



State of Washington



MICROSOFT OFFICE 365 TENANT DESIGN DOCUMENT AUGUST 21, 2015

Submitted by:

T.H. Maugh
Cloud Solutions Architect
Tel: (917) 388-1249 X1249
Email: thmaugh@microsoft.com





Table of Contents

- 1 Background and Objectives 1
- 2 Approach 2
- 3 Findings 3
- 4 Analysis..... 7
 - 4.1 Option 1 - Consolidated Tenant Design (CTD) 7
 - 4.1.1 Identity 8
 - 4.1.2 Federation 8
 - 4.1.3 Network..... 8
 - 4.1.4 Microsoft Exchange 8
 - 4.1.5 Lync/Skype for Business 9
 - 4.1.6 SharePoint Online and OneDrive for Business..... 9
 - 4.2 Option 2 – Department Multi-Tenant Design (DMTD) 11
 - 4.2.1 Identity 12
 - 4.2.2 Federation 12
 - 4.2.3 Network..... 13
 - 4.2.4 Exchange 13
 - 4.2.5 Lync or Skype for Business 14
 - 4.2.6 SharePoint Online and OneDrive for Business..... 15
 - 4.3 “Hybrid” Tenant Model 16
 - 4.4 Requirement Analysis - Pros and Cons..... 17
 - 4.5 Cloud Position Reference Matrix 18
 - 4.6 Requirement Analysis - Pros and Cons..... 20
 - 4.7 Business Requirements Matrix..... 23
 - 4.8 Solution Impact Matrix 24
 - 4.9 Decision Notes 26
 - 4.9.1 Overall Architectural Complexity 26
 - 4.9.2 Identity Framework..... 26
 - 4.9.3 Federation Topology/Integration 27
 - 4.9.4 Department Autonomy/Isolation..... 28
 - 4.9.5 E-Discovery / Regulatory Compliance 28
 - 4.9.6 Licensing..... 29
 - 4.9.7 Networking / Security..... 29
 - 4.9.8 Support..... 30
 - 4.9.9 Administration 30
 - 4.9.10 Implementation / Operational Costs 31
 - 4.9.11 Governance..... 31



4.9.12 Organizational Considerations 32

5 Conclusions..... 33

5.1 Adoption of Consolidated Tenant Approach..... 33

5.2 Adoption of Multi-Department Tenant Approach. 35

Table of Figures

Figure 1: Consolidated Tenant w/ Management Portal 7

Figure 2: Multi-Tenant (Department) Design..... 12

Figure 3: Hybrid Tenant Model..... 17

List of Tables

Table 1: Requirements Pros and Cons by Tenant Model..... 20

Table 2: Office 365 Business Requirements Alignment Matrix (Microsoft)..... 23

Table 3: Solution Impact Matrix 24



1 Background and Objectives

The State of Washington engaged Microsoft Consulting Services (MCS), a strategic consulting division of Microsoft, to review its selected design choices for Microsoft's Office 365 and Azure offerings. The design choices are twofold: (1) single tenant; and (2) multi-tenant, although there are variations within these two choices.

The State currently has approximately 60,000 employees at dozens of locations in Washington. The employees work for various departments within the State's organizational hierarchy. Several of the departments are relatively autonomous, and to a large extent, manage their own IT services. Most departments use IT services offered by WaTech, a central IT group that assists the various departments with technology decisions and the provisioning of specific technology solutions and support.

As with most large enterprises, the State has expanded its email and collaboration infrastructure over time, adding capabilities and extending capacity as demand has dictated. WaTech offers IT services to departments in order to leverage common State IT investments and services.

With the advent of cloud services, solution providers, such as WaTech, are adapting their service and cost models to incorporate Infrastructure as a Service (IaaS), Platform as a Server (PaaS), and Software as a Service (SaaS), which leverages their existing identity platform. In the case of the Microsoft Active Directory platform, both single tenant and multiple tenant architectures are possible and supported within the service.

This document is intended to assist the State in its design review process; however, it is not intended to provide a prescriptive recommendation. It is a review of the technical design considerations and an aggregation of the agency requirements involved in making a single tenant or multi-tenant design decision to support Office 365 and Azure services.



2 Approach

As a means to obtain the data necessary for conducting the review, a series of “discovery sessions” or “workshops” were held with a number of State departments. These workshops were designed to determine how current IT services were being used, and what features and functions were the most important from business and technology perspectives. The approach was structured as an open dialogue, with business and technology representatives from various State departments. In particular, the following groups discussed their use and understanding of Office 365, along with their specific technical or business needs when it appeared appropriate:

- Department of Ecology
- Department of Fish and Wildlife
- Employment Security Department
- Department of Corrections
- Department of Health
- Health Care Authority
- Department of Financial Institutions
- Department of Revenue
- Department of Labor and Industries
- Department of Transportation
- Department of Social and Health Services
- WaTech (Consolidated Technology Services)

The goal of the sessions was to elicit general comments about the existing Office 365 deployment, departmental requirements and where opportunities for improvement might exist in the collaboration environment. Specifically, the discovery sessions were designed to help understand the key factors governing the collaboration capabilities and needs from both business and technology perspectives. As part of the sessions, MCS s provided basic descriptions and capabilities of the Office 365 cloud services, including brief discussions of the following topics:

- Office 365 Tenant Design Options and Administration
- Network Capacity Concerns
- Firewall, Reverse Proxy and Application Publishing Configuration
- Federated Identity
- Administration and Delegation
- Licensing and License Assignment

In summary, the discovery sessions provided MCS the following information:

- Identification and details of the existing collaboration systems operational environment;
- Desired technical and business requirements related to Office 365 and Azure;
- Incorporation of Statewide IT policies applicable to integration and collaboration, and their suitability in regards to the design methodology presented; and
- Various business factors and relative levels of importance.

The depth of information obtained from each department varied. Some departments focused on the technical concerns while others were more focused on the business impact of potential decisions moving forward. The collective combination of input is summarized in the next section.



3 Findings

The State of Washington has a robust on-premises collaboration infrastructure supporting Microsoft Exchange 2010 (with Symantec Evault for Archiving), Lync and hosted SharePoint. These services are implemented in a single forest, single Microsoft Exchange organizational structure, with WaTech being the centralized Enterprise Services provider. This approach provides multiple levels of operational autonomy for the various State departments at the “child domain” level.

The current on-premises design closely aligns to the consolidated tenant model. It provided an opportunity for the State to reduce costs and complexity through the act of consolidating like components of their collaboration infrastructure. Several departments, such as the Department of Transportation and State Patrol, have their own collaboration environment. This provides a degree of autonomy and control, but arguably, the resulting configuration has also introduced additional complexity in administration and collaboration at a statewide level. Definition of these models and the assumptions behind them are required to appropriately establish context for the collection of data and analysis made in this document. The models and related options are defined below.

Option 1: Consolidated Tenant Design (CTD)

With Office 365, a Tenant is the logical Boundary for Security, Policy and Administration. In a single tenant design all departments would be encapsulated within a single instance of Office 365.

In a single tenant model, WaTech extends the current organizational model (Identity) to a single Office 365 tenant for collaboration, enabling them to maintain a similar set of benefits and controls in regards to centralized management, administration and operational support. With the tenant providing a logical boundary for Security, Policy and Administration, the existing processes and operational practices would transition to the consolidated model with minimal change.

Option 2: Department Multi-Tenant Design (DMTD)

In the Multi-Tenant Department Model, the Tenant is the logical Boundary for Security, Policy and Administration, and each department would be encapsulated within a single Office 365 tenant.

In the Multi-Tenant Department Model, WaTech continues to leverage the existing organization model for identity, but transitions to a centralized service provider in order to support separation of identity for tenant collaboration workloads. WaTech would continue to provide management of the core services that support the on-premises identity management environment, in addition to federated services (ADFS), which will require realignment to meet the requirements of the DMTD model.

In the current environment, departments have their own delegated administration roles. A factor for consideration would be the potentially increased overhead for self-



management, including, support and self-service as it relates to Office 365 services. It's realistic to expect that realignment of some administrative roles (Global Administration, for example) would be considered to align to current service delivery models based on individual departmental requirements.

As stated in Option 1, the Office 365 tenant provides a logical boundary for Security, Policy and Administration. The existing processes and operational practices in the current infrastructure would require an investment in time and resources to address the changes for delegation and administration controls to support the DMTD model.

Although these two models are "in scope" for this document and will be reviewed going forward, there is an additional model that is not provided for as a primary consideration, but warrant noting with some explanation. That model is:

Option 3: Tenant Hybrid Model – Variable Cloud Services

During the review of requirements, the "Tenant Hybrid Model" surfaced as another viable option for consideration as part of the overall design strategy. This option provides for integration of both the consolidated tenant design, in addition to allowances for some departmental tenants based on requirements (Options 1 and 2 combined). In this Hybrid Model, it's assumed that WaTech would continue to provide identity and core infrastructure services at an enterprise level, in addition to continuing to be the service broker for those departments in the Single Tenant.

In the "Tenant Hybrid Model", and as reflected in Option 2, the Multi-Tenant Department Model, additional administration and management of the tenant would shift to the department itself, and there would be multiple integration points for identity, federation and collaboration services as required across the tenant boundaries.

In alignment with the tenant options reviewed in this document, an architectural strategy for determination of the criteria on whether to place a department in a CTD Model vs. a DMTD Model will be required to provide a consistent strategy for implementation. In regards to Exchange Hybrid, the service can only be established between a single Exchange organization and a single Office 365 tenant at a time.

The Tenant Hybrid Model can be considered a viable option, but as a variation of Option 2 that could address specific desires for autonomy and isolation as required by departments and may be a future design consideration by the State. This option is considered out of scope for this document. However, due to it being a subset of Option 2, it is addressed, albeit minimally, in Section 4.3.

