One William St

State ICT architecture blueprint

This document offers current state and recommended future state architecture and implementation options.

Final

March 2014

v1.0.0

PUBLIC

Document details

Security classification	PUBLIC		
Date of review of security classification	November 2013		
Authority	Queensland Government Chief Information Officer		
Author	Queensland Government Chief Information Office		
Documentation status	Working draft	Consultation release	☑ Final version

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Queensland Government Chief Information Office
ggcio@ggcio.qld.gov.au

Acknowledgements

This version of the *One William Street – State ICT architecture blueprint* was developed and updated by Queensland Government Chief Information Office.

Copyright

Licence

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

Figures

Tables

1 Introduction

1.1 Background

The 1 William Street (1WS) development is now underway in Brisbane's central business district. When completed in 2016, this landmark office tower will provide a high profile tenancy for an estimated 4,500 Queensland Government employees, as well as private sector tenants.

On the upper levels the building will house the Premier, all Queensland Government ministers and their immediate staff[1], all directors-general and their immediate staff; and executive support for the directors-general including appropriate senior staff. A number of agencies will also be relocating their entire CBD workforce to the remainder of the government tenancy. It is expected that the floor layout design and desired work style and practices on the upper levels will be significantly different than that of the original concept.

In considering these variables it is important that departments remain mindful of the fact that the government has a stated intention for 1WS to be a showpiece of a new way of working and for the building to be *"modern, innovative and designed for a creative and adaptable workplace".* This vision will continue to guide thinking for the State's ICT blueprint as well as the design for the building.

1.2 Purpose

The purpose of this document is to translate the State's business requirements and scope of the 1WS ICT project into a high level services architecture.

The document will:

- Articulate the expected outcome for 1WS
- Provide an "umbrella" architectural document that can be referenced by agencies as they develop their target blueprints for 1WS. Agencies will undertake a gap analysis between their current state and the desired future state articulated in this document to inform service transition plans
- Define the overall architectural approach and identify any technology and service element options that will be outsourced to an ICT integrator/service broker and ICT service providers
- Guide the technical implementation planning activities and enable the costing of service components and ICT implementation activities in the 1WS ICT business case and strategic procurement plan
- Offer a repeatable architectural pattern for implementation and/or migration of other multi-floor, multi-agency buildings in the future.

[1] It has been determined that Ministerial Services will provide their own infrastructure and as such are outside the scope of this document, however the inclusion of Ministers and DG's will require a different floor layout and associated ICT approach than that of the original concept. The floor-plan design for these staff has limited open-plan areas and much more fixed office style. This fact combined with the style of working in Ministerial/DG areas may mean that there is less requirement for the full collaborative/shared ICT environment on these floors.

2 Business environment and requirements

2.1 Business drivers/objectives

The Queensland Government's objectives for developing 1WS are to:

- Enhance Brisbane's reputation as a vibrant city with modern, landmark architecture in a well-planned urban environment
- Accommodate the Queensland Public Service, and create a highly productive environment for team members focused on achieving the best outcomes for the businesses and people of Queensland
- Reinvigorate and act as a catalyst for change in the Government Administrative Precinct
- Achieve value for money for the State
- Create a high quality, sustainable development on the site
- Activate this project in the shortest possible time as part of the Government's priority to boost the State's economy.

The decision to co-locate Ministers and Directors General at 1WS was driven by several stated aims including:

- Better consolidation of government agencies with all government leaders in one place
- More coordinated delivery of services and infrastructure, resulting in less waste and rework
- Greater face-to-face interaction between government employees, improving communication and outcomes for the public service and customers.

2.2 Technology trends

Information technology is evolving rapidly in the areas of mobility, ubiquitous broadband connectivity, the consumerisation of information services and appliances, and the use of ICT to support collaboration. This is driving change in the requirements of government workplaces to meet the service delivery expectations of employees and citizens. At the same time, the requirement for optimal efficiency, cost effectiveness, and environmental impact has never been stronger.

