Indiana
A State that Works

Cloud Strategy
State of Indiana
September 2019

Version 1.0

Revision History

Version Number	Author	Date	Notes
1.0	Joseph Cudby, CTO	September 2019	Original Version

Table of Contents

State of Indiana, Cloud Strategy - Executive Summary

Improving the lives of Hoosiers with better, more effective services is one of the goals of the State. Our objective at the Indiana Office of Technology (IOT) is to enable you, our agency partners, to deliver on those missions in the most effective way possible. In addition, the objective of the Office of the Chief Technology Officer (CTO) can be summarized in 4 words, “Reduce Time to Mission.”

In March 2019, IOT outlined three strategic priorities that will allow us all to reduce time to mission.

1. Hybrid Everything – how to enable you to consume the right resource in the right place at the right time.
2. Development Velocity – how to enable you to use the right development tools & processes to deliver new online tools to your constituents more rapidly.
3. Data Exchange – how to enable you to share data more effectively within your internal application portfolio, between agencies and between agencies and external constituents.

Underpinning each of these strategic priorities is the clear objective to extract the maximum value out of the assets that exist in the enterprise. Consequently, it is in the best interest of our tax payers to use existing purchases, contracts and vendors and prioritize the evaluation of the applicability of existing assets to the new use cases over new purchases with new vendors.

Finally, IOT will work with our partner the Management Performance Hub (MPH) to define a standard process for dealing with Big Data and Artificial Intelligence projects across all agencies. IOT & MPH will combine the technical and legal tools at our disposals to support, understand and evaluate new tools & techniques.

Why does this strategy matter to our Agencies?

The state employs smart, motivated, mission-focused individuals & teams that want to be innovative and try novel ways to deliver services, BUT are unsure how to test their ideas.

By its very nature, most cloud capabilities can be consumed for short periods of time on a small scale. This allows new mission-ideas to be tested quickly, at small scale and at very low financial risk. If the test is unsuccessful, shut down the tech, stop paying and try again. If it is successful, it can be scaled up slowly to accommodate more constituents and refine processes.

IOT’s senior executives are critically aware of Cyber Security Risks and the value of a Hoosier tax dollar. These folks want ways to look their constituents in the eye and let them know that they are good stewards of their personal data and are striving for efficiency with the tax dollar.

“Cloud”, as defined later in this strategy document, has enormous potential to drive efficiency and reduce the risk of loss of personal data.

IOT’s commitment to the Agencies

The Indiana Office of Technology is committed to learning from our Agency Partners about their challenges and, with the State Enterprise of 36,000 employees in mind, make smart decisions about people, process and technology. These decisions will look to balance the need for Agility & Innovation with Security & Efficiency.

State of Indiana, Digital Transformation Council

A critical venue for IOT to listen and learn from our Agencies is through the State's Digital Transformation Council. This collaborative team is led by the State Chief Information Officer (CIO) driven by the CTO, with participation by key agency partner CIO's including those from DOR, IDEM, INDOT, ISDH, FSSA, MPH, BMV and IDOA.

The intent of the Council is four-fold,

- To solicit feedback and input from these leaders regarding their plans, business challenges and provide a forum for sharing lessons learned, and best practices.
- Through curated exposure to forward thinking executives, consultants & vendors, paint a vision of the Art of the Possible.
- To solicit feedback regarding IOT's roadmap of products, services and "State Ready" cloud capabilities.
- To identify specific strategic areas of interest at an Enterprise Level and establish working groups to dig deeply into those areas.

At time of writing, there are three working groups

- Office 365 Adoption - with the intention of extracting the maximum value from the States' Enterprise-Wide Office 365 Subscription.
- Development Velocity – with the intention of understanding the agencies' development tools, techniques and priorities. Then, identify Enterprise capabilities that meet the agencies where they are to increase development velocity.
- Data Exchange – with the intention of understanding the agencies' current data exchange situation, tools, techniques and priorities. Then, identify Enterprise capabilities that meet the agencies where they are to enable data to be exchanged.

Conclusion

The remainder of this document will go into details of why the State will focus efforts and energies with a small portfolio of Enterprise Scale, trusted partners and not be distracted with a large portfolio of "Best Of Breed" point solutions.

It will also explain how this focus will allow IOT to deliver a powerful portfolio of "State Ready" capabilities that can be implemented quickly and effectively for Agency Workloads with the outcome that Agencies Reduce Time to Mission.

Thank you for your attention & support.

Joe Cudby
Chief Technology Officer

Cloud Computing Baseline

What Cloud is not -Utopia.

The Cloud Service Providers (CSP's) provide a huge range of capabilities that are like Legos. As any 10-year-old will remind you, Lego's are not delivered assembled; the purchaser follows the manual to build the model. Cloud services are the same, it is incumbent on the purchaser to understand how to put it all together in a way that securely meets business requirements, and then spend time to optimize usage over time.

Definitions

If you ask folks that are old hands and those that are new to Cloud, everyone has a different definition or expectation. Consequently, for the purposes of a single agreed standard, the State will use NIST Special Publication 800-145's definition of cloud services. These descriptions and definitions are repeated below for clarity.

