2017 CLOUD STRATEGY

Prepared by Shukur Mohammad, James Taylor, EJ Widun

Revised 10/11/2017 1:31:00 PM

EXECUTIVE SUMMARY

As technology continues to evolve so does Oakland County Information Technology's (OCIT) infrastructure environment and development model. The overarching goal of OCIT 's Cloud Strategy is the ability **to run any time and run any where.** This means that OCIT needs to have the ability to support cloud and on-premise solutions; where the optimal configuration for performance, reliability and cost can be selected.

For the purposes of streamlining the run any time and run any where strategy, we will determine on a case by case basis where a workload should reside, and will construct environments where the solutions are either all in the cloud or on-premises. Splitting workloads between the cloud and on-premises reduces the effectiveness and efficiency of both technology platforms.

As we look toward our future, Oakland County (OC) is looking to establish a **Cloud First** approach to application infrastructures. The Cloud will provide Oakland County with several benefits including economies of scale, removal of non-value added tasks from daily workloads, increased innovation and improved collaboration across IT. We will establish the standards that govern our cloud environments and enable the Cloud First mindset through our Technical Design Review process.

Oakland County has been leveraging cloud computing technologies for some time. We have many successful Software as a Service (SaaS) implementations and some Infrastructure as a Service implementations. Our preliminary experiences with Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) suggest that they are suitable for agile, rapid development and deployments.

With the convergence of market trends, successful cloud deployments and upcoming technology projects, now is the time for Oakland County to transform the way we do business. **We cannot take our current processes and adapt them to the cloud. We need to create a new way of doing business that leverages all of the value propositions of cloud.** These new and improved processes may be applied to our on-premises infrastructure to take advantages of the lessons learnt in the cloud as a part of our **Outside-In** approach.

A true cloud strategy includes a holistic view of IT that requires partnership, collaboration and the support of leadership to remove the barriers to the cultural chage.

This Cloud Strategy will:

1. Define the cloud and its components creating a common and shared lexicon for OC.
2. Articulate the benefits, considerations, and trade-offs of cloud computing.
3. Identify the program, activities, roles and responsibilities for our transformation to Cloud First computing.
4. Provide a high-level roadmap for cloud migrations.
5. Provide a deicison framework for solutions to migrate to the cloud.
6. Define the Cloud connection methodologies.
7. Ensure the security requirements are included and met.
8. Establish the governance policies of the cloud.

DEFINITIONS, ATTRIBUTES & TAXANOMY

What is Cloud Computing?

"Cloud Computing is a style of computing where elastically scalable technical capabilities are delivered as a service using Internet technologies." – Gartner

Attributes of Cloud Computing

- Abstraction – infrastructure abstracted from the customer and delivered as a service.
- Agility – ability to provision and re-provision infrastructure resources since it is delivered as a service.
- Reliability – improved availability with multiple redundant sites.
- Scalability – ability to accommodate varying loads (scale-up, down or scale-out).
- Elasticity – ability to cope with loads dynamically.
- Security – provides a secure infrastructure.
- Performance – is reliable and can be monitored.
- Maintenance – is easier to maintain with self-service for all configurations.
- Multi-tenancy – ability to host multiple tenants.
- Metered usage – ability to monitor and control usage. Pay as you go model to reduce capital expenditures.

Cloud Computing can deliver System Infrastructure components (Network, Storage, Servers, Load Balancers etc.), Application Infrastructure components (Services, Platforms, Applications, etc.) and provides licensing flexibility (Bring your own License or purchase from the service provider).

Cloud Deployment Models

Deployment Model	Definition	Examples
Private Cloud	Cloud Infrastructure operated solely for a single organization, whether managed internally or by a third-party, and may be hosted either on-premise or off-premise.	OpenStack, VMWare Private Cloud, IBM SoftLayer, etc.
Public Cloud	Cloud Infrastructure made available to the general public or a large industry group and is owned by an organization providing cloud services.	AWS, Azure, Rackspace, etc.
Hybrid Cloud	Cloud Infrastructure delivered by some combination of private and public services, from different service providers. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.	Cloud bursting for load-balancing between clouds. Application deployed to the cloud infrastructure and data is on-premises.
Community Cloud	Cloud Infrastructure shared by several organzations and supports a specific community that has shared concerns (e.g., security requirements, policies and compliance considerations, industry	AWS GovCloud, Azure Government Community Cloud. AWS and Azure Government clouds host environments for several federal,

	requirements). It may be managed by the organizations themselves or a third party, and may exist on-premise or off-premise.	state and local government entities.

Cloud Computing Service Models

Figure 1 shows the comparison options of the different cloud computing service models. A typical deployment in the cloud environment for an OC application could include components in each of the three cloud service models.

