Practical Guide to Cloud Service Agreements

CSA: is an Agreements between cloud customer(buyer) and Cloud provider(seller)

Notes:

- CSA is different for IaaS,PaaS,SaaS.
- Cloud computing goals are:
  - Reduce cost
  - improve flexibility
  - increase reliability of the delivery of the service

CSA is composed of(not mandatory):

1. customer Agreement
2. Acceptable User Policy(AUP)
3. Service Level Agreement(SLA)

customer Agreement:

describe the overall relationship between the customer and provider

Service Management -> customer Agreement

Service Management: include processes and procedures used by the provider.
customer Agreement: is the explicit definition of rules, responsibilities and execution of processes formally agreed upon

AUP:

AUP prohibits illegal use of the Service

SLA:

describe levels of Service using various attributes(availability, performance, ...)and for each attribute SLA define `Thresholds` and `Financial Penalties associated with violation of these Thresholds`.

Note: there is usually a mismatch between metrics measured by the provider and those measured by the customer, specially in SaaS because application level services are impacted by many factors, This is why CSA for SaaS lack tight service level guarantees.

1-Understanding Rules and responsibilities

- **Roles** for cloud computing:
  1-cloud service **customer**
  2-Cloud service **provider**
  3-cloud service **partner**(why? trust issue)
  example: how can a cloud customer trust a cloud provider's internal operations? we employ a cloud service partner(Auditor)which have an insight into the provider internal operations, specially concerning security issues and the `Auditor` can give Attestations and Certifications to customers)

- **Responsibilities** are split between the customer and the provider
  customers should be aware who is responsible for some services or attributes of a given service(by reading the provider CSA)

2-Evaluate Data and Business level policies

Data policies are the most important

- **Data policies**:
  - **Date Preservation and Redundancy**: Backup/Restore/Integrity Checks
  - **Date Privacy**: answers how personal data is stored and used?
  - **Data Availability(uptime)**: tell if you have a maintenance schedules
  - **Change Management and Notifications:**
    Is there a change later on some policy?
    if yes how much time is given for customers to get prepared before a change is done?

- **Business policies**:
  - **Guarantees**: Services Attributes.
    example: service availability is 99.9%
  - **AUP**: answers: how the customer may use the service? what actions the provider may take in event of an illegal use of the service?
  - **List of Services not covered.**
  - **Excess Usage:** answers: do you want to exceed the customer specified usages thresholds of a service?(tip: no, because customers should correctly size their requirements)
  - **Activation**: answers: what is the precise start time of a service?
    for measurements on performance.
  - **payment and penalties model**: answers: how payment is made?(pay as you go/mothly)
  - **Renewals:** change services levels upon Renewals.

- **Transferability:** migrate to a new service provider without penalties.
- **Support**: table provides problems and their priorities and their:
  `response time`,`time to start fixing`,`the overall fix time`
  example:
  priority --- response time --- time to start fixing --- overall fix time
  p1 1h 1h 2h
  ....
  p3 4h 1d 2d
  ....
- planned maintenance: give time required for a planned maintenance(e.g:monthly)
  which is considered a part of the downtime of the service
  downtime = not uptime(ex: 0.01% =~ 8.5h per year) + planned maintenance
- subcontracted services: ensure that the service is provided only by the provider and that no third party is involved in some part of services the provider give.

3-Sevice level objectives:

In SaaS we need flexible CSA.
general service level objectives(should be taken via clear and consistent measurements):

- **uptime(Availability):**
  percentage of uptime for a service in a given observation period
- **downtime**
- **response time:** elapsed time from when a service is invoked to when it is completed (usually in milliseconds)
- **data persistence**
- **portability:** store data in standard formats to make it portable in case a customer changed his cloud service provider
- **scalability**
- **system qualities:**
  - **reliability**
  - **fault tolerance**

4-security and privacy to data and application

- **security classifications:**
  - **Access Control**(data ownership/protection)
  - **Archiving**(data retention and destruction in case of a provider change)
  - **Encryption**(specify security levels)

- **security considerations:**
  - **Estimate** asset sensitivity: Estimate CIA (Confidentially-Integrity-Availability)
  - **Restrictions**:
    - 1-Detect unapproved data moving
    - 2-monitor for large internal data migration with `DAM`(DB activity monitoring) and `FAM`(file activity monitoring)
    - 3-monitor for data moving to cloud with `URL Filters` and data loss prevention
    - 4-protect data in transit(moving in & out): data should be encrypted
    - 5-protect data at rest: encrypt stored data by client
  - **Audit**:
    Give the "right to Audit" to customer to enable them to audit the cloud provider or use a "certified third party"(`Auditor`) to audit
  - **Notifications**:
    the provider should notify the customer of the occurence of any breach of its system
  - **Privacy**:
    - Give the "right to be forgotten" to customers which enable them to delete their data and backups

5-**Service Management requirements:**

- **Monitoring and Reporting:**
  - monitor **response time**:
    - response time in the internal system
    - response time between cloud provider and customer
  - peak load **performance**:
    measurements and timing when the system is under pressure
  - monitor **performance**:
    - internal processing benchmarks
    - end-user experience measurements
  - problems **Notifications**:
    monitoring and Reporting on failures
    (monitoring by customer-side or provider-side
    notifications types:
    one-way-Notifications[customer report a service failure to the provider or
    two-way-notifications[the customer and provider notify each other in case of failure])

  - **user satisfaction** reports

- **measurements and metering:**
  while the service is sold by time or capacity
  CSA should include:
  - 1-**Accurate billing**
  - 2-different services should have **different methods of billing**

- **Provisioning:**
  - 1-**core Provisioning speed**: give the speed of deployment of new system,new data..
  - 2-**customization**: is customization allowed? if allowed be careful of additional delays.
  - 3-**testing**: testing automated deployment and scaling

  ...
  it's open to add whatever you want

- **update and patching:**
  - **Responsibilities** upon changes in services: who is responsible for a change? (customer/provider)
  - **Timeline** to implement the update and test it
  - **resolve** problems caused from changes.
  - **backout**: backout (to initial state) process if changes cause major failures

6-Disasters recovery plan:

Determines the acceptable downtime of a service

7-The **EXIT** process

- **smooth transition:**
  - give the customer the ability to terminate at any time(enable the customer to delete his data)
  - help the customer in case he want to change the provider
- **continuity**: details to ensure business continuity
- **portability:**
  data maintained on the provider's cloud resources should be stored using standard formats to ensure data portability

Conclusion:
Transparency of service level leads to successful service Management