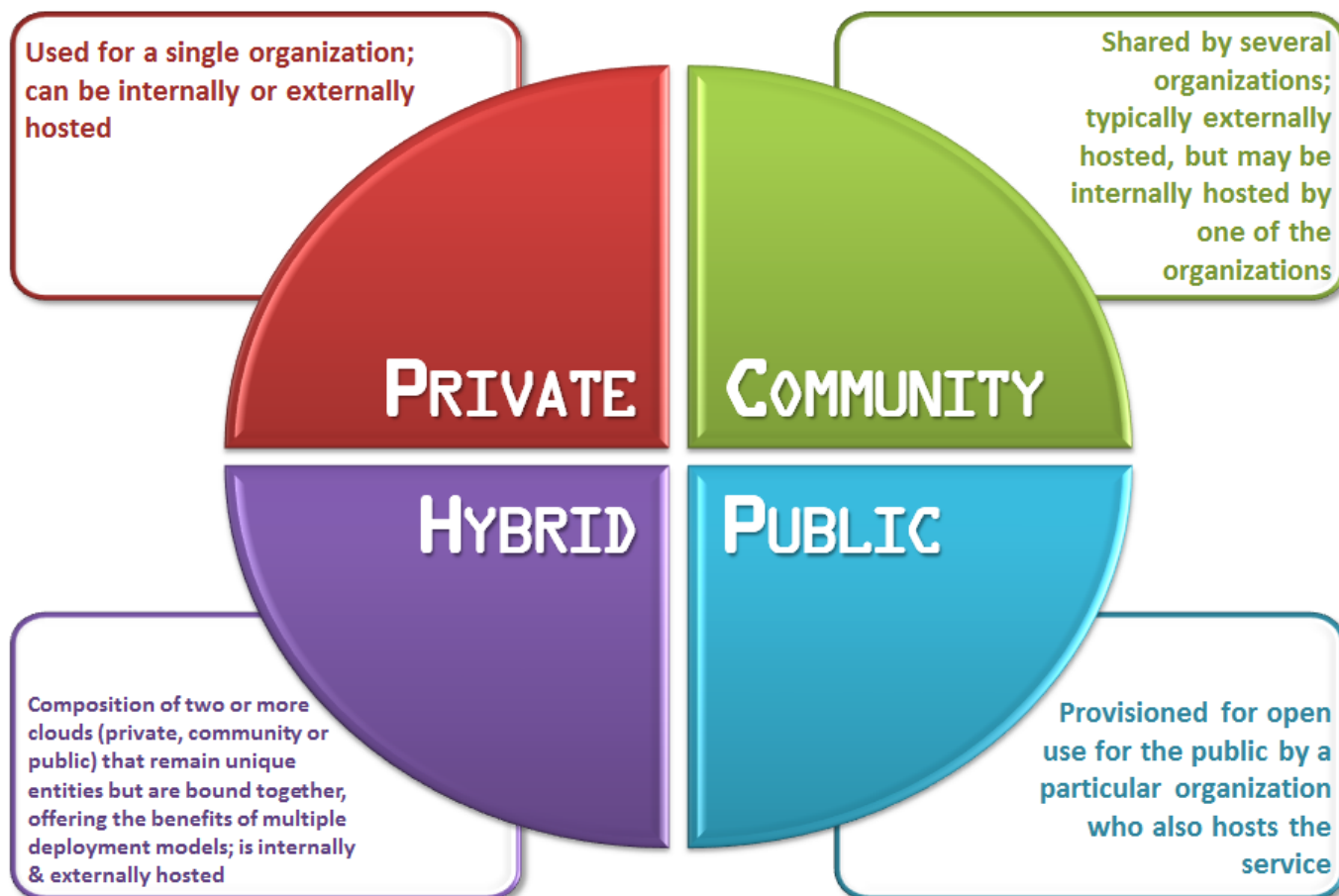


Tips for Cloud Computing

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software and information are provided to computers and other devices as a metered service over a network—typically the Internet (Wikipedia)



TYPES OF CLOUD COMPUTING

DATA MANAGEMENT CONSIDERATIONS

- 1) Where do the data/files/documents physically reside—what state or country? Where are all the backups? Do agency rules and/or state/federal law permit this?
- 2) What types of data/records would be stored “in the cloud”? Is there any sensitive data? Are there any security/privacy requirements spelled out in law—e.g. HIPAA, FERPA, PCI—that apply to these particular data/records?
- 3) Data ownership – who owns the data/records on the system?
- 4) How long are data/records retained by the provider?
- 5) How will your organization manage the records on that site? If data are backed up to redundant sites, how will records be deleted in accordance with records retention schedules?
- 6) Does the service provider’s agreement address how the agency can obtain their data/records if the service provider goes out of business?
- 7) How easily can public records/e-discovery searches be performed in the system?

SUPPORT AGREEMENTS CONSIDERATIONS

1. How scalable is the service? Is it easy to expand services if the agency experiences rapid growth? Or can it easily be cut back, in case needs decrease, so the agency is not paying for services that are no longer needed?
2. What is the process for migrating away from that cloud provider? How will you retrieve agency data/records stored in the cloud provider’s system? Is it in a format that can be imported into another application so it can be used?
3. What support options are offered by the cloud vendor? What are the service level agreements? Have you seen reviews from other clients of that cloud provider?

SYSTEM MANAGEMENT CONSIDERATIONS

- 1) What is the provider's disaster recovery plan? Do you/they have backups of all of your data/records? What is the process for backup retention and recovery?
- 2) What security protocols are followed by the vendor? Does the vendor retain a copy of the encryption key? Or is your agency responsible for managing this? (If the encryption key is lost or misplaced, the agency may lose access to data/records.)
- 3) Has the click through agreements (Terms of Service) or contract for cloud services been reviewed by legal, and signed by the person in your agency that has the authority within the agency to enter into contracts?
- 4) What are the scale, scope and capability of the vendor? Are they on financially sound footing to be around for a long time?
- 5) If doing business with multiple cloud providers, does your organization have capacity to track/manage the data in multiple systems? Data/public records will need to be inventoried, tracked and managed.
- 6) What is the agency’s plan for transferring knowledge about cloud account information when employee turnover occurs? How will the agency retain/transition account information from exiting employees?
- 7) How is user activity tracked? And are those logs accessible to the agency/system administrator? What is the process for obtaining this information?