Cloud Essential Characteristics:

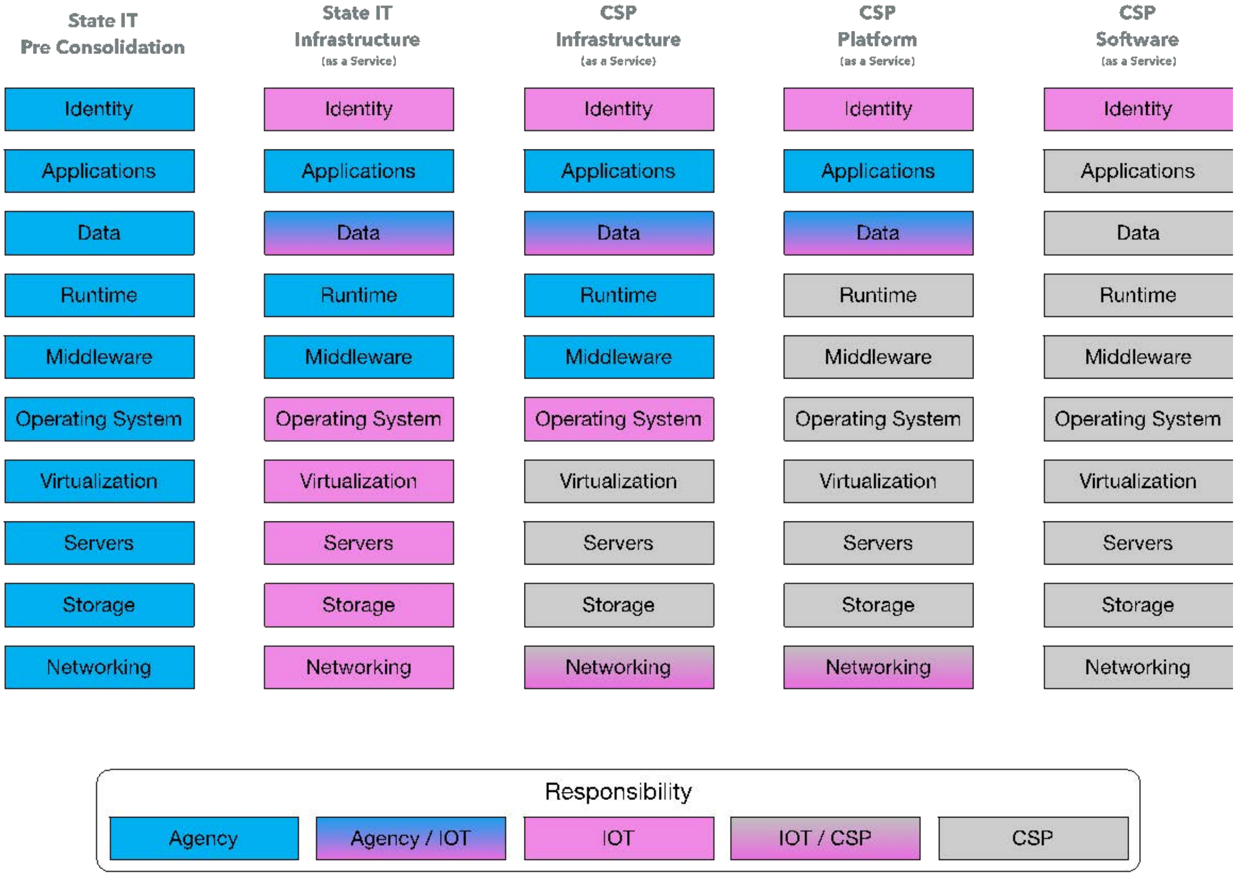
- On-demand self-service.
  - A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- Broad network access.
  - Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- Resource pooling.
  - The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- Rapid elasticity.
  - Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- Measured service.
  - Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

- Software as a Service (SaaS).
  - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer 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.

