Cloud Service Rollout

Chapter 9

Cloud Service Topics

- Cloud service rollout plans vary depending on the type of cloud service SaaS, PaaS, or IaaS and the vendor.

Unit Topics

- Identifying vendor roles and responsibilities
- Identifying organizational skill requirements
- Transitioning to live environments
- Preparing for incident management

Identifying Vendor Roles and Responsibilities

- Cloud service vendors extended the commonly used terms of agreement generally seen in software licenses to the cloud environment.
  - Customers click through a predefined list of licensing options that defines the user agreement and can finish the purchase only if all terms are accepted.
  - Trend is slowly losing power, especially when it comes to larger organizations.
- A key aspects of moving to the cloud is to provide data access anytime, from anywhere, on any device, as well as to be able to dynamically scale.
- Larger organizations understand that terms must be present in the service agreement to guarantee the delivery of those services and define what happens when the terms are not met.
- An important factors when deciding on cloud service vendors is the ability to negotiate the legal terms of the service agreement.

SLA Inclusions

List of customer and the cloud service vendor roles and responsibilities including:

Contract renewals

- Most vendors have an automatic contract renewal clause.
- Larger organizations tend to stay away from such contracts.

Contractual protection

- Service-level agreement (SLA) describing the availability of services and any penalties that might be accrued in case the SLA is not met.
- Organizations should also look for:
  - Protection and assurance on data access and privacy controls
  - Documented policies on data protection
  - Security certifications
  - Application of rules and regulations.

Insurance

- Rcommended to have insurance coverage in case of business interruption due to the inability of the vendor to maintain service terms.
- Some vendors will have insurance; others will not.

SLA Inclusions

Data loss

- Data loss caused by either vendor or customer.
- Larger organizations tend to share the responsibility of data storage more often than smaller organizations.
- Ability to have an in-house copy of the data must be discussed and added to the service terms.

Data location

- Most vendors copy the data stored across data centers in different cities
  - Sometimes different countries.
- Different countries and unions have laws that govern where data can be stored.
- Organizations and vendors must be aware of the regional laws and ensure that they are dealt with in the terms of service.

Data ownership

- Data stored with the vendor should be the property of the customer, not the vendor.
- Depending on the type of data being stored, it is necessary to protect it from being shared across other organizations and used by the cloud service vendor themselves.

Best Practices

- Terms of service needs to deal with the process of handing the data over to another vendor
  - In case the customer decides to change vendors in the future.
  - Harder in SaaS scenarios because the vendor hosts the applications and their data format might not be the same as a different vendor for the same service.
- The Cloud Industry Forum (CIF) developed a white paper in 2011 called "Cloud: Contracting Cloud Services, a Guide to Best Practice" that discusses the best practices for negotiating cloud services contracts; it is available at:

http://cloudindustryforum.org/

Best Practices For Negotiating A Cloud Service Contract:

Choice of law

- Organizations looking for a cheap or standard cloud service should contract under the vendor's standard terms, including the choice of law.
- Other organizations should negotiate contract terms with the vendor and choose the law based on their territory coverage.

Data control

- Vendors should disclose the list of data centers used to store the data, including backups.
- SLA between the vendor and the organization must also specify how backups are handled.

Best Practices

Service availability

- Vendors should have documented management systems, processes, and resources.
- Organizations should be able to access the average available time provided by the vendors in the different layers of services offered.
- Consequences for not meeting the SLA must be clearly identified.

Liabilities and indemnities

- Organizations should specify the purpose of contracting with the vendor.
- Unless the service adequately addresses this purpose, it is pointless to enter into the contract.

Deletion of Data

- Vendors should maintain a copy of the data being hosted even if the customer is not paying and not able to access the data.
- Before data is deleted, the customer must be notified with enough time to resolve any existing disputes.
- Vendor responsibilities vary depending on the type of cloud service being offered.