MCS determined during the review that the State's existing consolidated architecture is a single, unified infrastructure supporting Identity, Exchange, Lync and Collaboration workloads. MCS also noted that the current approach in regards to the consumption of cloud services is impacted by the following mandated data collection requirements:

- Department regulatory requirements (e.g. HIPPA/FERPA/FTI);
- Department security requirements; and



- Department BAA (Business Associate Agreement) requirements.

In addition, the departments stated that other factors are also deemed to be challenges and that they might ultimately impact the usability of a cloud-based solution. These factors include:

- Multiple Collaboration Services Providers – The intent is to design the future-state architectural solution to allow for multiple collaboration services providers, beyond just Microsoft. This consideration has a direct impact on the overall solution in terms of maintenance services, support services, and the relative cost of each.
- Identity and End User Experience –A focus on the ability to provide a unified approach to the on-premises and cloud infrastructure, and the impact to user perception is necessary for adoption of the platform. It was noted that Exchange and Skype for Business were foundational, “dial-tone services,” and the provision for a single user identity experience was required in order to provide consistency across differing applications where possible.
- Identity Plan - Without a cohesive plan for identity, the introduction of cloud services will drive additional overhead and complexity when addressing future workloads and integration requirements with services from various providers. MCS understands that WaTech has received funding to support this initiative, and is currently working to resolve these issues.

Another main objective of the discovery sessions was for MCS to gain an understanding of the business requirements and priorities that will directly impact discussions moving forward. This section highlights the needs presented by the departments during the discovery process, and sections 4.4 – 4.8 provide detailed information as a result of these expectations.

- *Tighter controls to manage compliance and regulatory requirements.*
 - Department Input: The departments have overall responsibility for regulatory and compliance issues, with WaTech providing and administering the isolation of data in Exchange today. In order to address changing requirements and enforce regulatory controls, some departments are exploring having their own tenant. WaTech is seen as the “man in the middle” from a support and configuration perspective. Some departments see an important benefit of separately managing their tenant and taking full responsibility for their unique compliance requirements.
- *Adaptability.*
 - Department Input: Departments’ business needs change frequently. A level of isolation would allow affected departments to adapt to those changes more quickly without impacting other departments.
- *Reduce technology costs via more efficient service delivery and lower maintenance burden.*
 - Department Input: The concern was present that, in either model, there will be additional charges for services transitioning to the cloud.
- *Agility in adoption of technology.*



- Department Input:
 - Collaboration between departments could improve. There are core IT applications and services that are leveraged, but most collaboration and requirements are managed and supported within the department itself.
 - Business drivers and requirements are often unique to a department. Departments have indicated a need to be able to quickly adjust their technology requirements independently of other department requirements.
- *Improved business continuity and resiliency.*
 - Department Input: Departments want greater control and input to enable an effective business resumption strategy in case of a serious outage.
- *Provide rapid response for department's business requests.*
 - Department Input: Departments understand there are requirements for an enterprise model and a central service organization – but multiple departments are of the opinion that they could better manage their collaboration infrastructure better than WaTech, with the goal of providing better service to their customers.
- *Immediate access to current technology and hardware resources as business demands.*
 - Department Input: Departments have differing requirements that drive the development and implementation of their applications. They need the flexibility to innovate and build out services based on the constantly evolving needs of each department, while minimizing delays resulting from the WaTech approval process.
- *Department autonomy.*
 - Department Input: Departments want more control of the services being provided where possible. There is a feeling that increased transparency and involvement in the support of various workloads would allow them to be more proactive to their customer.
- *Consistent performance and reliability.*
 - Department Input: Departments want more transparency and more administrative control of their paid services. Departments are looking for ways to obtain SLAs for services provided by their provider.

In summary, what Microsoft heard from the departments surveyed indicated:

- A desire for more autonomy and control over their environment based on individual department requirements (i.e. application design and implementation that are for constituent consumption vs. state employee consumption, agility and ability to prototype and stage applications in Azure);

- A need for better communication with WaTech, and to have increased involvement with technology solutions that impact the departments prior to the decision being made rather than after the fact as it's perceived today;
- A need for additional and better support;
- A need for assistance from WaTech in helping meet regulatory and compliance requirements; and
- A need for quicker responses to departments' technology change and addition requests in support of the departments' business needs.

4 Analysis

This section provides an analysis of the data collected and reviewed. First, it's important to establish a basis for the discussion. The two design options listed in the previous section will first be defined and basic assumptions noted before moving into an analysis of each.

4.1 Option 1 - Consolidated Tenant Design (CTD)

The following diagram graphically depicts the key elements of a Consolidated Tenant. Note that there is centralized management of the environment through a management portal.

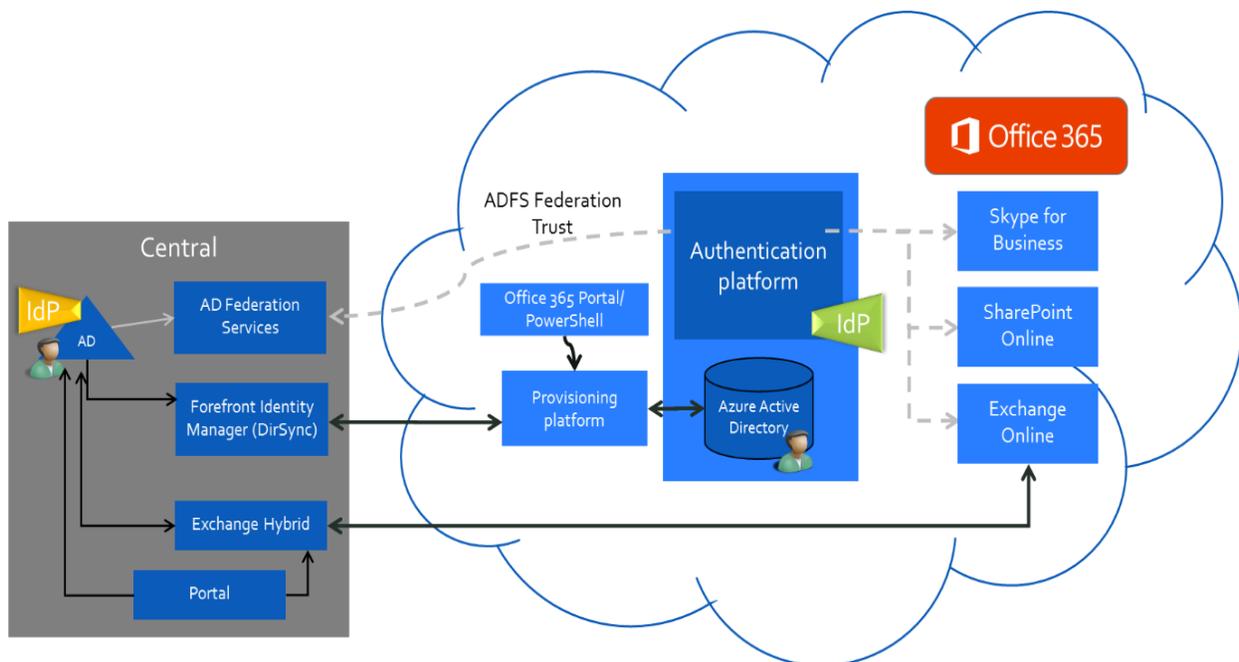


Figure 1: Consolidated Tenant w/ Management Portal

For analysis, certain assumptions are made to complete the exercise. These assumptions are briefly listed below:



4.1.1 Identity

The following assumptions are made related to the Identity features for the Consolidated Tenant:

- Single point for directory synchronization;
- Existing RBAC model for centralized and department delegation would extend to Office 365;
- No changes to the existing Security Groups (SG); and
- No changes to existing on-premises enterprise applications from an identity perspective, as the existing infrastructure is assumed to remain unchanged.

4.1.2 Federation

The following assumptions are made related to the Federation capabilities for the Consolidated Tenant:

- Single Point for Federation, with WaTech providing a single administration source for Active Directory Federation Services (ADFS);
- Single set of common claims rules; and
- Centralized (WaTech) support of federation endpoints across departments.

4.1.3 Network

The following assumptions are made related to the Network for the Consolidated Tenant:

- Resilient access to services available through appropriate network capacity planning; and
- Firewall, reverse proxy and application publishing endpoints on the existing network design to be managed by WaTech. (Note: The current approach has accommodations for increased traffic between the current Internet egress points and Office 365.)

Both the CTD and DMTD models presented are expected to have the same underlying impact on the network, and the ability for the state to consuming the service.

4.1.4 Microsoft Exchange

The following assumptions are made related to Microsoft Exchange for the Consolidated Tenant:

- Hybrid Mechanism (the ability to integrate Exchange to the cloud) available for departments to move in parallel to cloud;
- No requirements for GAL-sync (Global Address Synchronization) as the Exchange organization is a single structure;
- Symantec Evault configuration consistent with current deployment (WaTech would continue to manage existing Evault policies, and provide governance and support for the archive solution.);
- Management of EOP (Exchange Online Protection), DLP (Data Loss Prevention), and Transport Rules would be unchanged (These are global admin abilities within Office 365.



In the consolidated model, these functions are implemented and supported directly by WaTech, and would transition relatively intact.); and

- Management of Distribution Groups (DGs) would be unchanged (DGs would be continue to be managed by WaTech, allowing an enterprise based organization to ensure uniqueness and assign delegation to departments for self-management where appropriate.).