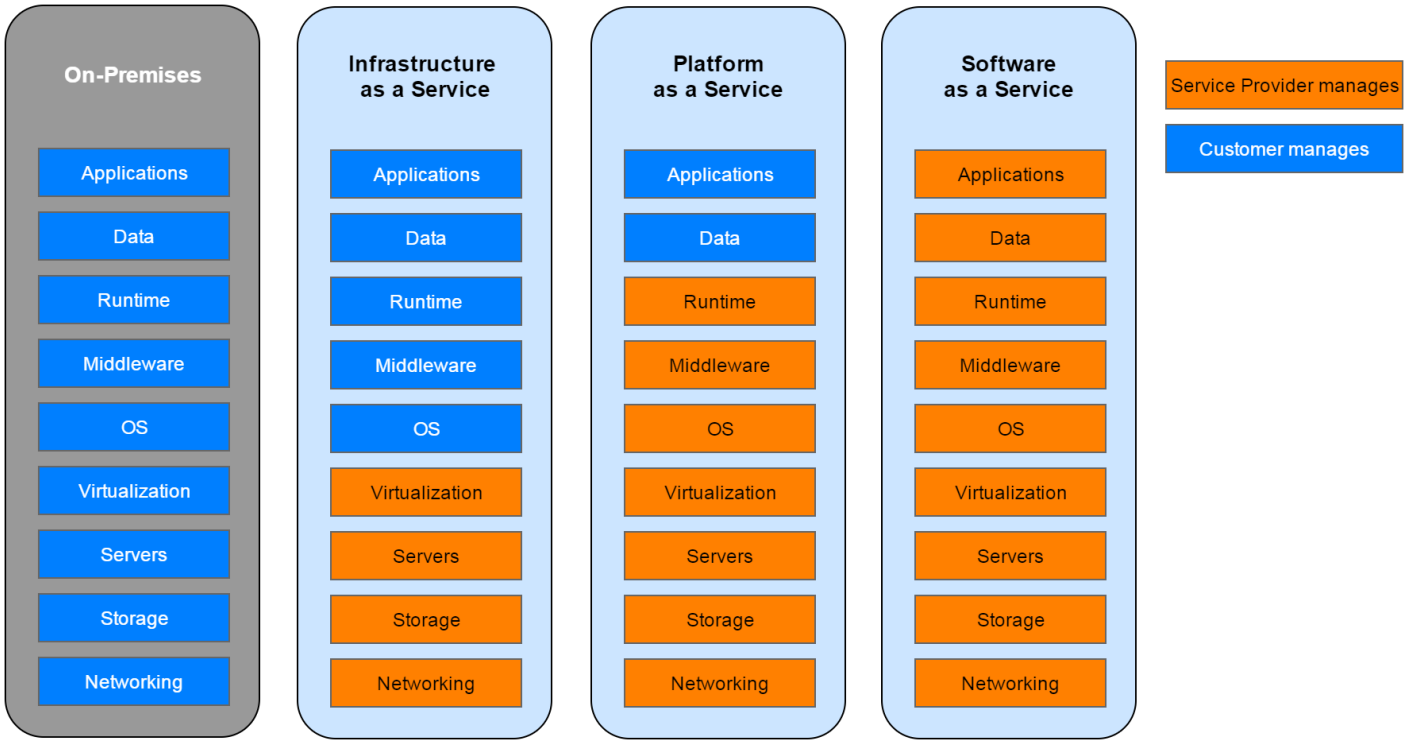

Figure 1: Comparing Cloud Computing service models

Software as a Service (SaaS)

The capability provided to the customer is to use the provider's applications running on a cloud infrastructure.The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Applications are typically upgraded and maintained by the SaaS provider.

Some examples include: SalesForce, Kronos, ArcGIS Online, Office 365, etc.

Pros:

- Quick implementation – since there is no hardware or software to setup and configure, the implementation times are greatly reduced.
- Zero planned upgrades – the service provider is responsible for all planned upgrades. OC may need to test the changes for some planned upgrades with the vendor.

- Patches and Upgrades – are automatically applied (more often on a scheduled timeframe). This ensures the customer always uses the most current version of the softwareand also includes the latest security patches.
- Availability and Redundancy – is the responsibility of the service provider.
- Backup and Retention – is the responsibility of the service provider.
- Security – is the reponsibility of the service provider. This includes security compliance testing, scans, certificates, etc.

Cons:

- Control – the customer has little control over the application other than who has access. The customer can alter configurations, but not to customize the core functionality.
- Vendor lock-in – switching to a new vendor may become difficult, especially with customizations.
- Patches/Upgrades – Patches and upgrades to the software are automatically applied (more often on a scheduled timeframe). There will not be an option to back out of certain patches or upgrades as the customer has may not have a say in the pre-established SLAs, maintenance windows, etc.
- Integration – integrating with on-premises data and applications may require additional effort, since the data is hosted by the service provider.

Platform as a Service (PaaS)

The customer is provided the ability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Some examples include: AWS RDS, Azure App Service, etc.