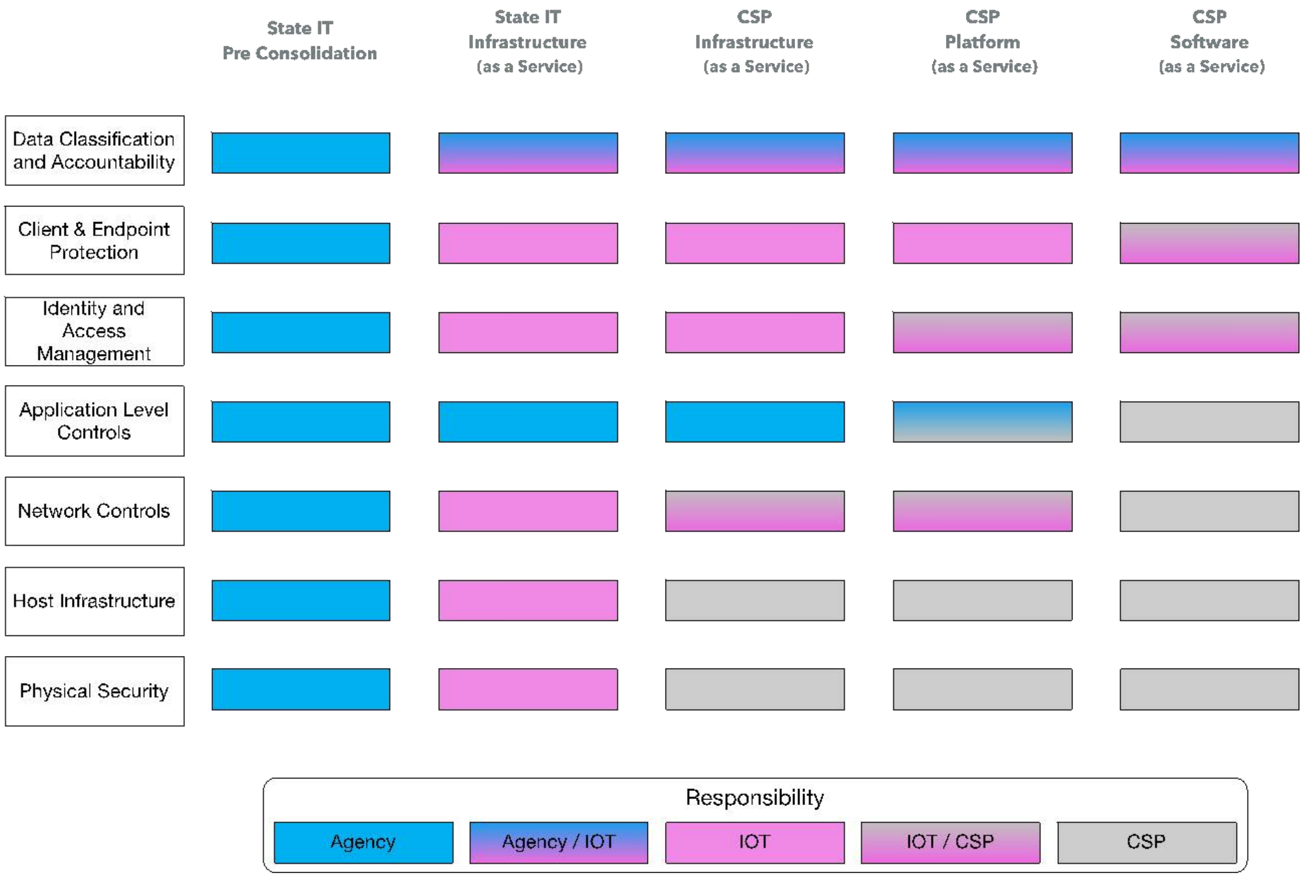
- Platform as a Service (PaaS).
  - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- Infrastructure as a Service (IaaS).
  - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
- Shared Operational Responsibilities in CSP models
  - The Graphic below illustrates the responsibility for technology at the State in these models. The far left indicates Traditional IT, or Pre-Consolidation where the Agency was responsible for everything, to Post-Consolidation with the Creation of IOT, through to how Agency's, IOT and CSP's would be responsible for infrastructure in the models above.



State IT Pre Consolidation	State IT Infrastructure (as a Service)	CSP Infrastructure (as a Service)	CSP Platform (as a Service)	CSP Software (as a Service)
Identity	Identity	Identity	Identity	Identity
Applications	Applications	Applications	Applications	Applications
Data	Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware	Middleware
Operating System	Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking	Networking

- Shared Security Responsibilities in CSP models

- The Graphic below illustrates the responsibility for Security at the State in these models. The far left indicates Traditional IT, or Pre-Consolidation where the Agency was responsible for everything, to Post-Consolidation with the Creation of IOT, through to how Agencies, IOT and CSP's would be responsible for infrastructure in the models above.



Deployment Models:

- Private cloud.
    - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
    - The State's Data Centers fall into this category.
- Community cloud.
    - The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
    - "Government Clouds" fall into this category. The CSP's have built the logical, physical and procedural controls to allow the infrastructure to meet Government Compliance requirements. NOTE – due to the extra work involved in certifying new capabilities, there is a lag between availability of capabilities in Commercial vs Government clouds. Sometimes capabilities may not be available at all in Government Community Clouds. IOT works very closely with our CSP partners to understand these limitations, Agency Requirements and identify the appropriate location for a workload.

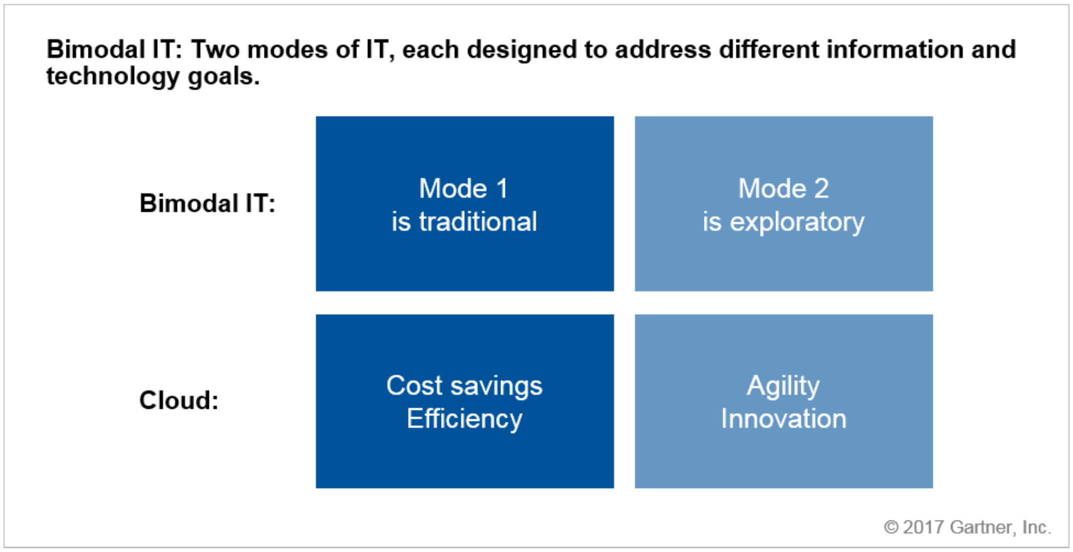
- Public cloud.
    - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- Hybrid cloud.
    - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). NOTE - This model would include consuming resources in the State Data Centers "On Premises" and resources from one or more CSPs.