4.1.5 Lync/Skype for Business

The following assumptions are made related to Lync/Skype for Business for the Consolidated Tenant:

- Single directory store for Skype for Business, with no mechanisms/policies to prevent users from communicating directly with other users within a single Skype for Business organization;
- Single model for Federation and Policy Settings with all policy configurations within the tenant being global in nature, impacting all departments;
- SIP (Session Initiated Protocol) domains for Skype for Business to provide the ability to show presence information within various applications (SIP and SMTP address integration in the single organizational model will allow for presence information to be presented to users, with little to no impact on current administration overhead);
 - *** The information provided is a given within the context of the service, and has been provided for planning and awareness.*
- E-Discovery and compliance within Skype for Business available through a single set of policies that will archive IM history to Exchange Online if the user's mailbox is configured for litigation hold (Individual application of policy can be defined per Office 365 at the tenant, department or user level regardless of the solution design.);
- Delegation and RBAC (Role Based Access Controls) necessary and required to allow each department to directly manage its own E-Discovery settings (In Consolidated Tenant, the delegation model directly affects the ability to compartmentalize data between departments.);
- Dial-in conferencing settings available only to users in that tenant (This would allow all users to consume a shared service, using the same configuration applied across the organization boundaries.); and
- Skype for Business Federation enabled on a per tenant basis, meaning that in the Consolidated Tenant model – if federation is enabled for a single department, that federation is available to all departments.

4.1.6 SharePoint Online and OneDrive for Business

Unlike Skype for Business and Exchange, SharePoint Online offers additional options for deployment, along with considerations for on-going use. As the departments weigh their options, rationalization of existing workloads and content will be essential in order to validate an appropriate fit for SharePoint within both models.



As a reference, a comparison of Office 365 services can be found at: <https://technet.microsoft.com/en-us/office/dn788955>.

The following assumptions are made for the implementation of SharePoint Online in a Consolidated Tenant:

- Similar to the current design in place today, the Consolidated Tenant in Office 365 will allow for WaTech to manage Global Settings within a tenant. Any limits established within SharePoint Online, would apply to all departments since they would be centrally managed.
- Storage management in SharePoint Online is another consideration in evaluating the impact of a design model. Depending on the nature of applications deployed, and the overall rate of consumption per department, service limits could quickly become exhausted. Information on the storage limits and features can be found at: <https://support.office.com/en-us/article/SharePoint-Online-and-OneDrive-for-Business-software-boundaries-and-limits-8f34ff47-b749-408b-abc0-b605e1f6d498?ui=en-US&rs=en-US&ad=US>.
- Managing to these limits could require additional operational and administration overhead within WaTech, since they will be establishing collection and site policy and managing storage across the tenant.
- There is (by default) 10GB of storage, plus additional storage of 500 MB per licensed user, with a hard limit of 100GB for site collections across a Single Tenant. There is also an overall subscription limit of 25TB. The base storage limits for Office 365 Enterprise (10 GB + 500 MB per subscribed user) will affect storage values across the tenant. For example, although SharePoint Online for Office 365 Enterprise plans imposes a limit of 1 TB per site collection and a limit of 500,000 site collections, a particular tenant might not sufficient storage available to contain 500,000 site collections of 1 TB each. For more detail on storage limits for SharePoint, please visit the link provided above.
- The central administration team (Enterprise admins) will be responsible for core Governance, monitoring and allocation of resources to ensure a balanced approach to service adoption and consumption.
- The object picker in SharePoint is not limited to one department or another, meaning in the consolidated model, all objects in the directory can be selected from the picker. When using the object picker in a Multiple Department tenant approach, only those objects within the tenant will be displayed. Consideration needs to be applied to make sure the right groups and users are delegated to when considering access and permissions to resources.
- Currently, Office 365 hybrid configuration for SharePoint Online is only supported between one AD forest with SharePoint, and one Office 365 Tenant. It's important to understand that at this time in the service, there are no other supported options for SharePoint Online.
 - *The information provided is a given within the context of the service, and has been provided for planning and awareness.*
- Being able to support Hybrid is a major consideration, as it allows for:



- Search and the ability of being able to search across both on-premises and Office 365 (Online) environments; and
- Business Connective Services (BCS), a feature of SharePoint, and the ability to access data in on-premises applications/systems from Office 365.
- SharePoint profiles are available for all SharePoint Online users in the tenant, and not partitioned per department within the tenant itself. Feedback received by MCS during the discovery sessions was that there is not a pressing need for inter-departmental collaboration, as it was more in line with the ability to collaborate effectively within each department. If the desire is to explicitly block collaboration between departments, implementing the appropriate security constraints in the on-premises environment will need to be in place before extending the infrastructure to the cloud.
- OneDrive for Business in the consolidated tenant model would allow for users to share content with any user within the tenant as an “internal user” since it also has no concept of a department.
 - *The information provided is a given within the context of the service, and has been provided for planning and awareness.*
- E-Discovery and compliance would extend the current practices and approach on-premises to SharePoint online, as eDiscovery centers are created at the site collection level. The consolidated tenant model could introduce additional vectors for data leakage across departments depending on the configuration. It is assumed that WaTech would continue to be the central point of enterprise configuration and service administration when delegating roles out to the departments.
- With approximately 60,000 users currently in the State’s user base, the ceiling of 10,000 unique external users that can be provisioned in the directory (i.e., external users who have accepted sharing invitations) could become a challenge as the size and scope of a large organization could easily pass that threshold. External sharing is enabled per “Site Collection” and OneDrive is considered to be a single site collection.
 - *Office 365 as a service is constantly revolving, and the ceiling of 10,000 unique external users is a defining factor in regards to how the service is presented for consumption today.*

4.2 Option 2 – Department Multi-Tenant Design (DMTD)

The following diagram graphically depicts the key elements of a Multi-Tenant Model. Note that similar to the Single Tenant Model, there is also a centralized management of the environment.

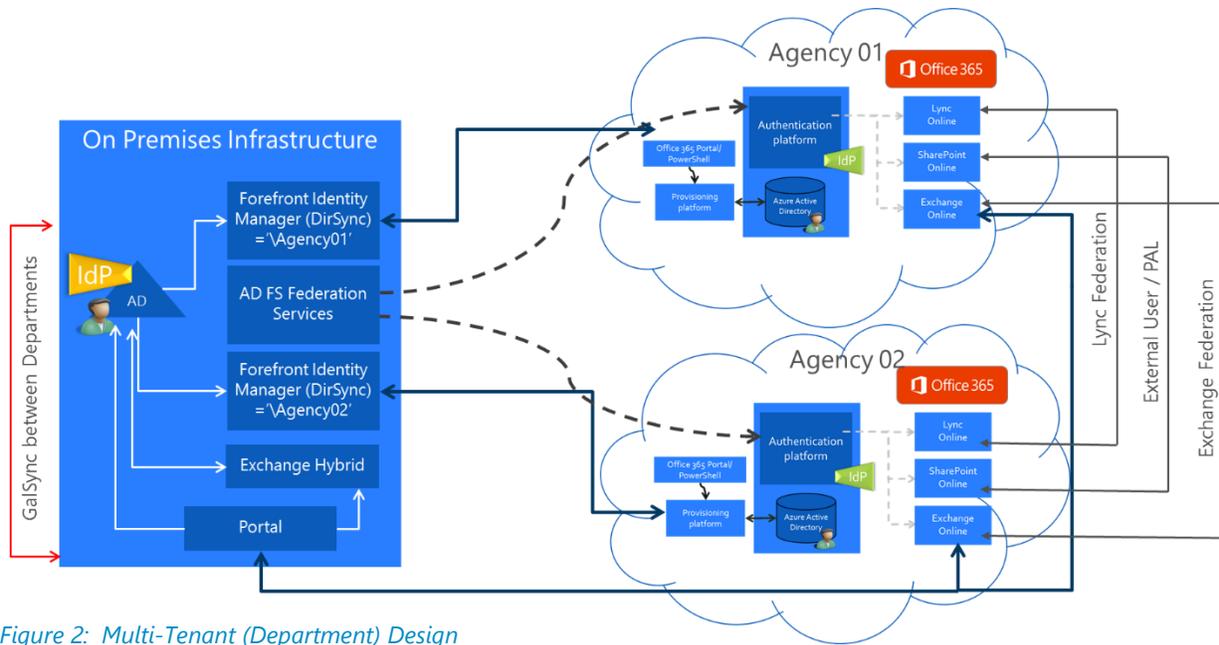


Figure 2: Multi-Tenant (Department) Design

For analysis, certain assumptions are made to complete the exercise. Assumptions associated with the review of the Multi-Tenant Model are briefly listed below:

4.2.1 Identity

The following assumptions are made related to the Identity features for the Multi-Tenant:

- Single point for Directory Synchronization using MIM (Microsoft Identity Manager), or multiple deployments of AAD DirSync with explicit filtering rules (to prevent the unwanted synchronization of users from one tenant into another);
- Existing RBAC model for centralized and department delegation would extend to Office 365, with some modifications depending on administering/ownership model for each tenant;
- No changes are expected to existing on-premises enterprise applications from an identity perspective, as the existing infrastructure is assumed to remain unchanged; and
- Existing Security Groups (SG) supporting the on-premises environment would need to be analyzed and possibly restructured to support the revised design. Enterprise based security groups would continue to be managed centrally – with that group providing naming standards across the architecture.

4.2.2 Federation

The following assumptions are made related to the Federation features for the Multi-Tenant:

- Single Point for Federation, based on the assumption that WaTech would continue to own/service the Federation Services;



- Per tenant ADFS Federation Gateway configuration to support individual tenant namespaces vs. single top level domain configuration of ADFS; and
- Increased administration overhead and complexity due to Individual Claims Rules for each tenant.

4.2.3 Network

The following assumptions are made related to the Network for the Multi-Tenant:

- Network capacity planning and service redundancy for Federation will provide for resilient access to services similar to the Single (Consolidated) Tenant model. The separation of individual departments based on the assumption of single identity and federation endpoints shouldn't change the bandwidth requirements in either model.
- As stated previously, WaTech currently manages the firewall, reverse proxy and application publishing endpoints on the existing network design. The current approach has accommodations for the increase in traffic between the current internet egress points and Office 365.