Pros:

- Server-less Architecture – the customer does not have to manage hardware, operating systems, database systems, and programming stack servers are not required to stand-up the components of the solution. This leads to faster implementation of the solution as there is no installation of the platform required.
- Allocated Resources – is configurable and can be scheduled and scaled in most cases, if required.
- Features – more features are readily available, which would otherwise require installation and configuration of additional components.
- Backups – are easily handled with standard and established procedures.
- High-Availability and Redundancy – can be configured.
- Security – is implemented with industry best practices for the platform.

Cons:

- Vendor lock-in – switching to a new vendor may require coding changes, and re-architecting, which can be time consuming, based on the complexity the solution.
- Patches/Upgrades – Patches and upgrades to the platform are automatically applied (more often on a scheduled timeframe). There will not be an option to back out of certain patches or upgrades.

Infrastructure as a Service (IaaS)

The customer is provided the ability to provision processing, storage, networks and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications and possibly limited control of select networking components.

Some examples include: AWS, Azure, Rackspace, IBM SoftLayer, etc.

Pros:

- Custom Architecture – the customer has complete freedom in designing the architecture as required by the applications. This means that the customer must manage operating systems, database systems and

programming stack servers. This provides complete control to building a custom architecture and implement custom components.
- Allocated Resources – is configurable and can be scheduled and scaled, if required.
- Backups – are handled with customer standards and established procedures.
- High-Availability and Redundancy – can be configured using customer solutions.
- Security – is implemented with industry best practices by the customer.
- Vendor lock-in – switching to a new service provider most likely will not require rearchitecting the solution and coding changes.

Cons:
- Maintenance – Since the architecture is designed by the customer, the customer holds the responsibilitues of administering and maintaining the entire architecture, which could include security, firewalls, monitoring, alerting, etc.
- Patches/Upgrades – Patches and upgrades to the to the infrastructure have to be managed by the customer.

WHY CLOUD?

Cloud is a Fundamental Shift in IT

Cloud computing enables IT systems to be scalable and elastic. We as OCIT, do not need to determine their exact computing resource requirements upfront. Instead, we provision computing resources as required, on-demand. Using cloud computing services, OCIT does not need to own data center infrastructure to launch a capability that reliably serves thousands of concurrent users, but instead can leverage the **pay-as-you-go** model for provisioning new infrastructure.

Using a public or community cloud like AWS or Azure would give OCIT access to infrastructure and services relatively inexpensively, in minutes. In our current environment, it would take months to procure and configure comparable resources and significant management oversight to monitor, maintain and upgrade systems. Applying cloud technologies across OC can yield tremendous benefits in efficiency, agility, and innovation.

Efficiency Improvements will Shift Resources Towards Higher-Value Activities

Improvements in efficiency will be seen in software applications and end-user support. These savings can be used to increase capacity or be reinvested in other alternatives, including citizen-facing services and inventing and deploying new innovations.

Services will be more Scalable

With a larger pool of resources to draw from, individual cloud services are unlikely to encounter capacity constraints. As a result, services hosted in the cloud would be able to more rapidly increase capacity and avoid service outages. Given appropriate service level agreements and governance to ensure overall capacity is met, cloud computing will make the OCIT's investments less sensitive to the uncertainty in demand forecasts.

Agility Improvements will make Services more Responsive

Cloud computing will also allow OCIT to improve services and respond to changing needs and regulations much more quickly. With traditional infrastructure, OCIT's service reliability is strongly dependent upon the ability to predict service demand, which is not always possible. Cloud computing will allow OCIT to rapidly scale up to meet unpredictable demand thus minimizing similar disruptions. Notably, cloud computing also provides an important option in meeting short-term computing needs; applications need not invest in infrastructure in cases where service is needed for a limited period of time.

Innovation Improvements will Rapidly Enhance Service Effectiveness

Cloud computing will not only make our IT services more efficient and agile, it will also serve as an enabler for innovation. Cloud computing allows the OCIT to use its investments in a more innovative way and will help OCIT take advantage of leading-edge technologies.

Assets will be better Utilized

Low utilization is not necessarily a consequence of poor management, but instead, a result of the need to ensure that there is reserve capacity to meet periodic or unexpected demand for key functions.

With cloud computing, total infrastructure resources are pooled and shared across large numbers of applications and organizations. Cloud computing can complement data center consolidation efforts by shifting workloads and applications to infrastructures owned and operated by third parties. Capacity can be provisioned to address the peak demand.

As utilization is optimized by migrating workloads to the cloud infrastructure, more value is derived from the existing assets and in-turn reducing the need to continuously increase capacity which means less expenditure on hardware, software, operations, maintenance, and power consumption.

Portability and Flexibility

Cloud computing gives OC the flexibility to alleviate capacity problems with on-premises infrastructure and hence provide the option to be portable with application deployments. Converting Capital Expense budget into Operational Expense helps us better plan and utilize our infrastructures in the cloud and on-premises. Having the option to deploy applications to multiple infrastructure platforms where optimal configuration for performance, reliability and cost can be selected based on the application requirements.