"Bi-Modal IT" (Courtesy of Gartner)

Throughout this strategy document, the terms "Agility & Innovation" and "Security & Efficiency" have been used. These terms align to the Gartner model of Bi-Modal IT. More information is included below to clarify what this means and how this model helps IOT clarify our thinking about products & services.

Driving more State services into the Digital Realm, i.e. "Digital Government" puts a number of conflicting pressures onto State IT. Gartner's concept of Bimodal IT can help clarify and explain these issues. While there are many uses of Bimodal concepts, at its heart, Bimodal describes two fundamentally different approaches to problem solving. In a Bimodal IT approach:

- Mode 1 — "Reliable IT" — Emphasizes safety and efficiency
- Mode 2 — "Agile IT" — Emphasizes innovation, speed and flexibility



Bimodal IT: Two modes of IT, each designed to address different information and technology goals.

Bimodal IT:	Mode 1 is traditional	Mode 2 is exploratory
Cloud:	Cost savings Efficiency	Agility Innovation

© 2017 Gartner, Inc.

- Cost and efficiency — Primarily financial issues, aligning with Mode 1.
    - This will often include discussions around capital expenditure (Capex) versus operating expenditure (Opex), total cost of ownership (TCO), reduced complexity and leverage.
- Agility and innovation— Primarily opportunity issues, aligning with Mode 2.
    - This will often include focus on speed, time to mission, and business and IT agility.

NOTE: The difference in the two modes needs to be understood, the mission outcomes of the efforts valued and projects will be implemented and managed differently.

What is “State Ready”?

What does it mean for a CSP capability to be State Ready? In essence, “State Ready” means IOT can fulfil our role as Service Broker and deliver something for agencies to consume in a turnkey fashion.

State Ready requires that IOT understands how to set up and configure the services in alignment with the State Security requirements, define the operational model with associated roles & responsibilities, and then bill back the Agencies appropriately.

The setup and configuration activities revolve around the policies, procedures, technology configuration necessary to support the State acquisition, security and management requirements.

The Office of the CTO is working with our Partner Agencies and CSP’s to deliver “Just in Time” (JIT) governance. This means that IOT & the Office of the CTO (OCTO) are focused on the services that Agencies need, and not spending time on the myriad of services that they do not. JIT governance is lightweight process designed to enable our Agencies to be agile, innovative and consume Cloud services in a manner that allows them to meet the State’s legislative, compliance and usage guidelines.

Since the nature of JIT governance is agile, in time there will be a body of governance, best practices and other guidelines developed but not a monolithic guidance document or standard.

Putting the CSP capability and State Ready requirements into a “Whole Product”

“The cloud may be a unicorn, but unicorns still poop, and they need someone to clean up after them.”

Taking ideas from Geoffrey Moore’s “Crossing the Chasm” and his model for technology adoption, in addition to the cloud technology itself, the following are needed for a successful implementation. The below and other elements noted later create a “Whole Product.”

- Pre-Sales Consulting (What do I need to solve my business challenge?)
- Procurement & financing (How do I pay for it contractually and on an ongoing basis? Can I optimize my spend?)
- Implementation support (How do we get this capability up and running to deliver on our mission?)
- User & Administrator training (How do we get our user community up and running?)
- Support, Optimization, Upgrades (How do we operate and maintain the thing we purchased with the people and processes we have?)
- Third party plugins to fill gaps (We need something that does “e-signature”, for example, and the vendor does not do it, how do we solve that challenge?)

The Office of the CTO recognizes that Services from any CSP are capabilities, but not a complete solution, not a “Whole Product” and certainly not State Ready out of the box.

Buying CSP capabilities (Legos’s) and hoping to build a model without the State Ready Whole Product (an instruction manual) is fraught with risk. These risks are due to people, process and technology gaps, which include:

1. Understanding the Art of The Possible is low, leading to business leaders asking vendors for a known solution rather asking for innovation.
2. Lack of expertise in the Agency in understanding how to evaluate new technology options, leading to confusion in prioritizing requirements, and sub-optimal choice.

3. Lack of expertise in the Agency to understand how to implement new technology, driving increased risk and extended timelines.
4. Lack of Agency expertise understanding how to manage projects with resources and partners that are no longer hosted in the IOT State Data Center.
5. Lack of resources in IOT to support CSP capabilities that have not been made “State Ready.”
6. Poor communication from IOT regarding State Ready capabilities, leaving agencies to figure it out for themselves.
7. Inconsistent messages from State IT opinion leaders leading to confusion amongst Agencies and IDOA
8. Poorly understood acquisition model for Cloud across Agencies, leading to confusion and sub-optimal acquisition plans.

Summary of key “Whole Product” needs

1. Just In Time governance completed for the CSP capability.
2. Ecosystem of trusted partners, aligned with the State standards and goals, in addition to the Agency business requirements.
3. Effective communication to State IT Leaders and their organizations of a road map of cloud capabilities “ready for state adoption”
4. Effective communication of successful use cases identifying the “Art of the Possible.”
5. State Ready way to fill technology gaps in off the Shelf CSP capabilities.