Best Practices: Responsibilities

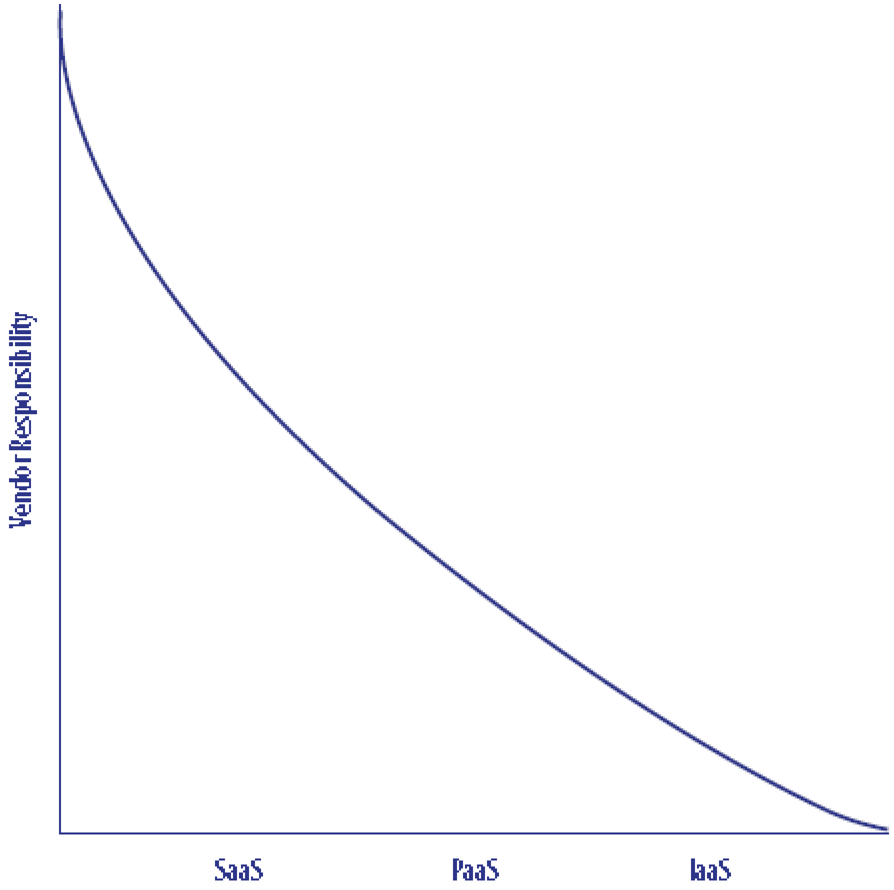

FIGURE 9.1 Vendor responsibility by type of service

- SaaS vendors will have more responsibility over the service provided than PaaS vendors, and PaaS vendors will have more responsibility than IaaS vendors.
- Figure 9.1 shows the vendor responsibility by type of cloud service.

Identifying Organizational Skill Requirements

- Moving an application to the cloud usually means transferring technical responsibilities of all, or part, of the application to a vendor.
  - Though technical skills are basically transferred to the vendor, they are still required at different levels.
- Customer may not be required to maintain expertise on the technology used to create and maintain SaaS applications, but they must understand how the applications work and their limitations.