4.2.4 Exchange

The following assumptions are made related to Exchange features for the Multi-Tenant:

- Hybrid Mechanism (the ability to integrate Exchange to the cloud) to provide rich coexistence would be a limiting factor in supporting transitions. "Which department would be allowed to migrate?" and "How to resolve issues during migration?" are factors that could prolong the implementation time for hybrids, creating a situation where one department's decision could impact other departments.
- Hybrid functionality limitations would make for an extended migration plan, and put additional strain on WaTech resources, as they would be required to perform hybrid configuration and administration tasks while assisting with the migration to individual tenants.
- Requirements for GAL (Global Address Synchronization) as the Exchange organization would be spread across multiple Office 365 tenants. This change in structure would require synchronization planning, filtering planning, and centralized administration overhead in order to validate identity consistency between the on-premises infrastructure and Office 365 tenants.
- Archival configuration would be impacted, as Symantec Evault in its current configuration would require an investment in the migration tooling, with possible ongoing costs.
- A possible end state would be to leverage Exchange Online Archives (EOA) versus Symantec's Evault; however, a comparison of the feature requirements would need to be performed to ensure the existing policy requirements can be met. Moving existing archives to Exchange Online Archives would require an investment in resources (personnel and hardware) to hydrate the data from the Evault archives, validate map retention policies and establish security settings.



- Should Symantec Evault continue to meet the requirements of the departments, then additional cost and resources would need to be planned to separate departments into unique instances of Evault to directly support their tenants. (Note: This needs to be confirmed with the vendor, but the assumption is that it's a one to one relationship with the vault. Departments would have to move to a vault for their own tenant, and as such would have to recreate the policies, hydrate and migrate the data to the new instance.)
- Should the decision to separate departments into multiple instances of Symantec's Evault, it is assumed the department would not take on the administration of their individual vault and the associated policies in place with WaTech while similar, would have to be updated to reflect the decentralized change to archive storage. Each department would require assistance and coordination with WaTech to support the migration off the current platform.
- A level of Enterprise-based architecture and policy for Distribution Groups (DGs) would continue to be managed by WaTech with an emphasis to validate that there is a standard set of guidelines in place, as it's assumed departments will continue to be directly responsible for the creation and implementation of DGs post transition.

4.2.5 Lync or Skype for Business

The following assumptions are made related to Lync and Skype for Business for the Multi-Tenant:

- Skype for Business has a single directory store with no mechanisms or policies to prevent users from communicating within a single Skype for Business organization. In the Multi-Tenant model, federation between departments would be required for the native collaboration functionality provided within the on-premises and consolidated tenant structure. It's also assumed that administration of the service for Skype for Business would be within each department, with coordination with WaTech to support the existing infrastructure.
 - Unlike Exchange and the configuration of GAL Sync, the directory store leveraged for Skype for Business will only natively provide for the selection of users in that tenant currently. There is no integrated address book for Skype to allow all departments to share a unified address list. Users would be responsible for the addition (and deletion) of accounts as required,
- The Federation and Policy Settings in the DMTD model would leverage the natural tenant boundary for having separate federation and policy requirements for Skype for Business on an individual tenant basis. Administration in this model is assumed to be at the department level, not centralized.
- SIP (Session Initiated Protocol) domains for Skype for Business provide the ability to show presence within various applications. SIP and SMTP address integration in the single organizational model will allow for presence information to be presented to users. Each department has their own namespace currently, so this would require some coordination with WaTech to ensure the tenants namespace and federation components are aligned.



- E-Discovery and compliance within Skype for Business will be through a single set of policies that will archive IM (Instant Messaging) history to Exchange Online if the user's mailbox is configured for litigation hold. Individual application of policy can be defined per Office 365 at the tenant, department or user level regardless of the solution design. Delegation and RBAC (Role Based Access Controls) are necessary and required to allow each department to directly manage their own E-Discovery settings. In the Multi-Tenant Model, the Office 365 tenant is the boundary, preventing overlap.
- Skype for Business Federation would be subject to the requirements of the department, and would be implemented as such. Should one department decide not to implement federation with another, those users would not be able to rely on IM/Presence for communications. The assumption is that this would be managed at the department level.

4.2.6 SharePoint Online and OneDrive for Business

The following assumptions are made related to SharePoint Online and OneDrive for Business for the Multi-Tenant:

- While the on-premises administration and identity model would stay relatively intact, the Multi -Tenant approach would transition the burden of configuration and administration from WaTech, as the respective departments would manage Global Settings, and limits directly against their own tenant.
- The stewardship and configuration of tenant level settings would transition to individual department analysts. Being responsible for the enterprise architecture, WaTech would take on an enterprise architecture role related to the infrastructure and standards to provide a continued continuity and consistency within the organization.
- The storage concerns in the consolidated tenant are reduced significantly, as the reduced sizes of the departments as compared to the State as a whole allow for more growth. Storage would transition from being centrally managed by WaTech to each department managing their configuration and deployment of SharePoint components. It's assumed, as stated above, that WaTech would provide an enterprise architecture role in relation to adoption to ensure consistency in regards to a common approach.
- The object picker in SharePoint in the Multi-Tenant approach is now limited to a single department. In the Multi-Tenant approach only those objects within the boundaries of department tenant would be displayed. Similar to the approach for group and user management within the Child Domains on-premises today, this would ultimately extend to the department approach as well.
- Currently, SharePoint Online is only supported to run in hybrid mode between one AD forest and one Office 365 tenant. There are no other supported options for SharePoint Online. This means there would be no true hybrid for SharePoint online with the on-premises organization model. A SharePoint hybrid environment enables trusted communications between SharePoint Online and SharePoint Server 2013. With a "trusted framework," administrators can configure integrated functionality between services and features, including Search, Microsoft Business Connectivity Services, SAP, and Duet Enterprise Online for Microsoft SharePoint.



- In addition to leveraging Active Directory for identity, SharePoint profiles are available for all SharePoint Online users in the tenant, and the Multi-Tenant model would allow them to be configured and portioned based on a department's information architecture, vs. an enterprise strategy. This could lead to inconsistencies across the enterprise in how services are designed and implemented.
- Since all departments in the Multi-Tenant approach are treated as external users, it's much easier to explicitly block collaboration between departments, as the existing on-premises domain structure and the hard boundary of the department tenant would be leveraged to provide those restrictions.
- As stated above, the Multi-Tenant model and OneDrive for Business allow for users to share content with any user within the department tenant as an "internal user". All other departments would be seen as external. This could increase the administration burden back to the departments as they would have to plan for integration across tenants when it comes to inter-department collaboration.
- E-Discovery and compliance would change, as the current practices and approach on-premises to SharePoint are managed by the enterprise services team. Since the department in this scenario now owns the administration and configuration of its tenant, the eDiscovery centers would be directly under the purview of those administrators, and no reliance on enterprise services would be required.
- The multi-department tenant model provides for a different consumption footprint, as the size of the individual tenants would be smaller, making the likelihood of hitting the ceiling of 10,000 unique external users no longer a possible concern as in the consolidated model.
- Departments are responsible for the configuration of external sharing, which is enabled per Site Collection and with OneDrive being a site collection. Specifically, they could enable specific rules that meet the requirement of the department.

4.3 "Hybrid" Tenant Model

Since a "Hybrid" Tenant Model is possible, it bears comment. The following illustration is provided simply to define the model and provide a reference point for any discussions in the future related to this model.

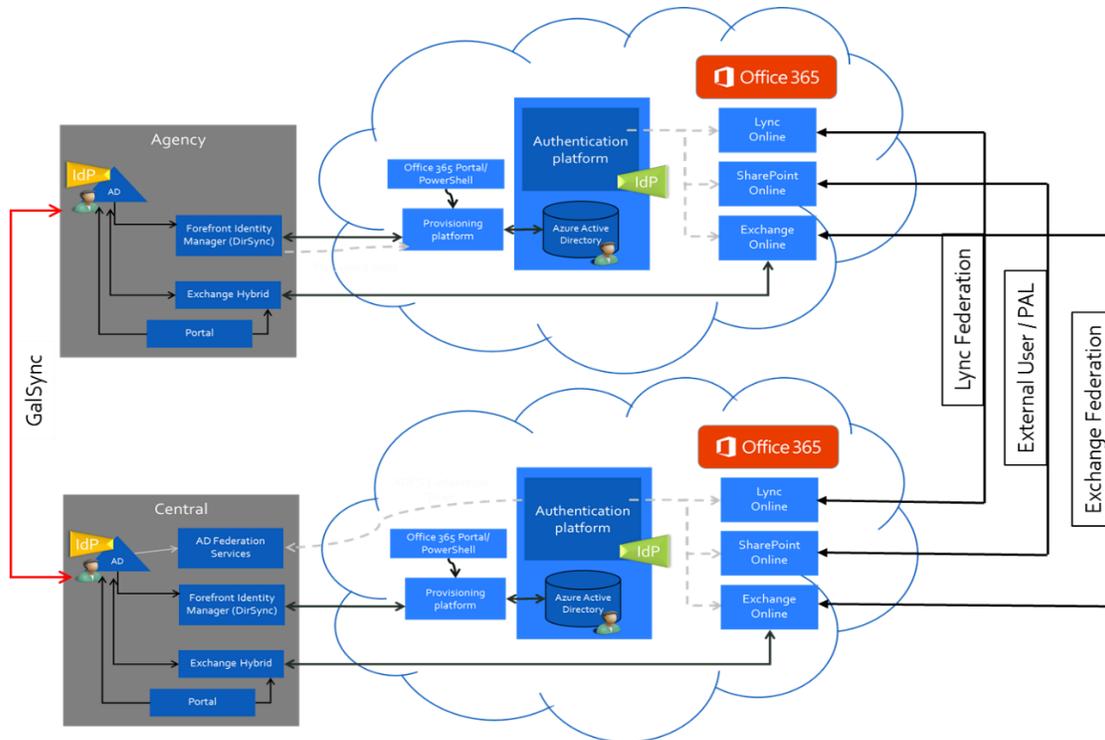


Figure 3: Hybrid Tenant Model

The “Hybrid” Tenant model is a subset of the Department Tenant design, as it allows for the integration of both a consolidated tenant for those departments wanting to leverage the current approaches, while allowing for the introduction of a multi-tenant support model for those departments wanting to branch out.

