization Management Program (TX-RAMP) website

https://dir.texas.gov/texas-risk-and-authorization-management-program-tx-ramp

DIR TX-RAMP Assistance and Questions

Contact TX-RAMP@dir.texas.gov

Agency Instructions

Identify relevant stakeholders, such as business owners, procurement, contracting, IT, and information security teams. Gather feedback to identify indicators if a solution is a cloud computing service and customize the list of questions on the next page using their feedback to accommodate your agency's needs. Once updated, educate staff on your procurement processes to help staff identify if TX-RAMP certification is required before contracts are finalized.

Version History

Date	Version Number	Description
4/3/2023	1.0	Published document

Cloud Service Identification

Cloud Characteristics

Help staff undergo an initial identification of whether a product is a cloud service and can be useful when selecting cloud services that meet their specific needs and requirements. If the product does not meet most of the criteria, it may not be a cloud service, and staff may want to discuss the solutions further with their designated IT contacts. If a product has these characteristics, it is likely to be cloud-based. However, it is important to note that some products may have some of these characteristics but may not be fully cloud-based. Therefore, it's always best to check if necessary.

Cloud Identification Decision Tree

- If the system is managed by a third party
- If the third party provide only IT/Cloud support
- If the confidential data located in a multi-tenant production facility
- If the data/system hosted on shared hardware
- If the service be categorized as IaaS, Paas, or Saas
- If the agency or system automatically provisiona or de-provision resources based on need
- If the agency pays for services based on usage

Cloud Identification Details and Considerations

1. Can the product be accessed through a variety of devices, including computers, tablets, and smartphones?
   A 'Yes' response could mean, it may be a cloud product.
   The ability to access the product from any device with an internet connection is a key feature of cloud services and cloud services are designed to be accessible from anywhere with an internet connection, so if the product cannot be accessed in this way, it may not be a cloud service.

2. Can the product easily scale up or down based on user demand?
   If Yes, it may be a cloud service.
   Auto-scaling is a feature that adjusts computing resources, load balancers, databases, and other components to match changes in user demand. However, products that are license-based, may not have this capability and require additional licenses to scale up or down based on user demand. Therefore, it's important to keep in mind that the absence of auto-scaling could suggest that the product isn't a cloud service.

3. Is there redundancy built into the product to ensure high availability and data resilience?
   If Yes, it may be a cloud service.
   Cloud services are designed to be highly available and resilient, so they typically have redundancy built into their architecture. If the product does not have redundancy built-in, it may not be a cloud service.

4. Is the product hosted on shared infrastructure where resources are shared with other users?
   If Yes, it may be a cloud service.
   Cloud services are often hosted on shared infrastructure to provide cost savings and scalability. If the product is hosted on dedicated infrastructure, it may not be a cloud service.

5. Does the product use a pricing model where you only pay for what you use?
   If Yes, it may be a cloud service.
   Cloud services often use a pay-as-you-go pricing model to provide cost savings and flexibility for the resources that you use, such as storage, bandwidth, or computing power. Pay-As-You-Go scales up or down based on your changing needs, without having to worry about paying for unused resources. If the product does not use a pay-as-you-go pricing model, it may not be a cloud service.

- Is the product priced on a subscription basis, rather than a one-time purchase?
  A 'Yes' response could mean, it may be a cloud product.

- Consider how the product provides access to software applications, infrastructure resources, development resources, or other information resources.
  Software-as-a-Service (SaaS) products are cloud-based software applications that are accessed over the internet.
  Infrastructure-as-a-Service (IaaS) products are cloud-based infrastructure resources that are accessed over the internet.
  Platform-as-a-Service (PaaS) products are cloud-based development platforms that provide tools for building, testing, and deploying applications.

6. Does the vendor manage software and system updates for the product?
   If Yes, it may be a PaaS or SaaS cloud service.
   If no, it may potentially be an IaaS.
   Cloud service providers often provide update to ensure that they are always up-to-date and secure.

- Responsibility for Maintenance: Who is responsible for maintaining the product and ensuring its availability?
  If the provider is responsible: The product may be a SaaS. SaaS providers are responsible for maintaining the software application and ensuring its availability to users.
  If the user is responsible: The product may be an IaaS or a PaaS. With IaaS and PaaS products, users are responsible for maintaining and configuring the resources that they are using.

- Does the product require any physical hardware or on-premise servers to operate?
  A 'No' response could mean, it may be a cloud product.

- Does the system have the ability to expand its capacity to meet customer demand?
  A no response could mean that the system is most likely not a cloud.