For any cloud strategy to be successful, these gaps will need to be filled by a “State Ready, Whole Product.”

A key to filling the gaps is the Adoption Center, located in the Office of the CTO. Its purpose is to provide assistance to key agency integration personnel to support the aggressive adoption of the new capabilities identified in the services / capability’s road map. (More details on the Adoption Center will follow)

Business Baseline

If we make the assumption that there are two classes of outcomes, Mode 1 - Safety & Efficiency and Mode 2 - Agile & Innovative, a thoughtful hybrid cloud strategy supports each. A thoughtful cloud strategy will evaluate each project and its desired business outcomes.

Business Outcomes

Within the guiding vision of "Reducing Time to Mission," the OCTO will work with our Partner Agencies to evaluate the desired business outcomes. We will work with the Partner Agency to identify which of the outcomes align to Mode 1 v Mode 2, as defined above, and then identify an optimal allocation of Hybrid resources to deliver on those outcomes.

Simply defining the expected outcome as "Greater Efficiency" will not be sufficient.

Benefits

A key benefit of a clear cloud strategy and consistent approach, as outlined in this document, is the ability to take lessons learned from one workload and apply it to another. This approach can ensure alignment to the requirements of the two modes of operation. Using a Workload by Workload approach, we will work with the agencies to identify potential cost savings or service improvements, as well as enabling agility & innovation.

Risks

Lack of Agency Engagement is the biggest risk to the State. The outcome of Agencies going their own way will be a fragmented, insecure and poorly executed use of CSP resources. The probable end state of a fragmented approach will be poor & disparate governance, spotty and ineffective security, limited reuse of lessons learned and few opportunities to take advantage of economies of scale. Successfully achieving mission outcomes will be made more difficult in a fragmented model.

Goals

The key goal of this cloud strategy is to enable the vision "Reduce Time to Mission" by clearly articulating how the State will leverage hybrid resources to drive agility and innovation, while still supporting security & efficiency.

Cloud Service Strategy

When IOT will consume Cloud Services.

IOT will consume Cloud services where they supplement or augment our current offerings in a way that will benefit our Agencies and Tax Payers.

In Mode 1, IOT will be enabled to consume Cloud storage rather than expand hardware on premises, thereby reducing capital expense and moving to a consumption model. IOT will also migrate users H: drives from on premises SAN storage into Microsoft's OneDrive For Business. This will allow the State to take advantage of the Office 365 Centralized Governance, effective collaboration capabilities and overall resilience of the platform.

Then in Mode 2, IOT will consume Azure DevOps cloud-based Continuous Integration (CI) – Continuous Deployment (CD) tool chain and migrate off of TFS on premises. This will speed up our ability to deploy code into the State Data center, as well as CSP infrastructure.

IOT's consumption of CSP capabilities before releasing to the agencies has a number of advantages. We can validate the use case, governance steps, roles & responsibilities and develop some training & best practices for agencies – in other words, confirm that the service is "State Ready."

When IOT will build capabilities on Premises.

We will build out new or additional capabilities on premises where, based on the workload, there is a compelling reason to do so.

For example, this could be the replacement for the Mainframe or the need to meet specific security requirements such as the management of highly sensitive assets (like Domain Controllers).

In addition, if Agencies have legacy applications that are not good candidates to move to a CSP, those will stay on premises and IOT will support the infrastructure.

Hardware Purchases

There will also be workloads where it makes sense to purchase hardware.

Typically, this scenario is where a capability needs to vertically scale – i.e. you need a bigger and bigger box rather than lots of small boxes (Such as SAP HANA). Vertical scaling, plus reasonably consistent usage patterns, do not typically lend themselves to cloud. In this instance, IOT will work with the customer to evaluate the ROI for a Capex vs Opex model.

How IOT will be the Cloud Service broker

Cloud is complex and ever evolving. Consequently, staying on top of the available capabilities equates to multiple full-time jobs. The Office of the CTO has those full-time cloud architects whose sole function is to develop and manage the road map of State Ready CSP Services. There are individuals in the OCTO dedicated to Azure, AWS, SaaS platforms (Office 365, Dynamics / Sales Force), Development Velocity, Data Exchange and Cloud Security & Identity.

These folks have deep relationships with our partners to enable IOT to get to the answer Agencies need quickly.

As discussed earlier, IOT’s objective is to help agencies realize the benefits of cloud by providing the “State Ready Whole Product” and providing ways to fill the people, process and technology gaps between the Promise of Cloud and the actual reality of implementing these capabilities.

IOT will also build out the shared plumbing necessary for any agency to consume the services. For example, this includes high speed, dedicated network connections.

Beyond simply negotiating a contract with a CSP, IOT will engage with CSP’s to curate the appropriate solution that meets the State Agency’s needs. In addition, IOT is making investments into effective & strategic Vendor Management practices that will allow the State to identify trusted partners who understand the direction, financial models and other requirements for successful consumption of Cloud Services by the State.

Financial Models

Governance

When IOT enables an agency to consume CSP resources, someone with Financial Authority must approve the purchase. Moving to the “Pay for what you use” model, there is the likelihood of fluctuations in monthly bills.

Enabling staff with no overall fiscal responsibility to consume additional CSP resources will have a direct impact on overall costs. To manage this fluctuation, IOT will work with the agencies to implement resource management policies, as well as notifications for spend against targets at the CSP.