During the discovery sessions there were very few requirements noted for cross-department sharing as would be expected in typical, large entity deployments. While there is the occasional need to provide for collaboration functionality, a majority of the effort across workloads stays within the various departments. Microsoft can provide for the unified infrastructure regardless of tenant design and approach, and this is across all workloads as required.

4.4 Requirement Analysis - Pros and Cons

As presented in findings section, the consumption of cloud services is impacted by the following mandated data collection requirements:

- Department regulatory requirements (e.g. HIPPA/FERPA/FTI)
 - These requirements can be met by either the CTD (Consolidated Tenant Design), or the DMTD (Department Multi-Tenant Design) model. In the CTD approach, Microsoft provides for HIPPA/FERPA/FTI regulatory compliance across the entire tenant, meaning WaTech would continue to be responsible for departmental isolation to support these requirements. In the DMTD model, each Tenant would



be covered individually, meaning any incident resulting in regulatory non-compliance outside of the tenant boundary would be contractually enforceable.

- Department security requirements
 - Depending on the planned administration model in addition to the Office 365 tenant controls, the separation provided by the DMTD model would provide for additional granularity on security controls and features that WaTech would likely manage directly in the CTD model. For example, in the CTD, WaTech could maintain ownership of the Global Administrators security group in the tenant and delegate a subset of functionality to a department. When comparing this to the possible approach for administration of the DMTD model, the department itself may take on the role of the Global Administrator, with WaTech being delegated rights in the tenant to provide support for core services.
- Department BAA (Business Associate Agreement) requirements
 - The DMTD model could allow for individual BAA agreements between the department and Microsoft, versus a blanket BAA that would cover all departments in the CTD model. This benefit of this approach would allow for WaTech to provide for unique agreements between the departments and cloud providers based on specific requirements.

4.5 Cloud Position Reference Matrix

The following table provides a consolidated overview of the points presented across the various tables represented in this document. The abbreviations in the table refer to either Department Multi-Tenant Design (DMTD) or Consolidated Tenant Design (CTD).

Table 0: Cloud Position Reference Matrix

Requirement	Consolidated Tenant (CTD)	Multi-Department (DMTD)	Adv.	Ref.
Office 365 Tenant Design and Administration	Increased workload for WaTech to manage the tenant so that each department has appropriate level of delegated authority and is isolated from other departments in tenant.	Increased workload for each department in providing for administration of their own tenant.	CTD <i>CTD was chosen for the immediate adaptability of current operations/processes in place today, with a minimum of change</i>	Table 1, Table 3
Federated Identity	Single ADFS (already in place).	Additional configuration of ADFS required. May lead to requests for departmental ADFS.	Equal <i>This was rated Equal as the ADFS topology would remain consistent across both deployment</i>	Table 1



Requirement	Consolidated Tenant (CTD)	Multi-Department (DMTD)	Adv.	Ref.
		deployments.	<i>options</i>	
Administration and Delegation	Single AAD DirSync (already in place).	Multiple AAD DirSync (or new MIM solution) required.	CTD <i>CTD was chosen for the simplicity of the design, and integration with established processes.</i>	Table 1
Licensing and License Assignment	Economies of scale possible, but increased workload for WaTech to manage licensing 'pool'.	No 'pool' required, but additional licensing (such as PAL in Design Diagram) may be required.	DMTD <i>DMTD was selected as each agency could self-manage their licenses within the confines of "their" tenant.</i>	Table 1, Table 3
Compliance and Regulatory Requirements	Isolation from external entities enforced by tenant boundary. Isolation from other departments enforced by WaTech administration.	Isolation from all entities (external or other departments) enforced by tenant boundary.	DMTD <i>DMTD was selected as it solves a current technical challenge, by providing for complete data isolation between departments using the tenant as a boundary.</i>	Table 2
Reduce Technology Costs (Implementation / Operational)	Overall cost burden is less than with multiple tenants.	Increased complexity to integrate operations, in addition to increased costs for migration and operational run state.	CTD <i>CTD was selected as the model has less complexity, and operational processes remain constant in regards to existing processes.</i>	Table 2, Table 3
Business Continuity / Reliability	Simplified infrastructure and approach will result in efficiencies for BCP and reliability.	Unique BCP/DR requirements for each tenant, and associated hardware / infrastructure costs.	CTD <i>CTD was chosen as a single organizational model provides less complexity and infrastructure to support DR/BCP scenarios across the state.</i>	Table 2
Department Autonomy /Department Isolation, Technology Enablement	WaTech must set global parameters that will affect all departments in consolidated tenant.	As sole occupant of a tenant, departments can set global parameters at will.	DMTD <i>DMTD was selected it provides the ability to allow the departments to manage their own tenants Global settings, separately from all others.</i>	Table 2, Table 3



Requirement	Consolidated Tenant (CTD)	Multi-Department (DMTD)	Adv.	Ref.
Overall Architectural Complexity	Minimized impact to existing processes for both migration and operational readiness.	Architecture Design and Review of existing processes to support decentralized structure.	CTD <i>CTD extends, and takes forth the existing administration and operational model currently established and supported by the State, without the introduction of major changes.</i>	Table 3
Identity Framework	No need for multiple filtering and synchronization lowers overhead and cost of adoption.	Requires WaTech implementation of complex FIM (or future MIM product) synchronization and filtering (which will not be usable by Skype for Business).	CTD <i>CTD was chosen for the simplicity of the design, and integration with established processes.</i>	Table 3
E-Discovery / Regulatory Compliance	Isolation from other departments enforced by WaTech administration.	Isolation from all entities (external or other departments) enforced by tenant boundary.	DMTD <i>DMTD was selected as it solves a current technical challenge, by providing for complete data isolation between departments using the tenant as a boundary.</i>	Table 3

4.6 Requirement Analysis - Pros and Cons

Requirements for the review were defined by the Statement of Work presented to the State prior to the start of the review. Based on the findings, associated analysis and using the SOW-identified requirements, the following table presents a summary of the “Pros” and “Cons” for each requirement mapped to the two Models under review.

The abbreviations in the table refer to either Department Multi-Tenant Design (DMTD) or Consolidated Tenant Design (CTD).

Table 1: Requirements Pros and Cons by Tenant Model

Requirement	Consolidated (CTD)	Multi-Department (DMTD)
Office 365 Tenant Design and	Pros: <ul style="list-style-type: none"> Existing Enterprise LOB 	Pros: <ul style="list-style-type: none"> Existing Enterprise LOB Applications and



Requirement	Consolidated (CTD)	Multi-Department (DMTD)
Administration	<p>applications and administration practices remain unchanged.</p> <ul style="list-style-type: none"> Individual Domain Namespaces are supported. <p>Cons:</p> <ul style="list-style-type: none"> Delegation of rights within a single tenant (for example SharePoint online Site collection and storage) may not meet department requirements. 	<p>administration practices remain unchanged.</p> <ul style="list-style-type: none"> Individual Domain Namespaces are supported. Delegation of rights from central administration model to department IT staff may provide additional controls. <p>Cons:</p> <ul style="list-style-type: none"> Decentralized administration model would increase resource overhead per department, and introduce deviation(s) from established policy. Group Management for DLs would require an increase in administration overhead to maintain isolation and avoid collisions between tenants.
Network Capacity Concerns	<p>Network capacity and bandwidth concerns would evolve and require updates as the service and department requirements continue to grow/mature.</p>	
Firewall, Reverse Proxy and Application Publishing	<p>Based on the requirements for the State, centralized management of the network and establishing Firewall, Proxy and application publishing roles independent of Office 365 remain consistent with the processes and approach in place today.</p>	
Federated Identity	<p>Pros:</p> <ul style="list-style-type: none"> SSO (Simple Sign On) using <i>UserID@DomainName</i> allows for minimal disruption to enterprise LOB applications. Single ADFS, in an H Geo-Redundant configuration for Failover. Central administration of core service wouldn't change. <p>Cons:</p> <ul style="list-style-type: none"> Single ADFS Farm, even with isolated claim rules would have common configurations (such as IP Subnet Boundaries) for all departments. Single Claims trust would require all departments to share common authentication 	<p>Pros:</p> <ul style="list-style-type: none"> Individual support of subdomain namespaces required, allow for more granular claims based rules. Centralized administration complexity would increase, due to support of multiple claim rules and tenants. <p>Cons</p> <ul style="list-style-type: none"> Decentralized model could drive departments into self-deployment of ADFS in their own infrastructure. Increased complexity to support multiple department tenants increase administration overhead.