CREATING THE CLOUD CULTURE

The shift toward a Cloud First mindset requires a shift in culture. This will be an ongoing shift, in which we will need to exemplify and improve our collaboration throughout the entire organization.

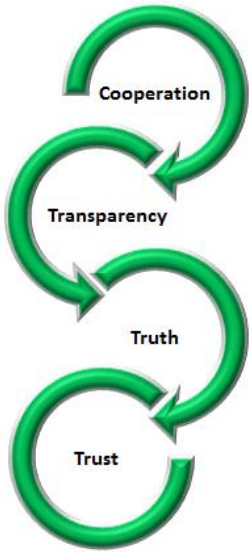

Figure 4: Oakland County Culture of Collaboration

Building off this model of culture of collaboration as shown in Figure 4, we are recommending the following roles to help ensure Collaboration and a clear delineation of responsibility.

IT Steering – This group will be responsible for setting the strategic objectives for the effort, securing funding and providing continual change management support for the mind set change. This will start with helping share the message of the mindset through the celebration of successful events.

Architecture Team and CTO – This group will provide the current state and future strategic direction for this effort. The team will assist in the planning of cloud development, execution and integration strategies on a project by project basis. This group will identify and lead the implementation of governance of Cloud which will balance between performance, optimization, fiduciary and fiscal responsibilities.

IT Security and CISO – This group will establish the requirements for security, compliance and data. The group will also consult on the execution of individual projects ensuring the alignment to the requirements and constraints defined by the team. This group will have representation in establishing the governance process.

Applications Team – This team is responsible for the execution of projects to the Cloud First mindset. This team will ensure the business and service delivery needs are implemented in the most effective and efficient manner. This group will have representation in establishing the governance process.

Server and Network Administration - This team is responsible for the day to day operations of the cloud environment. This includes monitoring performance servers and network. This group will have representation in establishing the governance process.

We will leverage our new Technical Design Review Process for the Architecture, Security, Applications and Server and Network Administration Team to collaborate on the right solution on a project by project basis.

ROADMAP FOR CLOUD MIGRATION

Figure 5 shows the overall roadmap for cloud migration and adoption for Oakland County. It is broken into multiple phases (color-coded), each of which will be discussed below.