Also, Cloud is not a one & done activity, there are always opportunities for cost optimization. IOT will work with the agency to provide the data they need to optimize resource decisions on a regular basis.

Pricing

IOT has negotiated a rate card with the cloud providers. All consumption data will be downloaded into Pinnacle on a monthly basis to then bill back to the agencies. IOT will work with CSP’s on an ongoing basis to evaluate pricing vs consumption to ensure that the State is receiving value for tax payer dollars based on our Enterprise Purchase history.

Payment Models

Chargeback

As discussed, CSP consumption is billed directly back to the agency. For fiscal 2020 There is a 25% uplift from IOT on the consumption charges billed to the agency. This uplift is to offset the costs associated with being the service broker and the managed service provider.

- Monitoring & Management
- Contract Maintenance
- Cloud Architect Support
- Governance & Policy development

NOTE: IOT is committed to deliver value to the tax payer & agencies and will examine the costs and usage of Cloud resources through Fiscal 2020 and evaluate charge back models on a regular basis.

Capital Expenditure (CapEx) vs Operational Expense (Opex)

The primary value proposition of Cloud resources is that of consumption-based pricing and an operational cost (rent) model rather than a capital-based (own) cost model. Agency partners need to budget for operational & maintenance costs for services hosted with CSP’s for the **life of the workload**, rather than a single Capex acquisition, depreciation model for hardware. NOTE: This is no different to paying monthly for resources hosted in the State Data Center.

Cloud Principles

“Case by Case” also known as “Workload by Workload” review – NON-OPTIONAL

IOT will work with the agency customers to review each project and associated workload to identity the appropriate resource type and allocation. This is a non-optional step, as one size does NOT fit all. The huge value to our agencies is that we can all take advantage of the learnings, build on success and avoid making the same mistakes.

The Fiscal 2020 objective is for IOT to evaluate State IT Workloads, of which it is aware, against the defined list below.

The Fiscal 2021 objective is for Agencies to evaluate, with IOT’s assistance, new State IT Workloads against the list below. This will require IOT to provide education and support for the Agency IT procurement & technology staff.

Definition - Configuration vs Customization.

Configuration is where existing native capabilities of software or 3rd party add-ons are used to deliver the services. This approach limits issues with future maintenance such as patching, and vastly reduces the support costs.

Customization is where the State would have to write (or have written) code to deliver a missing function. The greater the customization, the greater the challenges with future system maintenance and the greater the support costs.

Typically, configuration is faster and cheaper, but it may not exactly fit an existing business process. Customization can tailor the application specifically to existing business processes; however it is more costly and slower. There is often opportunity to modify a business process (retrain staff, take steps out of a process, perhaps re-order them) to leverage the native capabilities of software to achieve cost savings.

Definition – No-Code / Low-Code

A No-Code solution is delivered, using everything out of the box and simply configuring the software’s native capabilities. Classically trained Developers are typically not needed for this activity, however people trained in the solution are required.

A low-code solution is delivered with minimal customization and can leverage the platforms’ native customization capabilities. For example, writing code to support business rules, or custom UI logic. A full stack developer is typically not needed for this work.

Brokering Services / recommended preference of service

To achieve the “Reducing Time to Mission” vision, workloads will be evaluated against a prioritized list of delivery models. IOT will function as the service broker, with the following as the order of preference for service consumption.

1 – “Configure” an existing platform using a No-Code / Low-Code solution.

The fastest & most efficient option for an Agency to deliver capabilities to their constituents is to configure a solution using an existing Ecosystems of People, Process & Technology.

Consequently, IOT will prioritize “State Ready” platforms. Examples would be MS Office 365 (SharePoint), MS Dynamics 365, MS Power Apps or Salesforce. There are limited contractual requirements for the platform with no installation requirements. Often additional business processes can be implemented on these platforms with existing licensing and staffing.

2 - Consume via Software as a Service (SaaS).

If configuration of an existing platform is not an option, a hosted or SaaS version of a custom solution would be the next best option. We would prioritize SAAS providers where the State already has a contract and integrations. There are requirements for new SAAS vendors that align to State Standards and IOT can provide the State’s SAAS provider questionnaire to agencies.

In the SAAS model, the vendor is responsible for the operations and maintenance of the infrastructure, and often they are using Microsoft Azure or Amazon Web Services. The agency is responsible for the configuration of the software solution and their data.

3 – Buy existing Commercial Off the Shelf Software solution and host with a CSP

If there is no opportunity to configure an existing platform, or identify an existing hosted SAAS version, we would recommend purchasing “Commercial Off the Shelf” software and configuring it, limiting customization as much as possible.

The solution could be hosted at a CSP or on-premises, depending on the requirements of the solution.

~~Ideally~~, The State’s vision is to consume based on “configuration” and avoid as much customization as possible. Avoiding customization is a way to avoid lock in, simplify upgrades and ensure flexibility.

NOTE: In order to avoid customization, it is likely that agencies will need to review and potentially re-engineer business processes, potentially in line with the processes supported “out of the box” in the chosen technology.

NOTE: Development on the IN.gov platform falls into this category. That is a solution that is clearly understood, supported and currently hosts in excess of 200 State applications. The State has opportunity to leverage reuse of existing development assets and lessons learned.