Requirement	Consolidated (CTD)	Multi-Department (DMTD)
Administration and Delegation	<p>requirements/rules.</p> <p>Pros:</p> <ul style="list-style-type: none"> • Single Directory Store, means single implementation of AAD DirSync. • Existing Administration and Delegation model moves forward to Office 365. • Consistency in delegation of roles and administration function across all tenants. • Exchange DL (Distribution Lists) Management is available. • Symantec Evault and Enterprise LOB applications remain unchanged. • Exchange Hybrid supports all departments. <p>Cons:</p> <ul style="list-style-type: none"> • Department boundaries and structure are management and defined within product capabilities. • All departments would be restricted to administration controls in the tenant (i.e. IM Federation Policy, IRM Policies). 	<p>Pros:</p> <ul style="list-style-type: none"> • Department boundaries and isolation are enforced by native Office 365 Tenant boundaries. • Tenant Admin boundaries allow for departmental policies for IM Federation, IRM Policies, etc. <p>Cons:</p> <ul style="list-style-type: none"> • Single Directory Store with Multiple Office 365 tenants require Multiple AAD DirSync appliances, or MIM (Microsoft Identity Manager) to coordinate identity. • Existing Management Model would have to be restructured to support departmental approach. • Increase in administration resources is expected. • Variation in management tools and processes between departments are also expected. • Symantec Evault requires redesign and additional cost for deployment to support multiple tenants. • Exchange Hybrid must be configured for a single department for migration at a time.
Licensing and License Assignment	<p>Pros:</p> <ul style="list-style-type: none"> • Single Methodology for Assigning Licenses is possible. • Centralized License Management is also possible. <p>Cons:</p> <ul style="list-style-type: none"> • Additional process is required for pooling licenses, assignment of licenses and decommissioning of licenses. • Centralized License Management, since each department to purchase their 	<p>Pros:</p> <ul style="list-style-type: none"> • Individual Management of Licenses is available. • No pooling of Licenses is allowed. <p>Cons:</p> <ul style="list-style-type: none"> • Decentralized licensing/adoption structure may not allow for economy of scale. However, there is no price advantage to pooled licensing.



Requirement	Consolidated (CTD)	Multi-Department (DMTD)
	own licenses is required.	

4.7 Business Requirements Matrix

In addition to technical requirements, the determination of “how the tenant options apply” to business needs is equally important. The intent of the table below is to indicate for specific business requirements if one model has an advantage over the other. The abbreviations in the table refer to either Department Multi-Tenant Design (DMTD) or Consolidated Tenant Design (CTD).

Table 2: Office 365 Business Requirements Alignment Matrix (Microsoft)

Requirement	Tenant Model Best Aligned With
Adaptability	DMTD/CTD
Maximize ROI	DMTD/CTD
Compliance and Regulatory Requirements	DMTD <i>This was given a higher rating than CTD due to the ability to shift the burden of management from WaTech to the department, and leverage the natural boundaries of the tenant for data isolation.</i>
Reduce Technology Costs	CTD <i>The Consolidated Tenant Model introduces less costs by extending the existing operational and administration processes to Office 365. While some addition configuration to processes might be required, the overall cost burden is drastically less than DMTD.</i>
Agility in Adoption	DMTD/CTD
Improve Service Reliability, Ability to Meet Established SLAs	DMTD/CTD
Business Continuity/Reliability	CTD <i>A simplified infrastructure and approach based on familiar architecture and design will result in efficiencies for BCP and reliability.</i>
Department Autonomy	DMTD <i>While there will be an increase in cost and administration overhead as some controls naturally transition to the department, data autonomy and isolation is inherent within the tenant, allowing for the natural boundaries to take the place</i>



Requirement	Tenant Model Best Aligned With
	<i>of existing isolation and segregation policies currently leveraged.</i>
Technology Enablement	DMTD <i>This was weighted in favor of the Department Multi-Tenant Model as it would allow more empowerment of the department to set technical direction and adoption of features – independent of other departments.</i>
Performance and Reliability	DMTD/CTD
Transparency	DMTD/CTD

4.8 Solution Impact Matrix

The impact matrix below was created to address business concerns based on the discussions during the various sessions.

The Abbreviations in the table refer to either Department Multi-Tenant Design (DMTD) or Consolidated Tenant Design (CTD).

Table 3: Solution Impact Matrix

Business Requirement	Tenant Model most aligned with
Overall Architectural Complexity	CTD <i>While the CTD may increase the administration complexity, it provides for a simpler infrastructure that aligns with the existing design approach, minimizing impact to existing processes for both migration and operational readiness.</i>
Identity Framework	CTD <i>A simplified, very straightforward approach to identity, without the need for multiple filtering and synchronization configurations for each department. This lowers the overhead and cost of adoption.</i>
Federation Topology/Integration	DMTD/CTD <i>Both designs were validated as equal do to the fact that they both provide a mechanism to scale beyond the confines of the current on-premises infrastructure.</i>
Department Autonomy	DMTD <i>The DMTD model allows for a reduction in administration complexity, as the tenant boundary becomes the administration boundary between departments.</i>



Business Requirement	Tenant Model most aligned with
Department Isolation	<p style="text-align: center;">DMTD</p> <p><i>The DMTD model allows for a reduction in administration complexity, as the tenant boundary becomes the administration boundary between departments.</i></p>
E-Discovery / Regulatory Compliance	<p style="text-align: center;">DMTD</p> <p><i>The DMTD model allows administration for eDiscovery and regulatory compliance at the tenant boundary, as it becomes the administration boundary between departments.</i></p>
Licensing	<p style="text-align: center;">DMTD</p> <p><i>The DMTD model allows for a reduction in license management, as the tenant boundary becomes the administration boundary between departments.</i></p>
Networking / Security	<p style="text-align: center;">DMTD/CTD</p> <p><i>Both designs were validated as equal due to the fact that they both provide a mechanism to scale beyond the confines of the current on-premises infrastructure</i></p>
Support	<p style="text-align: center;">DMTD/CTD</p> <p><i>Both designs were validated as equal due to the fact that they both provide a mechanism to scale beyond the confines of the current on-premises infrastructure. The ability of support to adapt to the requirements of the selected model allow for equal footing when determining approach suitability to the design.</i></p>
Administration	<p style="text-align: center;">CTD</p> <p><i>While the CTD model may increase the administration complexity as it requires WaTech to design, delegate and enforce boundaries between departments, it provides for a simpler infrastructure, aligned with the existing design approach, minimizing impact to existing processes for both migration and operational readiness.</i></p>
Cost (Implementation / Operational)	<p style="text-align: center;">CTD</p> <p><i>While the CTD model may increase the administration complexity, it provides for a simpler infrastructure, aligned with the existing design approach, thereby lowering both the cost of adoption of Office 365, and minimizing the changes to existing operational and administration processes.</i></p>
Governance	<p style="text-align: center;">DMTD/CTD</p> <p><i>Both designs were validated as equal do to the fact that they both provide similar mechanisms to allow for the adoption of common governance models</i></p>



Business Requirement	Tenant Model most aligned with
	<i>across the service and on-premises environments.</i>
Organizational Considerations	DMTD/CTD <i>Both designs were validated as equal due to the fact that they both allow for varied approaches to extend the current organizational structure to the cloud.</i>

4.9 Decision Notes

4.9.1 Overall Architectural Complexity

Taken as a whole, the question asked is “Which solution is more complex as it relates to implementation and supporting identity and department requirements?” [Note: “DMTD” refers to Department Multi-Tenant Design and “CTD” refers to Consolidated Tenant Design.]

- Input: CTD is more complex to manage and operate than the DMTD. This is because of the additional controls and policies required when transitioning from an on-premises messaging environment to the cloud. The controls required to provide a portion of the boundaries are present by default in a DMTD model. For example, in regards to the definition of search scopes for compliance and eDiscovery, the tenant boundary in Office 365 provides for the autonomy and isolation for each department. In the shared model, construction of appropriate security policies to constrain actions will be required to mimic the required functionality.
- In addition to the configuration and administration of the tenant, external applications such as Symantec’s Evault have to be taken into consideration. The move to the consolidated Tenant is less disruptive and costly as compared to the requirements for separation, isolation and migration of data from the existing archiving platform to another endpoint.
- Non-Technical Considerations: The consolidated tenant model provides for a streamlined approach to identity and federations specifically. Out of the box configurations for AAD DirSync and ADFS would be able to accommodate most of the requirements presented. The tradeoff for reduced complexity in configuration is the increase in complexity in maintain boundaries within the tenant between departments. As the service introduces new features, a constant revision of the rules and policies in place is required to confirm continued data isolation/autonomy.

4.9.2 Identity Framework

When discussing the available options for the consumption of cloud services, the primary question that should be asked regarding the planned design should be “How does the adoption of cloud services enhance or detract from the solution currently being provided?” In addition, “Does the user experience improve or will the user experience become more convoluted?”



Identity planning is central since it is arguably the most visible part of any cloud service from a user perspective.

- Input: The current model envisioned works for the established environment. In addition, the Consolidated Tenant Design also works since the core components are in place and there are processes designed for the management of those services. However, when taking into account the unique requirements of the various departments, in addition to outliers that are not subscribing to the current model, changes are required to validate a cohesive identity strategy. Departments have tight control of their identities on-premises, and additional controls and consideration are needed to address any overlap in the transitions effort to the cloud models. For example, the introduction of the DMTD model would require the adoption of FIM (Forefront Identity Manager) to help manage not only the object requirements, but to perform the GAL Sync functionality required to maintain organizational unity.
- Non-Technical Considerations: The consolidated tenant model provides for a streamlined approach to identity and federations specifically. The considerations for identity and centralized controls in a DMTD model would require the introduction of a more robust, and customizable solution (FIM) in order to maintain a cohesive GAL and collaboration infrastructure.

Azure Active Directory Premium features will complement and enhance both CTD and DMTD options. As such, Azure Active Directory Premium can be applied to both options and is not highlighted as a factor in tenant design/option selection. For more information regarding Azure Active Directory Premium feature, and a comparison with Azure AD Basic, please reference: <https://msdn.microsoft.com/en-us/library/azure/dn532272.aspx>.