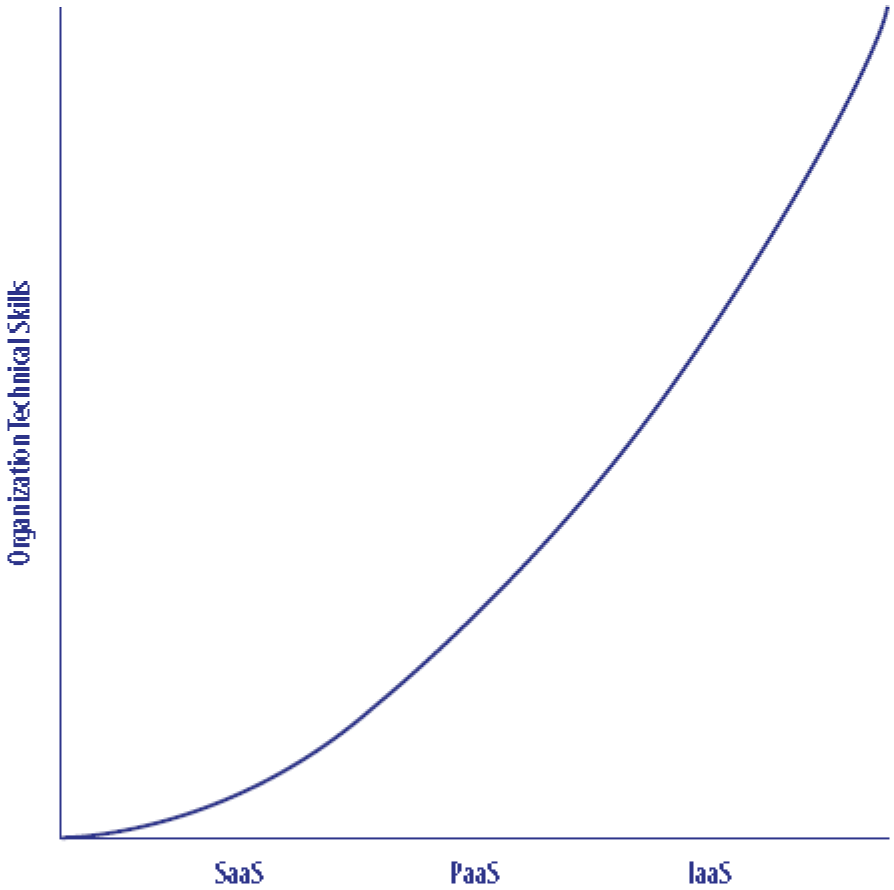

FIGURE 9.2 Technical skills vs. cloud service

- Figure 9.2 shows the relationship between technical skills required by cloud service.

Software as a Service (SaaS)

Technical skills

- Since the vendor maintains the application, technical skills acquired by the organization to maintain a SaaS solution are minimum.
- Depending on the scale of the project, organizations might have their service desk operators trained on basic usage of the SaaS solution.
- Yet, some SaaS providers will also provide help desk services, which should be integrated with the service desk maintained by the organization.
- This integration can be as simple as having service desk operators redirect calls to the vendor's support website or call center.

- Even though most SaaS vendor provide monitoring tools and reports that show the overall availability of the service to their customers, it is important to monitor the SaaS solution from the organization's perspectives.

- Consider whether the new SaaS solution is replacing an existing service.
  - You might need to migrate the existing data from the existing solution to the SaaS solution.

In summary, the technical skills required by the organization to maintain a SaaS solution contracted from an outside vendor are:

- Basic skills on using the solution for service desk and training purposes.
- Monitoring skills to ensure the SaaS solution is accessible to end users.
- Migrate data from existing solutions to the SaaS solution.

Project management skills

- SaaS solutions are vendor developed and maintained.
- When acquiring a SaaS solution, you must be able to manage the implementation of the solution within your organization.
- Users must be trained on the new solution.
- If the solution replaces an existing system, data may have to be imported from the existing system into the new SaaS solution.

From a project management perspective, you have to:

- Create and implement a training and adoption plan.
- Create and implement a data migration plan when required.
- Create and implement a pilot program.

Vendor Management Skills

- Service terms and SLAs must be negotiated with cloud vendors carefully.
  - Going to the cloud involves trusting a vendor to keep applications running.
- Dealing with these vendors becomes a daily activity.
- With SaaS solutions specifically, you must be able to negotiate the right SLA terms and ensure that the requirements for the solution are met by the vendor's service.
- Once the service is in production, you must be able to communicate efficiently with the vendor on SLA monitoring metrics, problem management, and change requests.

In summary, these are the actions required for vendor management when acquiring a SaaS solution:

- Negotiate the SLA
- Communicate on SLA metrics
- Manage expectations for changes in the system

Data Integration And Analysis Skills

- In a SaaS, data storage is done by the service provider.
  - If you are migrating an existing application to a SaaS application, you need to work with the vendor to plan how data will be migrated.

Business and financial skills

- Organization must be able to make a case for cloud computing and show the return on investment (ROI).
- Necessary to have metrics that can be used to tell if the business performance being met by an application matches the cost of keeping it in the cloud.

Security and compliance management skills

- Organizations are regulated based on their type, type of data handled, and location.
- When hosting data in the cloud, an understanding of many regulations becomes extremely important.
  - Sarbanes-Oxley (SOX)
  - Health Insurance Portability and Accountability Act (HIPAA),.

Platform as a Service (PaaS)

Technical skills

- Since the vendor will maintain the virtual operating systems, technical skills acquired by the organization to maintain a PaaS solution are directly related to the application being developed.
- When migrating to a PaaS solution organizations need to ensure their developers are well trained on the APIs offered by the PaaS vendor.

In summary, the technical skills required to maintain a PaaS solution:

- Basic skills on using the solution for service desk and training purposes.
- Monitoring skills to ensure the PaaS solution is accessible to end users.
- Data migration from existing solutions to the PaaS solution.
- Development skills on the APIs provided by the PaaS vendor.