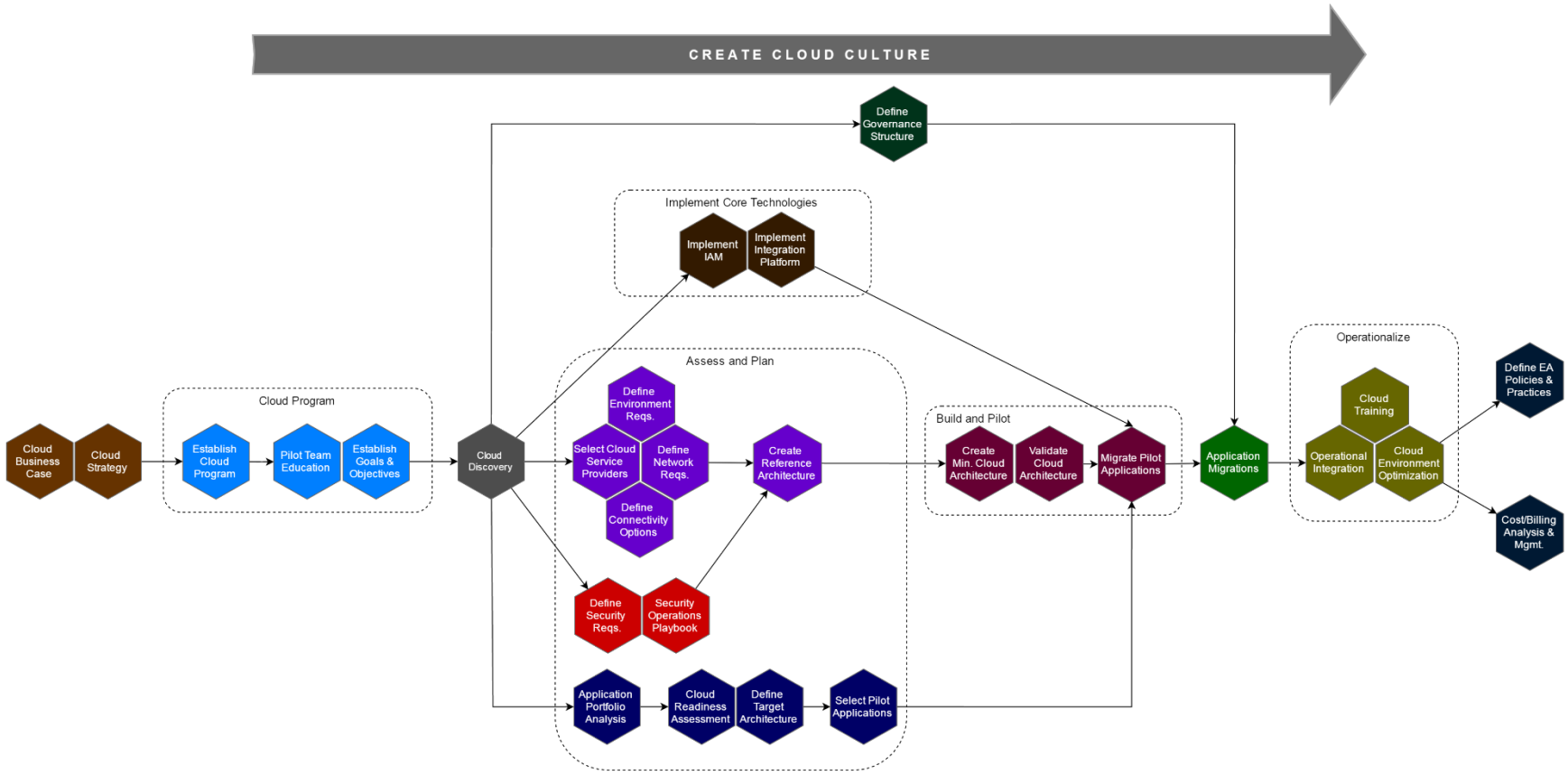

Figure 5: Oakland County Cloud Roadmap

1. Create a Cloud Strategy

A cloud strategy will increase the understanding of how decisions about the cloud can affect and improve the delivery of work at OC. It will help us understand best practices, which will translate into speed and agility to improve availability and delivery of software and services for OC customers. It will also contain the definitions of cloud computing in terms of Oakland County's view and a roadmap for how implement a Cloud First strategy.

2. Establish a Cloud Program

The first step on the Cloud Roadmap is to establish a cloud program and identify projects to implement the strategy.

The Cloud Program will:

- Gain the understanding of cloud computing and infrastructures.
    - Research the latest technologies in provisioning servers and environments.
    - Get trained on cloud technologies and best-practice implementations.
    - Gain extensive knowledge on provisioning “Infrastructure as Code”.
    - Develop and implement cloud models needed for OC's future based on migrations and further resource needs.
- Evaluate the current cloud deployments and make suggestions for improvement or migrations to new OC standards.
- Have a cloud ready environment available for migrations and future deployments.
    - Prepare governance and automation procedures for IaaS, PaaS and SaaS models.
    - Implement security policies.
    - Establish standards for communication with on-premises infrastructure and resources.
    - Determine the integration platforms and processes for cloud services.
- Establish Goals and Objectives for Cloud implementations.
- Migrate pilot applications to the Cloud.
- Begin the migration process with Application services.

3. Cloud Discovery

This phase will identify and inventory existing Oakland County Cloud IaaS, PaaS and SaaS deployments. These services will eventually be brought under the standard policies and procedures that will be established as a part of the Cloud adoption and implementation.

4. Define Governance Structure

Policies and processes for governance in the Cloud environments will be established and implemented in this phase. This includes, but is not limited to support, monitoring and alerting, SLAs, patching, etc.

5. Implement Core Technologies

To be successful in migrating applications to the cloud environments, core solutions need to be in place. Here are some of the solutions identified:

IAM – An upgraded SaaS based IAM solution will greatly reduce the amount of manual effort involved in integrating users to cloud platforms and applications. An IAM solution provides:

- Standard authentication method for applications migrating to the cloud.
- Standard authentication method to authenticate and administer cloud resources.
- Standard authentication method for SaaS applications.

Integration Platform – Integration platforms help different applications and services talk to and share data with each other. An integration platform helps:

- Ensure that the same datasets are being used across different applications. Metadata and versioning ensures the data is kept consistent.

- Integrate different types of applications independent of platform, programming language or operating system, so they can be bound together in workflows and processes.
- Collaborate between distributed and scattered applications, regardless of where they are deployed.
- Take security considerations into account so that data is shared is only with the right resources.

6. Assess and Plan

Requirements for the cloud environments will be gathered after consultations with the appropriate groups within OC and external vendors. These requirements will not be fixed, but will be living documents as they will change as the underlying cloud technologies change and as our experience with the cloud grows.

Select Cloud Service Providers

This phase will comprise of researching and defining the criteria of when to use cloud environments for Oakland County. We will position Oakland County for innovation and provide the flexibility of using the right environment for each solution.

Define Cloud Environment Requirements

This step of the cloud environment requirements phase will determine the requirements for logging, log retention, monitoring, alerting, reverse proxy, load balancing, PaaS vs. IaaS, storage types, VM type evaluations, High-availability, DR, etc.

Define Network requirements

This step of the cloud environment requirements phase will be used to determine the IP address ranges, subnets, Firewall requirements, firewall logs and retention, etc.