4 – Build - Cloud Native

If there is no existing solution, then building the solution in a “Cloud Native” way would be the recommended approach. Applications typically have a 8-10 year lifecycle, and leveraging the most current, proven tools and techniques will provide the best option at future proofing the development efforts. This option will likely require cultural change in people and processes in the agency, however, very much aligns to the desire to deliver Agility & Innovation.

For existing State applications, there are opportunities to “refactor” the on premises codebase to take advantages of new features and capabilities in a CSP. In this hybrid model, new features could be built at a CSP leaving existing features on premises and over time as more functionality is moved to the CSP, less processing would occur in the legacy system.

For a Mode 2 project, and In this model, there would be extensive use of technologies such as Platform as a Service, Software as a Service and Development Platforms hosted at a CSP. The ideal would be to go deep with the CSPs capabilities.

5 – Build – Legacy Technologies / On Premises

This is not a recommended approach and would be undertaken as a last resort.

“Lift & Shift”

IOT will work with agencies to evaluate the opportunity to Lift & Shift on a workload by workload basis.

Straight Lift-and-Shift migration of existing virtual machines to a private cloud should be a last resort. Making the assumption that the State can achieve Mode 1 Security & Efficiency gains with a “lift & shift” WITHOUT additional work to optimize the implementation is simply exchanging a State Owned and operated data center for another owned by someone **other** than the State. **This process will increase costs**.

HOWEVER, if there is an active effort to optimize the application infrastructure (reduce “over provisioning” of compute, memory & storage resources), re-engineering application architecture, to take advantage of cloud native capabilities (“Pets vs Farm Animals” [1] / “Rapid Elasticity”), a lift and shift may make sense to offset other operational issues.

For example, it may make sense to migrate an existing application as a stop gap while agencies are re-factoring this application to take advantage of Cloud Native capabilities.

“Multi-Cloud”

According to Gartner, there are two main types of Multi-Cloud, Redundant and Composite.

Redundant means that there is an entire copy of a Workload in a second Cloud Provider. This approach carries a lot of overhead and would only be recommended in very specific cases. Please review the Tier 1 - Disaster Recovery paragraph in the Contingency Planning Section of this guide for additional guidance.

Composite means that there are select services from multiple cloud providers to deliver a solution. Where an Agency workload has requirements and IOT has existing “State Ready” capabilities, we will certainly work with agencies to evaluate the operational impacts of linking multiple CSP’s into a single Composite solution.

Cloud Native

There are design patterns that are “Cloud Native” and are aligned to leverage the core capabilities of CSP’s, such as Rapid Elasticity. We will work with Agencies to leverage, where possible, “cloud native” design patterns and capabilities.

Where is the State today?

Inventory

In alignment with the Application Inventory processes maintained by the State CISO, all Agency applications hosted with CSP’s will be tracked in the States GRC systems.

IOT is working with the Project Success Center to simplify the onboarding process to get to a CSP. Additionally, IOT will maintain the list of State Ready CSP services.

[1] https://www.slideshare.net/randybias/architectures-for-open-and-scalable-clouds

Security

Governance

The Office of the CTO is working closely with the State CISO and MPH to apply Just In Time Governance to the CSP capabilities that our Agency Partners wish to consume. This is a key element of "State Ready."

We are also working to establish Tenant Level governance and communicate this to our Agency Partners. These are decisions that are "made once and impact everyone." Agencies may then make additional decisions for their CSP resources that are more restrictive to align with their requirements.

Compliance

The State has tenants in both the Commercial Cloud and Government Community Cloud. As stated before, IOT will work with the Agency and CSP to identify the appropriate location for each workload. Indiana State aligns to FEDRAMP and consequently, wherever possible, Commercial Clouds will be prioritized.

By way of example, the only State workloads that may need to be in Government Community Clouds are those that have CJIS or IRS Pub 1075 requirements. Other standards such as FEDRAMP (FISMA) Moderate, PCI, HIPAA, & SOX are often provided in Commercial Cloud.

Based on the type of services consumed by the Agency, there will be associated Roles and Responsibilities (R&R). As each workload is evaluated, the appropriate R&R will be developed, specifically what responsibilities fall to the CSP, to IOT and to the Agency.

Supporting Elements

Architecture

In alignment with the Bi-Modal IT categorization, and within IOT, there are a number of Cost & Efficiency projects underway. We are focusing on enhancing internal capabilities such as IT Systems Management (Ticketing/ CMDB), monitoring, Billing, CSP Networking and operational skills. The result of these projects will allow IOT and Agencies to more effectively consume CSP services aligned to Mode 2 - Agile and Innovative.

IOT is working on an ongoing basis with each CSP to optimize the State Tenant architecture. This means that IOT will ensure that the implementation supports Central Billing, work with the Agency to collect operational and security telemetry, and to ensure that appropriate Agency Control policies are in place.

Staffing

The Office of the CTO provides architectural support, governance, billing & subscription management.

As of this time, the State has engaged a Managed Services Provider, to manage and monitor the Azure resources for agencies on a 24*7 basis. IOT will also look to engage, in the short term, an MSP with a specialization in Amazon Web Services.

The intention is to train and reskill the IOT internal teams to take on CSP support and operational responsibility, however this will take time. Access to the Cloud MSP's will be provided through a ticket opened through the IOT Helpdesk.

Contingency Planning

As it relates to the State's relationship with CSP's, IOT takes a 3 Tier approach to contingency planning.