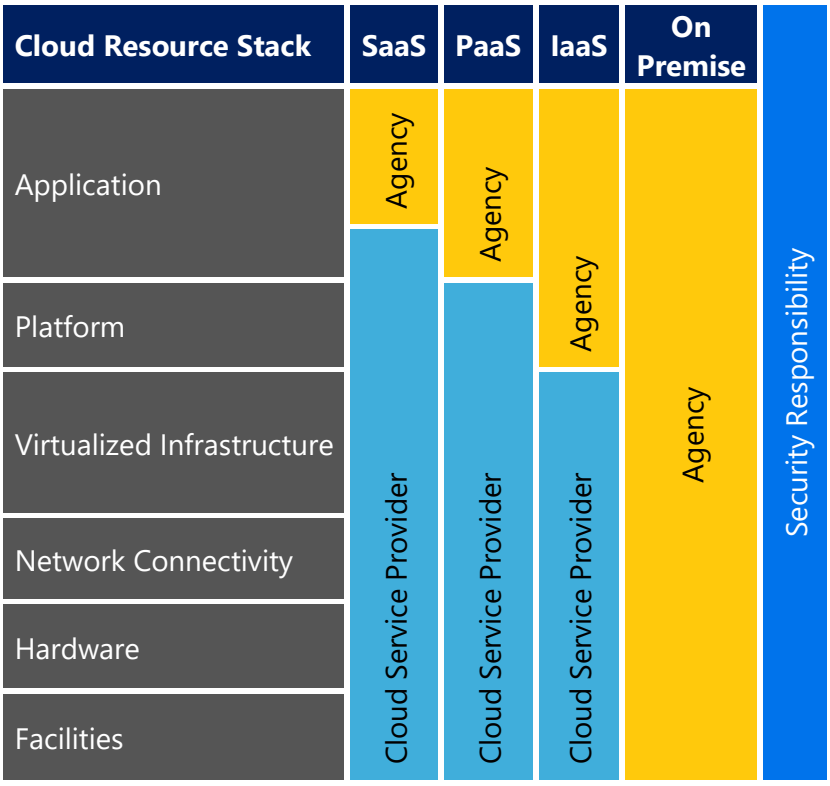
- Does the system allow the consumer to build anything other than servers?
  A no response could mean that the system is an IaaS.
  A yes response could mean that the system is either a PaaS or a SaaS.

- Does the system offer various developer toolkits and APIs?
  A yes response could mean that the system is a PaaS.

- Does the system offer only applications that are available by obtaining a login?
  A yes response could mean that system is a SaaS. A no response could mean that the system is either a PaaS or an IaaS.

- Examine where responsibility lies between the customer and the service provider.
  Review a shared responsibility model between the service provider and the customer, understanding assigned responsibilities or characteristics could mean that the product is a cloud service offering. Consider who is responsible for the following: Client and end-point protection, Identity and access management, Application-level controls, Network controls, Host infrastructure, and Physical security.

Table 1. The following table illustrates the differences in scope between the cloud consumer (agency) and cloud provider for each of the service models discussed above. The delineation of security control responsibility is heavily dependent on the service and deployment models of the solution the agency is adopting. For example, if the solution is a SaaS e-mail solution, the agency may be responsible for a small subset of security control responsibilities including Access Controls. If the agency is deploying their own applications to a PaaS or IaaS solution, they will have greater responsibility for securing the application layer, and potentially the platform and middleware; and may have shared responsibilities in the TX-RAMP Security Controls with the exception of possibly the personnel and physical security requirements.



- Is the contract for an IT service to build a solution?
  A yes response could mean that the service is a development service and not for a SaaS, in which a custom developed solution is being built for a customer. However, consider where the custom-built solution is hosted, where the application is hosted may be a PaaS or IaaS.

- Is the cloud product or service not subject to TX-RAMP due to meeting the criteria for out of scope of TX-RAMP?
  Review the TX-RAMP Program Manual, section 6. TX-RAMP Level Determination, and TX-RAMP Overview Points and Scoping video for more scoping information.

- Is the cloud product or service already listed on the TX-RAMP Certified Cloud Products.
  Products that have a Provisional, Level 1, or Level 2 TX-RAMP Certification are listed on the DIR TX-RAMP webpage - TX-RAMP Certified Cloud Products.
  Products with a provisional certification permit a state agency to contract for the use of a product for up to 18 months without receiving full TX-RAMP certification and will need to be certified through a TX-RAMP assessment or equivalent within the provisional status period to maintain compliance with program requirements.
  FedRAMP and StateRAMP authorizations may also be leveraged to achieve Level 1 and Level 2 TX-RAMP certification.