Define Connectivity Options

We have identified the four methods to connect to cloud environments:

ISP/Internet **–** This will be the primary method of connecting to the cloud and will be used for Cloud Administration and all hosted Web Applications and services in the Cloud. This requires that our ISP/Internet connectivity is robust, secure and reliable at all times.

IPsec VPN **–** This will be used for back end connections to data and databases hosted in the cloud, non-public applications hosted in the cloud that require dedicated/sustained bandwidth and cloud administration activities that require dedicated bandwidth. Since this also uses internet bandwidth, reliability of our ISP connections is paramount.

Bonded Connection **–** This will be used for secure, private connections to the cloud environment where connectivity and bandwidth are mission critical. This is a more expensive option and should be utilized judiciously where there cannot be any compromise in the reliability, security and performance of the connection.

SD WAN - This will be used for secure private connections to the cloud environments where reliability, redundancy, connectivity and bandwidth are mission critical. This will also help prioritizing and managing the cloud bandwidth including bonded connection.

Cloud Security Requirements

Security is a shared responsibility between Oakland County and the Service Provider. This applies to both SaaS and PaaS/IaaS deployment models. A high-level overview of the responsibilities is indicated in Figure 6.

Even though the infrastructure provided by Public, Community and Hybrid IaaS and PaaS service providers is shared between multiple customers, security and isolation is provisioned by virtual networks for each customer. This guarantees the security of customer data within the virtual network.

This phase will identify and enforce the security requirements and standards in the cloud.

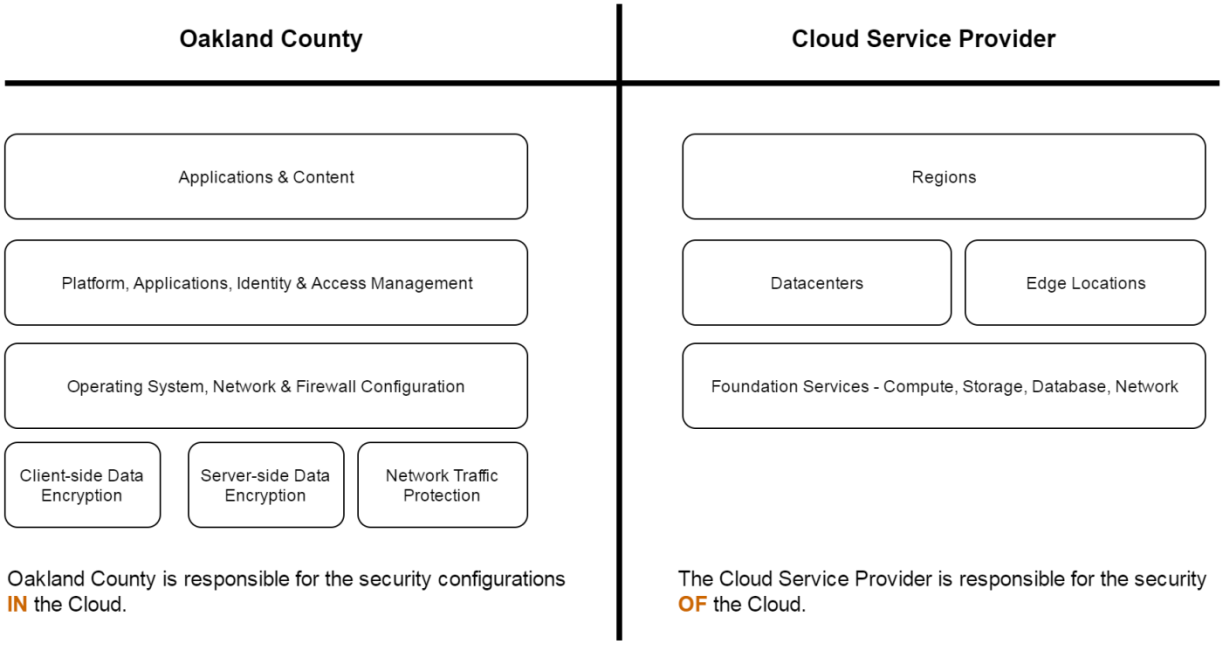

Figure 6: Cloud Security responsibilities

Create Reference Architecture

Once all the requirements are gathered, a reference architecture can be created for applications and services that will be hosted on the Cloud Architecture. This architecture will include options for high-availability, redundancy and DR and will be tested out with the pilot application deployments.

Applications Assessment and Readiness

Oakland County's existing application portfolio should be evaluated to determine next steps in migrating to the cloud. We have identified the following paths each application can take as shown in Figure 7. We will evaluate solutions to manually migrate or automate migrations using third-party products.