4.9.3 Federation Topology/Integration

In consideration of the options, the existing ADFS model is resilient and sufficiently agile to support the requirements of both options presented. The topology of the DMTD does place a heavier burden on administration and integration overhead, which could transition into the CTD as well. The end result being, that ADFS will only require minor changes to support either model.

- Input: DMTD and CTD are equal in complexity. The existing federation structure in place today can support both design models depending on department requirements. Additional consideration may be required for the design (restructuring the federation approach away from a single top level domain to support individual department domain names) in order to provide additional granularity and controls to the department in the centralized on-premises model. For example, in both models separation of the domain names from *.wa.gov at the top level, to claims rules supporting dshs.wa.gov and dor.wa.gov would allow for an additional level of granularity for policy decisions and functionality across both models.
- Non-Technical Considerations: The federation topology in place today can support both scenarios, with minor configuration changes. The State may wish to consider implementing Claims trusts for ADFS for each department (<department>.Wa.Gov),



before a top level domain is created in ADFS. This will allow for a single ADFS infrastructure that can be configured to support requirements for each department in either scenario.

4.9.4 Department Autonomy/Isolation

In reviewing the business requirements and noting that departments generally expressed a desire for more autonomy, the approach attempted to ascertain whether or not the options presented increased self-sufficiency and isolation of data.

- Input: DMTD is more complex. While the CTD will provide for department autonomy, it will require additional management and overhead to ensure those boundaries remain consistent and enforced. The higher rating given to the DMTD is by nature of an Office 365 tenant, the security boundary is the tenant – and no further isolation from other resources is required. The idea is that the support for tenant isolation and security oversight in the centralized model would transition from WaTech directly to each department in a DMTD model, with WaTech providing the common framework for identity, federation and networking services. While department independence can be achieved in the CTD, the expectation for meeting regulatory compliance falls squarely on the provider to ensure isolation across the supported workloads.
- Non-Technical Considerations: The natural security boundary of the tenant will reduce the administrator overhead for WaTech. This is because in the current model (and the proposed DMTD); departments have the rights and processes to manage their existing infrastructure. The DMTD builds upon this framework, as the department would be responsible for the administration of their tenant, and would have connectivity into the central organization based on the reference architecture developed by WaTech.

4.9.5 E-Discovery / Regulatory Compliance

In reviewing the options presented, both models had to validate that the architecture enhanced the compliance requirements of the departments. It's clear that leveraging the native boundaries of the Office 365 tenants and moving the administration function for isolation and eDiscovery to the department removes the burden of management and configuration from WaTech – allowing the departments an additional level of self-sufficiency. However, this is not without additional costs/burden, especially in regards to support of archiving. The ramifications of a change in design will have serious impacts on the adoption, configuration and costs for Evault. This not only applies to long term operational costs, but the overhead and resources required to migrate and integrate to multiple technical models.

- Input: DMTD is more complex. The CTD lends itself to support eDiscovery and Regulatory requirements on a department by department basis, but similar to the autonomy and isolation points made above – those boundaries will have to be defined, and maintained in order to be enforced. This level of isolation can be maintained but it will require additional processes and overhead for ensuring the separation of responsibility, delegation of roles, and functional isolation from a regulatory and compliance standpoint. In the CTD model, each department would be directly



responsible for the controls, and limits they put in place to support their Regulatory and Discovery needs, without concern of overlap into other departments.

- Non-Technical Considerations: The DMTD model will reduce central administration overhead, and give more control and ownership to the departments. Departments will be able to continue to manage their own data for compliance and discovery, and will rely on the natural separation between Office 365 tenants to enforce those edges. WaTech would no longer be required to provide processes and operational support to ensure the isolation of data in the centralized organizational structure.

4.9.6 Licensing

“How does the model reflect the ability for pooled licensing?” “Does the solution architecture allow for scaling up (or down) of the infrastructure as required based on department capacity and growth?”

- Input: DMTD is more complex. Licensing overall has very similar requirements for a solution design perspective. The higher rating on the DMTD model was as a result of the ability for each department to directly purchase and administer their licenses. The CTD model requires departments to pool them in a centralized approach. When looking at the ability to provision/de-provision licenses a common framework – applied centrally or distributed - could be used; making the overall process follow a similar architecture strategy. This functionality doesn’t currently exist for either scenario and would require development.
- Non-Technical Considerations: The CTD approach adds additional costs and resource requirements in the shared model, as there is no default automation in the service to manage the pooling of licenses, with each department procuring their own, individual software licenses. WaTech would need to enhance their existing automation and reporting to manage the distribution of licenses as part of the provisioning infrastructure, and to confirm license availability when a department goes to assign it. In the DMTD model, there is no need to develop license administration reporting, as each department will be isolated and responsible for their own management and service.

4.9.7 Networking / Security

“Does the solution design allow for individual department security requirements in addition to those of the State as a whole?” “Can the design accommodate individual requirements in a granular fashion, providing for a layered “defense in depth” strategy on a per department basis if required?”

- Input: DMTD and CTD are equally difficult. From a networking perspective, this is not weighed in favor of either of the solutions. The net result is the infrastructure and components in place to support the State would remain consistent. Additional review of the current network pipes in order to plan for appropriate traffic in regards to consumption and capacity would be required no matter what model is decided upon. Network performance will be critical in establishing what the end user experience will be. When looking at a security posture, it’s clear that there are certain advantages in the



DMTD model from separation of IRM Policy, allowing each department to “bring its own encryption key,” to data isolation and autonomy allowing each department to set, control and enforce their own policies without encroaching on other departments.

- Non-Technical Considerations: In both cases, there may have to be an expenditure of effort in order to ensure that there is sufficient bandwidth to support the transition to the cloud. Regardless of the tenant design strategy, the consumption of data would continue to be very similar across both options. From a security standpoint, the central administrator role would be reduced, as more control would be returned to each department, allowing them to leverage the inherent security within the tenant, and set policy without compromising a shared tenant.

4.9.8 Support

“What does the complexity and solution architecture do to the support model? Does this drive a functional change with the current WaTech service provider?” “Does this impact the Microsoft support contracts?” “Does one model provide additional department benefits over another?”

- Input: DMTD and CTD are equally difficult. The DMTD model was rated desirable, because it would effectively change the underlying support characteristics for Exchange and Skype for Business. In the CTD model it’s assumed that WaTech will still be the broker for support between departments and Microsoft. In the DMTD model, support components for Exchange and Skype for Business would be directly between the department and Microsoft (and WaTech for identity as needed). The ramifications to this approach are the change in the roles and skillsets required to support the infrastructure from a WaTech perspective.
- Non-Technical Considerations: With each department currently acquiring licenses and support from Microsoft (the latter in addition to WaTech), the DMTD model would reduce some of the support burden and costs attributed to service delivery today. It’s quite possible that in the DMTD model, the current relationship for support between WaTech and the departments would evolve to a WaTech/Microsoft/Department hybrid based on the components being supported, and responsibilities within the tenant.

4.9.9 Administration

“How do the proposed architectures affect administration?” “How is governance impacted?” “Are there sufficient controls in place in the model to allow for department administration and overlap with the centralized administration model?”

- Input: CTD is more complex to manage, as administrators of the CTD tenant will have to create the DMTD tenant boundaries, and manage them directly. This is rated in the favor of a DMTD model, because the net result is since there will be less shared services as in the current model, and the departments would be able to be more self-sufficient in the context of their own tenant. This would also lower the operational complexity by moving some centralized services back to the individual department tenants, in addition to operational costs of having department data provisioned within the same infrastructure, effectively taking use of the natural barriers or the tenant boundary. Microsoft would



integrate with WaTech in taking the role of the service provider for those online services, and ensuring service availability and uptime against SLA requirements. There would be a coordination of effort between departments and WaTech for Identity and Federation, but that support model would take a different role as the service continues to evolve.

- Non-Technical Considerations: Looking at the administration effort of keeping data and services isolated per department in a consolidated tenant, using the natural boundaries of the Office 365 tenant will only help lower the costs for administration. In addition to the licensing concerns presented above, most departments in Exchange today retain a level of administrator capability in the current organization (for compliance/eDiscovery and mailbox management), and this would not change. What would change is the additional overhead required to confirm there is isolation between administrative scopes in the tenant.

4.9.10 Implementation / Operational Costs

“Fundamentally, does the solution architecture introduce or change costs – both in organizational terms, in addition to the costs to support the technology solution being proposed?” The Consolidated model certainly minimizes the risk to the environment, as the changes required for implementation are minor when taking into account the large scale, and required changes to implement and support a Multi-Department approach.

- Input: From an implementation perspective, the CTD model is less expensive from a transition standpoint. From an operational standpoint, the CTD administrative burdens would increase the costs to support DMTD on the departments directly, as they would be responsible for their tenant. The existing approach by nature should cost less, and the cost for implementation supports that. However, when looking at transitioning workloads to the cloud, addressing the unique business requirements of each department, and adding to that the growing breadth of options available – it’s questionable if the existing model would remain a low cost. The reduced complexity of the Federation and Identity components becomes negated when we look at the additional overhead required to fully isolate departments, the legal repercussions as a result of a failure to provide the required data isolation and the complexity of overlying a myriad of policy settings into a single, cohesive model will prove to be challenging at best.
- Non-Technical Considerations: In either option, there are going to be elevated costs as networking, identity and management of the solution is taking into account. While some support areas and infrastructure costs are removed (Exchange for example), those costs and recovery models would transition to support Identity and other workloads core to supporting Office 365.

4.9.11 Governance

It’s expected that some shift in the way governance is determined would be required if departments take on more of the centralized administration tasks that are performed by WaTech today, such as self-management and configuration of the SharePoint Online



infrastructure components. The assumptions put forth in this document is that WaTech would continue to support the custodial requirements of managing the State, with more coordination with individual departments to ensure alignment to a common architecture strategy.