Tier 1 - Temporary Disaster Recovery

For Disaster Recovery (DR) the key is to be able to temporarily fail over to alternate capacity. Typically, the State will choose to implement failover from one cloud region to another region in the same cloud. This removes the issue of cross-cloud portability from the problem. IOT's DR team will work with the Agency and CSP to define a DR strategy that meets the mission requirements.

This does not address DR for SaaS applications. This scenario can only be addressed through proper data backup of all SaaS data. IOT will work with the Agency to understand the capabilities of the SAAS provider to achieve data backup suitable to meet regulatory compliance needs.

Note: This may require additional costs and/or third party tools. IOT will work with the Agency to ensure that there are contractual penalties for outages.

Tier 2 - Combatting vendor lock-in

Contracts & Connectivity

As the Service Broker, IOT makes the commitment to our Agencies that we will work for the Service Level Agreements (SLA's) that the State deserves and will work with our Agencies and the service providers to ensure compliance.

The State has multiple cloud contracts and is working with IOT network operations, Internet 2 and the CSP's on consistent access methods targeting the ability to move Mode 1 workloads, with minimal cloud integrations from one provider to another.

In the case of SaaS contracts, IOT will look closely at the costs of data retrieval at the end of the contract term and work with the agency to ensure that these costs and operational requirements are understood.

NOTE: Typically, migrating from one CSP is easier in a Mode 1 based IaaS world than in a Mode 2 PaaS/SaaS world.

Managing Vendor "Lock-in"

Vendor "Lock In" with a CSP can come as a result of working heavily with one vendor and consequently having the costs of changing vendors being incredibly high. These high switching costs, rendering the ability to change vendors uneconomical, is a minimal concern in the CSP market, however avoiding such potential Lock-in is a series of tradeoffs.

NOTE: Open Source is not an alternative to Vendor Lock-in in the sense that you still pick a platform and the ecosystem that supports that platform. You may not have a single commercial vendor that you pay for support, however you are paying someone for support.

Focus heavily with a Primary vendor

Typically, a strategic decision made at the higher levels of the organization to focus on one vendor.

Pro -

- Consistent operational, people and process interfaces with vendor ecosystem.
- Simplified Security tooling and increased visibility.
- Standard tools, technologies, processes for interacting with the platform ensuring the effectiveness of the support team.
- Purchase volumes drive down unit costs.
- Simplified adoption strategy and lower adoption effort leading to greater adoption and reduced single points of failure across the entire ecosystem.
- Clearer choices for State Agencies regarding the tools to pick for the job at hand.
- Leveraging all the capabilities of the cloud platform to deliver against Mode 2 – Agility & Innovation based Agency Mission Objectives.

Con –

- Real or perceived limits to pricing leverage.
- Legitimate switching costs in people process and technology to switch from an ingrained vendor ecosystem.
- Limits on product & service capabilities from one primary vendor may impact agencies ability to deliver on business requirements.
- Security flaws that may impact the entire vendor ecosystems.
- Potential limits on support for third party applications / integrations.
- With appropriate contract management and executive involvement these risks can be mitigated.

Pick Best of Breed

Typically, many decisions made further down in the organization

Pro –

Engineers & Business Analysts are typically given the freedom to identify the "right tool for the job" and given the opportunity to optimize the solution to the individual business requirements.

Con –

This approach leads to fragmentation in technology solutions and capabilities, leading to multiple contracts, multiple support vectors, and often multiple solutions to the same problem. There are support challenges across the IT organization with many single points of failure and confusion amongst the State as to which tool to choose for which purpose.

Reduce the impact of lock-in through a hybrid approach

In order to support Mode 2 - Agility & Innovation goals for a 36,000-person enterprise, IOT will focus its initial efforts and energies with a small portfolio of Enterprise Scale, trusted partners and not be distracted with a large portfolio of "Best Of Breed" point solutions. This focus allows IOT to deliver a powerful portfolio of "State Ready", capabilities that can be implemented quickly and effectively for Agency Workloads with the outcome of Reducing Time to Mission.

This focused approach has the added benefit of supporting Mode 1 - Security and Efficiency goals.

Tier 3 - Vendor Exit strategy

As we discussed earlier, given that each workload is unique and specific processes will vary, IOT will make the commitment to back the Agency and work to minimize the risk of exit both before and after an event. We will follow a framework similar to that outlined below.

Prework: Establishes a foundation for the strategy. During this stage, IOT & the Agency forms a team to:

1. Define the unacceptable conditions that might trigger an exit.
2. Develop and maintain exit migration plans for the Agency.
3. Govern the design of application-specific exit plans.
4. Triage cloud outages and other adverse event to determine severity and actions and assisting with exit decisions.

Phase 1 — Define high-level exit strategy: Gathers the application-specific requirements and alternative provider information needed for building exit plans for individual applications.

Phase 2 — Build application-specific exit plans: The formal phase of taking all the cloud application requirements and dependencies and putting an exit plan together in detailed, documented form. The application or project team must follow the guidance and oversight of the cloud event triage team to develop a detailed exit plan from the cloud service or provider.

Phase 3 — Triage events and determine whether to leave the provider: Defines processes that the cloud event triage team will use to decide whether to initiate an exit plan in response to an event or trigger in the public cloud service.

Phase 4 — Implement the exit plan: Outlines the required steps the application or project team must follow to ensure the original exit plan is still relevant and prescribes the process to exit a public cloud service.