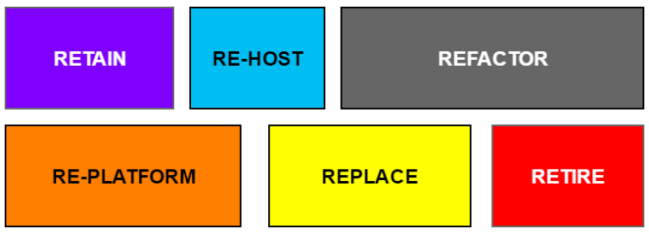

Figure 7: Application Migration Paths

Re-Host (Lift and Shift) – This type of migration will be simplest, where the application can be moved to a cloud environment without any changes to the infrastructure or services in the cloud or any changes to the application code.

Refactor (Re-Architect/Decouple) – This is the most complex of migrations where the applications and the infrastructure will have to be modified. A few modules of the application might need to be rewritten to accommodate the migration to the cloud.

Re-Platform (Lift and Re-Shape) – This type migration requires a change to the infrastructure or platform the application is hosted on. For example, we might have to use a different data storage for file systems on the cloud platform. Migrations can be achieved

Replace (Drop and Shop) – This type of migration will replace the existing application with a SaaS application or a COTS application that can be hosted in the cloud.

Retire – These applications are slated for retirement and do not need to be migrated.

Retain – These applications will not be moving to the cloud. There could be various reasons that can affect this decision some of which could be the complexity of the application, integration, or security and compliance.

These migration paths are explained in more detail in Figure 8.

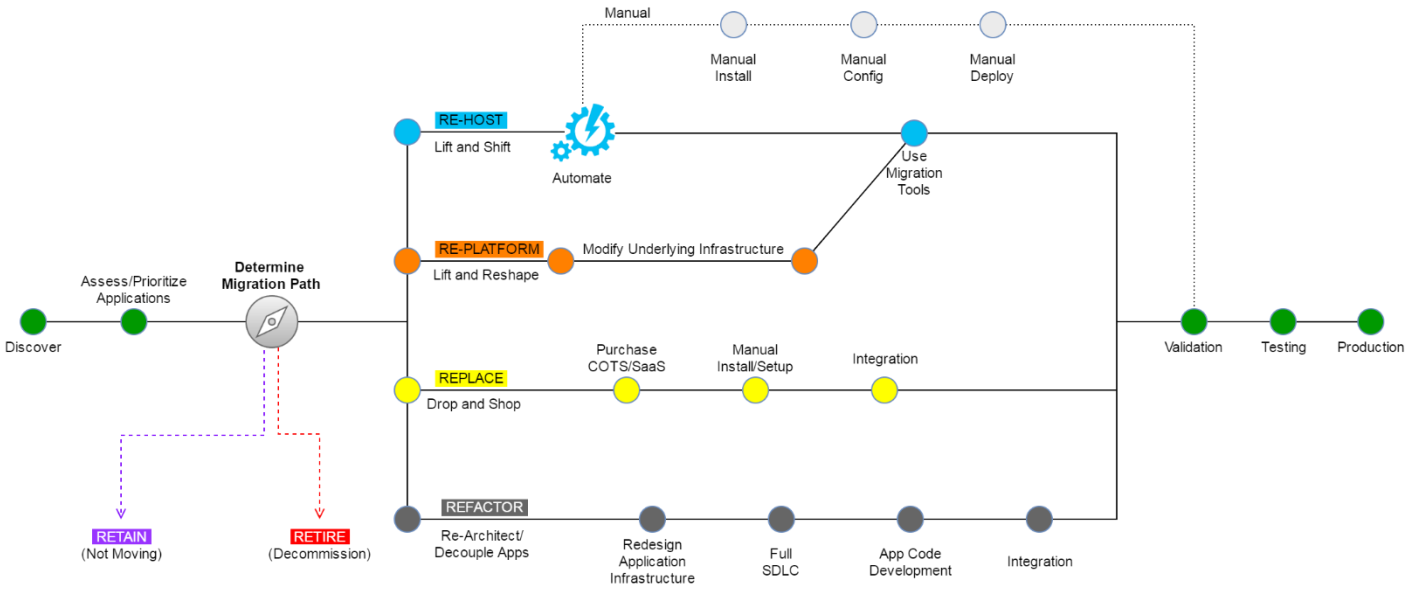

Figure 8: Application Migration Routes

Figure 9 shows the decision tree for new application initiatives at Oakland County. We should look at SaaS and cloud based deployments before making the decision to host the application on-premises.