- Input: The complexity of implementation and operations for the DMTD/CTD models are equal in nature. Both models have a need for a defined governance and Informational Architecture strategy, especially as multiple vendors and workloads are introduced. A broad, sweeping governance policy that is centrally mandated would be required for consistency in approach across the infrastructure. As discussed during the sessions, these broad goals are designed to provide a baseline policy and allow for more specific governance and policy for each department as we delve deeper into the application stack. The rating specifically leans towards a DMTD design as it offloads some of the governance and management activities from WaTech directly to the departments.
- Non-Technical Considerations: With a consolidated organization, a broad governance model will allow for consistency across the entire organization. However, the various requirements of the departments will have to be balanced within the structure to provide a consistent set of controls, and approaches to various collaboration workloads. When applying this to the DMTD design, providing for the ability for each department to have their own governance model, with no centralized (or consistent) information architecture, which could add additional challenges to collaboration as the solution matures.

4.9.12 Organizational Considerations

"Are functional changes to the existing infrastructure and organizational model required for implementation?" "Are there additional dependencies required in the solution design?"

- Input: DMTD and CTD have equal organizational impact in regards to implementation and operational support. Regardless of the end result, the intent of all solution designs presented is to ensure that Washington State can still function as a single entity. Regardless of a CTD or DMTD model, the experience to the end user would be a single, collaborative infrastructure. In order to support a DMTD model, additional investments in the design and management of these services will be required – specifically around Exchange integration and management of identity.



5 Conclusions

Before making a final conclusion in regards to the data presented, it may be important to understand what the next steps are depending on the design selected. To help weigh the impact into the decision the approaches, below is a high level review of the possible steps and requirements to move ahead with each solution.

5.1 Adoption of Consolidated Tenant Approach.

- Establishing Identity Synchronization (Completed)

This allows for the extension and synchronization of identity in Office 365. The AAD DirSync server provides an anchor point to associate a user with various aspects of the service (Exchange, SharePoint, Skype and Office Pro Plus). Some consideration into change the domain namespaces should be given as it would allow for more isolation of the departments from a federation perspective.

- Establishing AD FS Federation with Office 365

This allows the service to leverage the on-premises Active Directory infrastructure as the source of authentication for the services. The existing infrastructure is currently configured to support a single top level domain, meaning all subdomains are also routed to this federation endpoint as well. It's recommended that the ADFS design be re-evaluated, and trusts between the existing tenant and ADFS be established using the individual departments child domains. This would allow for more granularity and control between tenants in a centralized structure. It would also allow for identity uniqueness for users (SMTP Mail Address = SIP = UPN), providing for a common experience – and options in the future should decentralization be a priority.

- Establishing Hybrid for Exchange

The existing Exchange environment (Exchange 2010) can leverage Hybrid integration with the Office 365 tenant. This is important for providing rich coexistence between the on-premises infrastructure and the tenant. Hybrid provides for:

- Mail routing between on-premises and cloud-based Exchange organizations;
- Mail routing with a shared domain namespace. For example, both on-premises and cloud-based organizations use the @wa.gov SMTP domain;
- A unified global address list;
- Free/busy and calendar sharing between on-premises and cloud-based Exchange organizations;
- Centralized control of mail flow. The on-premises organization can control mail flow for the on-premises and cloud-based organizations;
- A single Outlook Web App URL for both the on-premises and cloud-based Exchange organizations;
- The ability to move existing on-premises mailboxes to the cloud-based organization or off board back to on-premises;



- Centralized mailbox management using the on-premises Exchange Management Console (EMC); and
- Message tracking, MailTips, and multi-mailbox search between on-premises and cloud-based organizations.
- Extend Administration, Delegation and Search Scopes to Office 365

Once Hybrid is configured, the State will then need to migrate the required settings, delegation and RBAC configurations in order to ensure alignment with the on-premises environment. The existing administration concepts and processes will be leveraged in order to provide near-seamless integration with existing processes today. Mail related services such as Symantec Evault would need minimum configuration changes, as it would continue to see the Office 365 tenant as part of the existing messaging platform.
- Configure Split Domain Integration for Skype for Business

This would allow WaTech to extend the current deployment, to have their Office 365 tenant be a logical extension of the on-premises namespace currently provided for with Skype for Business. Once established, this would allow for the creation of users directly in the Skype Offering, thereby having direct integration and access to the address list of the entire organization.
- Configure/Update Licensing Process for Services

License management and servicing is not only directly related to Office 365, but also for enablement of service features such as Exchange, Skype for Business and SharePoint. A process for ingesting and assigning the licenses from multiple departments will be required, as there are no mechanisms in the tenant to handle this by default. All provisioning and licensing approaches should also have a reverse mechanism to allow for the reclamation of licenses back into the respective pools. It's understood that there are management processes in place for this assignment today – and those would have to be reviewed for suitability given the requirements of the service.
- Migration of Mail/Resources to Office 365

Once Hybrid, and the extended compliance and security components have been established – then WaTech can begin the process of migrating mailboxes to Office 365, The consolidate model will allow for all departments to benefit from a parallel migration process, provided sufficient resources and infrastructure is available. Once migration of a particular department is completed, those on-premises resources can be decommissioned.
- Transition from Lync to Skype for Business

Unlike Mail Migration, the migration to Skype for Business is a "cut-over" type approach, and should be planned accordingly. Since this is part of the existing organization with the split-domain configuration, the client transition should be relatively straight forward, with a minimal amount of touch required.



5.2 Adoption of Multi-Department Tenant Approach.

- Revisit Identity Synchronization

Planning and consideration will have to be put into place as there will be additional requirements to drive identity synchronization with a single on-premises organization, and multiple Office 365 tenants. The identity solution will either require the deployment of multiple AAD DirSync servers, with complimentary synchronization filters and processes to ensure object uniqueness across tenants. This will require an increase in hardware, resources and integrated processes to manage on a large, statewide schedule. FIM (ForeFront Identity Manager) or MIM (Microsoft Identity Manger – replacement for FIM) could be centrally deployed and managed, providing the provisioning logic and rules for tenant isolation, in addition to providing the required GAL Synchronization functionality that the absence of a single tenant would require. In both cases, namespace planning and Exchange DL (Distribution List) planning will require revised naming standards and cooperation to ensure there are no adverse impacts as a result of the separation of tenants.

- Establish AD FS Federation with Office 365

As in the consolidated model, ADFS allows the service to leverage the on-premises Active Directory infrastructure as the source of authentication for the services. The existing infrastructure is currently configured to support a single top level domain, meaning all subdomains are also routed to this federation endpoint as well. It's recommended that the ADFS design be re-evaluated, and trusts between the existing tenant and ADFS be established using the individual departments child domains. This would allow for more granularity and control between tenants in a centralized structure. It would also allow for identity uniqueness for users (SMTP Mail Address = SIP = UPN), providing for a common experience – and options in the future should decentralization be a priority. The expectation is that this will have a similar footprint for both options as presented.

- Establish Hybrid for Exchange

The existing Exchange environment (Exchange 2010) can leverage Hybrid integration with the Office 365 tenant. This is important for providing rich coexistence between the on-premises infrastructure and the tenant. Hybrid configuration will become more problematic, as there can only be one hybrid configuration for the on-premises exchange environment with a single Office 365 tenant at a time. This means once hybrid is configured for an individual department, no other department could move to Office 365 (from a mail perspective) until migration was complete.

Migration complete would also mean not only the state of the production mailboxes, but any required migration of Symantec Evault as well. Again – this would require further investigation with the vendor to determine what options are available for Evault, and their associated costs.



- **Extend Administration, Delegation and Search Scopes to Office 365**

Once Hybrid is configured, the State will then need to bring across the required settings, delegation and RBAC configurations in order to ensure alignment with the on-premises environment. The existing administration concepts and processes will be leveraged in order to provide near-seamless integration. Mail related services such as Symantec Evault would need minimum configuration changes, as it would continue to see the Office 365 tenant as part of the existing messaging platform. This would require additional effort than in the CTD model, as search scopes, permissions and delegations would require review and isolation in order to determine suitability for migration into an individual department tenant. Some thought and consideration into a revised enterprise naming standards for DLs would be required, as the expected shift from the central organization model would require some controls to enforce object uniqueness.
- **Configure Domain Federation for Skype for Business**

Unlike the split domain configuration in the consolidate tenant, with departments having their own namespace and tenants it makes more sense to establish federation trusts for Skype for Business than trying to enable the split domain model. This would allow WaTech to leverage the current deployment, and provide for integration with various departments Skype for Business environments on an ad hoc basis. It's assumed that there would be an increase in administration as the roles would transition over to the departments.
- **Configure/Update Licensing Process for Services**

License management and enablement will transition from WaTech to the department as part of the overall tenant administration. This could lead to fragmented approaches in how licenses are assigned and consumed in Office 365, and WaTech would take on the custodial role to ensure consistency in adoption across the enterprise.
- **Migration of Mail/Resources to Office 365**

Once Hybrid and the extended compliance and security components have been established – WaTech can then begin the process of migrating mailboxes to Office 365, The challenge in this model is two-fold: (1) it requires a department to complete migration before the next migration can begin, and (2) it depends on the ingestion (or migration) of archive data as well. Should there be complications in either one of those processes, no other departments can migrate until they are resolved. This could introduce a much longer process for migration, impacting the perceived ROI and cost benefits the cloud offers.
- **Transition from Lync to Skype for Business**



Unlike Mail Migration, the migration to Skype for Business is a "cut-over" type approach, and should be planned accordingly. Since this is part of the existing organization with the split-domain configuration, the client transition should be relatively straight forward.

After reviewing the data collected, including operational and transition concerns, and completing the assessment phase, it's clear that Office 365 is able to support all options being considered.