PaaS Project Management Skills

- Users must be trained on the new solution, and if the solution replaces an existing system, data may have to be imported from the existing system into the new PaaS solution.
- From a project management perspective, you have to create and implement:
  - Training And Adoption Plans
  - Development Plans
  - Data Migration Plans When Required
  - Pilot programs

Infrastructure as a Service (IaaS)

Technical skills

- Include all the skills previously discussed in the PaaS section, along with the skills necessary for operating system deployment, and maintenance.

In summary, the technical skills are:

- Basic skills on using the solution for service desk and training purposes.
- Monitoring skills to ensure the IaaS solution is accessible to end users.
- Data migration from existing solutions to the IaaS solution.
- Development skills on the APIs chosen by the organization.
- Deployment skills on the operating system, or systems, chosen by the organization.
- Patch management skills on the operating system, or systems, chosen by the organization.

IaaS Project Management Skills

- Users must be trained on the new solution.
- If the solution replaces an existing system, data may have to be migrated from existing system into new IaaS solution.

From a project management perspective, you have to:

- Create and implement a training and adoption plan
- Create and implement a virtual machine deployment plan
- Create and implement an operating system patching plan
- Create and implement a development plan
- Create and implement a data migration plan when required
- Create and implement a pilot program

Transitioning to Live Environments

- The transitioning of a cloud-based application from a test environment to a live environment varies depending on the type of cloud service being used.
- Often SaaS applications are the easiest because they are mostly owned by the vendor.
  - Switch from test to live does not require any changes by the customer.
- PaaS vendors like Microsoft and Salesforce.com provide a test environment in which virtual machines can be executed to run a cloud-based solution before moving into full production.
  - These vendors often provide the capability needed to copy the test environment settings, including virtual machines, virtual switches, and applications to a live environment.
- IaaS vendors and PaaS vendors work in a similar way. However, IaaS vendors might not provide any tools for migration.
- Check with vendor and understand what kind of migration support is offered by its specific platforms.

Migration

- Hybrid scenarios, where the organization has a private cloud and a public cloud, deal with migration to a live environment in different ways.
- Choice of technology dictates how transition will occur.
- Organizations using Microsoft System Center and Azure can take advantage of AppController, an application used to manage and deploy services across private and public clouds based on System Center and Azure.
- Independent of technology and type of cloud services being used, Internet bandwidth must always be taken into account.

Internet Bandwidth

- Applications that were once accessed in the local network are now hosted in a public cloud, accessed over the Internet.
  - Necessary to ensure that the organization has enough bandwidth to guarantee user access to the applications.
- Some organizations consider changing Internet service providers to be on the same network as the vendor used to host their cloud services.
  - Decreasing number of hops between the organization and the vendor.

Prioritizing applications

- Some routers and firewalls can use technologies—such as Wide Area Application Services (WAAS) from Cisco—that allow rules to be created to prioritize bandwidth usage based on the application being accessed.

WAN design

- Depending on cost analysis, the WAN design of an organization might have to change to accommodate the traffic going over the Internet.

Preparing for Incident Management

- The Information Technology Infrastructure Library (ITIL) defines incident as "Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to or a reduction in, the quality of that service."
  - Stated ITIL objective when dealing with incidents is to "restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price."
- Incident management is a core process of every organization that relies on IT services.
- Process owned and operated by the Service Desk function in ITIL.
- No matter how complex an organization's enterprise architecture is, all incident management processes can be simplified, as displayed in Figure 9.3.

Preparing for Incident Management

- No matter how complex an organization's enterprise architecture is, all incident management processes can be simplified, as displayed in Figure 9.3.