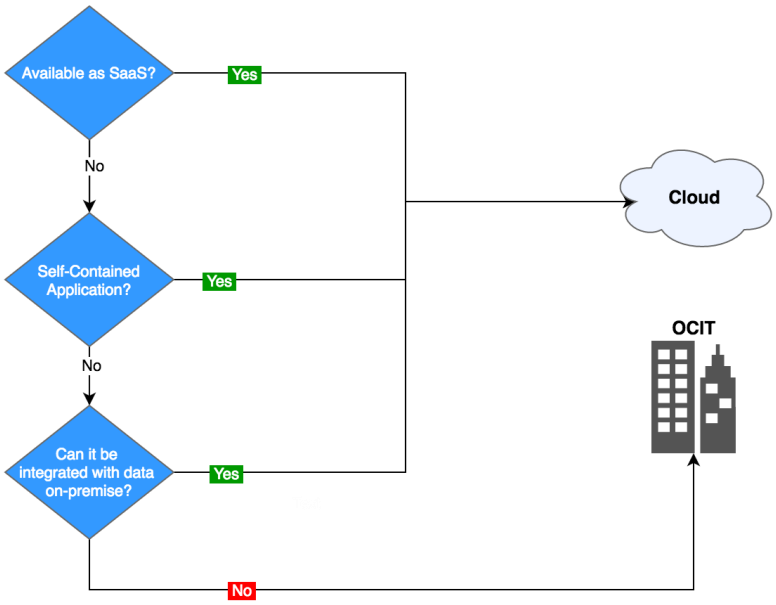

Figure 9: New Application decision tree

Select Pilot Applications

Once the applications analysis and cloud readiness is complete, a list of applications will be selected for pilot migrations. These applications will be selected based on distinct criteria like .Net applications, Java applications, COTS, applications that require high-availability, applications that require auto-scaling, etc.

7. Build and Pilot

Create base (minimum) Cloud Architecture

This will be the phase where we implement the Cloud Environment where and when needed based on the requirements identified in the phase above. At the end of this phase, we aspire to have one functional IaaS based cloud network with IPsec VPN connectivity which meet the overall environment and network requirements. The cloud environment will be scripted so that it can be used to create similar environments within the same service provider. We will also identify any additional solutions required to satisfy the requirements.

Migrate Pilot Applications

This phase will migrate the pilot applications that were identified in the prior steps and will utilize the cloud architecture that has been built. This will provide us with the experience to effectively migrate the rest of the applications and also the benchmarks on estimates and effort to do so.

8. Application Migrations

Once all the phases of the previous steps are complete, we can start with migrating the applications based on the established priorities. This may be accomplished by a migration tool or a manual process.

The high level components of migrating applications to the cloud are shown in Figure 10. Based on the amount of data that needs to be uploaded to the cloud, we have to employ a different method (one of which is manually shipping the data to the service provider).

Figure 10: Application migration phases

9. Operational Integration and Environment Optimization

As we migrate toward our cloud first mindset, the Pilot Team will be leveraging tools for streamlined integration and environment optimization. The Pilot Team will partner with the Architecture Team on the implementation and use of an API integration standard as well as tools to highlight environment performance and tuning. The application readiness assessment will be a direct input into how we start our Cloud moves, which will help in the overall environment optimization.

10. Define EA Policies

The Architecture Team will be defining the standards and policies for Cloud use. These standards and policies will evolve and be refreshed over time. It is imperative to leverage the Technical Design Review Process to ensure alignment with our standards.

11. Cost/Billing Analysis & Management

Cloud is a true pay as you go expense. It is critical to manage and control the cost structure of the environment. A finely tuned and optimized environment is critical to the fiscal success of Cloud. This phase will create the process of how the governance team will ensure proper cloud sizing. The results of this analysis will be reported to IT Steering.

APPENDICES

Appendix A - Abbreviations and Acronyms

- OC – Oakland County
- OCIT – Oakland County Information Technology
- SaaS – Software as a Service
- PaaS – Platform as a Service
- IaaS – Infrastructure as a Service

Appendix B - Systems/Applications Migrations and Considerations

To effectively move applications to a Cloud IaaS/PaaS, we have to identify all the integrations and their endpoints. These integrations will determine the level of complexity in migrating the applications and the processes used to share information.

Here is a template to identify the integrations for applications with examples of possible values:

Endpoint *Examples:* • *SQL Server DB* • *Oracle DB* • *Web Service* • *API* • *Flat Files* • *Web Page* • *Application*	**What Format is used for the data exchange?** *Examples:* • *JSON* • *XML* • *TXT* • *CSV* • *N/A*	**Which protocol/port is used for communication?** *Examples:* • *HTTP/80* • *HTTPS/443* • *TCP/1433*	**Which application/process is accessing the endpoint?** *Examples:* • *Batch process* • *Web application* • *Thick client application*	**Who is accessing the endpoint?** *Examples:* • *OC user in AD* • *External user in AD* • *Anonymous*	**Is the endpoint the source or destination for the data?** *Examples:* • *Source* • *Destination*

REFERENCES

- Reference Architecture – https://en.wikipedia.org/wiki/Reference_architecture

LINKS

- AWS Regions and Services – https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/
- AWS CJIS Compliance - https://aws.amazon.com/compliance/cjis/
- Azure Regions and Services – https://azure.microsoft.com/en-us/regions/#services
- Azure Compliance – https://www.microsoft.com/en-us/trustcenter/Compliance