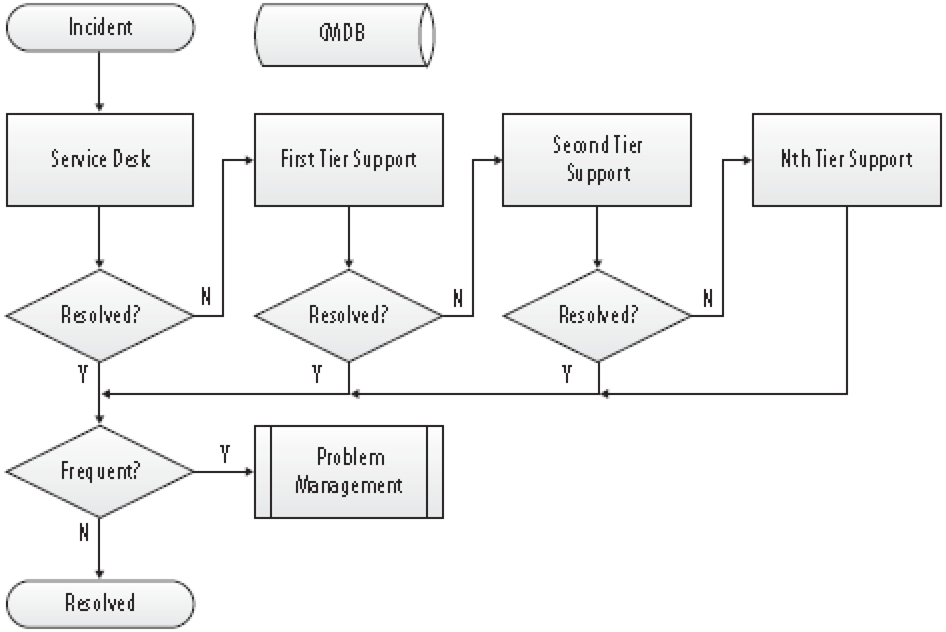

FIGURE 9.3 Incident management process

Different incident management processes and software

- Each cloud vendor might have its own process for incident management.
  - May use different systems to track incidents.
- Organizations must consider if their incident management software must interoperate with thevendor's incident management system.

Lack of transparency

- Not only may the process and software used for incident management be different for each vendor, most organizations are not privy to the details of how incident management works for vendors, creating a black box.

Multiple vendors

- Most organizations use different cloud vendors for different services.
- Very common to use more than one SaaS vendor and a different vendor for PaaS or IaaS.

Black Box Issues

- Escalates the black box issue because each vendor might have its own process, as shown in Figure 9.5.

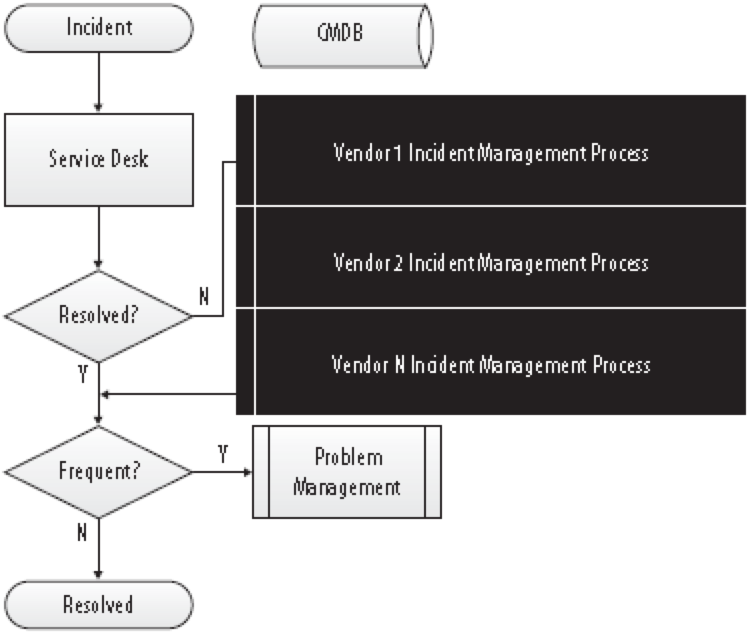
Incident
CMDB
Service Desk
Vendor 1 Incident Management Process
Vendor 2 Incident Management Process
Vendor N Incident Management Process
N
Resolved?
Y
Frequent?
Y
Problem Management
N
Resolved

FIGURE 9.5 Incident management process black box

Summary

- To better prepare for incident management in a cloud environment using different vendors, it is important to define clearly each vendor’s service description, service- level agreement (SLA), and support agreement.
- Service description must be detailed and specify the service being provided by the vendor in clear and concise language to ensure that both the organization and the vendor understand what is being provided.
- Service-level agreement must specify the availability of the service being contracted in the service description and account for penalties if the SLA is not met as well as contain all assurances needed by the customer as discussed earlier in this chapter.
- Support agreement must specify who is responsible for each line of support and how data is to be integrated between the disparate systems.
- Organization and each individual vendor agrees upon each of these elements.
- Important for the organization to integrate the processes provided by each vendor with its internal incident management process to allow better control of incident management as a whole.

Questions???