The modern workplace will need to support on-line, any-time, any-where, any-device access to Government information and applications. This information will increasingly be in rich media formats and be required in real-time. Information will also need to be served to a variety of mobile end-user devices, which will increasingly be owned by the employee ("bring-your-own-device") and be moved into, around and out of the office. This variety in device usage and ownership, and the need for rapid and ad-hoc collaboration with fellow workers and visiting colleagues, will require flexible broadband connectivity to the office network in both wired and wireless modes. The employee experience will be that of seamless integration between office and mobile devices.

Mobility around the office will support "hot-desking" modes of working to increase the efficiency of the office accommodation and provide cost-effective support for part-time telecommuters. The use of mobile phones, soft-phones and wireless "follow-me" roaming (rather than dedicated number desk phones) such that the employee is accessible any-time, any-where, on any device will improve this capability and

support collaborative virtual team structures. Video communication will become common and will be part of a Unified Communications and Collaboration experience that will support inter-office, field worker, and teleworker collaboration from a wide range of device types (mobile, PC, room-based videoconferencing).

The ability to share general office facilities such as conference rooms will be enhanced with in-room presentation and conferencing facilities that integrate with the network. Printing services will be provided through consolidated multi-function devices, with efficiency and security enhanced through the use of "follow-me" connectivity and locked/PIN/card swipe printing controls. Physical access security will support multi-tenant use of the accommodation.

2.3 Vision

A key characteristic of the 1WS development will be the provision of a more flexible workplace – An aim is that the office will become a place of creativity and ideas rather than a centre for routine processing activities. To achieve this transition, the workplace needs to facilitate high levels of interpersonal communication for teams and project groups, and also maintain a work environment that supports individual tasks. In addition, the workplace must support organisational reconfiguration and be adaptable to new ways of working. The implication is a move away from workplaces that reflect organisational hierarchy and towards a definition of space, accommodation standards and fit-out design based on users' needs. This outcome needs to be achieved within space and cost benchmarks[2].

Given the majority of staff perform roles that do not necessarily lend themselves to a mobile style workforce, it is expected that this will change over time. To enable this transformation the workplace characteristics highlighted above need to be enabled by the underpinning IT environment acting as the "bedrock" whilst business initiates change to embrace new ways of working.

Vision:

'The collaborative design and adaptive technology within the building will offer occupants the opportunity to achieve higher levels of mobility and productivity; benefiting employees and the Queensland Public'.

[2] Office characteristics are derived from the Queensland Government *Office Accommodation and Fit-out Standards (October 2012).*

2.4 Principles

There are a range of technology, operational and implementation principles that will guide the ICT solution and services for 1WS.

Technology principles

The proposed technology design principles for 1WS are outlined below:

Ref	Principle
TP1	Adopt open standards based ICT infrastructure, technologies and services – vendor proprietary protocols/extensions to be considered only for optional value-add features.
TP2	Adopt a pragmatic approach to security by shifting from a network-based perimeter model to identity, application and endpoint controls. Physical and virtual identity needs to be converged and underpinned by an identity management model (access to applications and data will be based on identity and location).
TP3	A single physical wired and wireless LAN will be deployed. LAN/MAN and Internet gateway infrastructure will be provided as-a-service and shared by all Government tenants. Logical agency separation will be provided if required.
TP4	Infrastructure cabling, communications rooms and racks (roof, basement and floor) will be services provided under building facilities management and shared between agencies.
TP5	The design will be ecologically sustainable and energy efficient, and it will comply with the 5 Star Green Star[3] vision for the 1WS building.
TP6	Power and structured communications cabling should be separable from furniture systems, and enable easy reconfiguration if changes in floor layout are required over time.
TP7	Data centre facilities will not be housed within the tenancy.
TP8	The architecture must support a high level of staff mobility (anywhere, anytime, on any device connectivity) – a capability fundamental to the One Network initiative.

Table 1 - Technology principles

Operational principles

The proposed operational principles for 1WS are outlined below:

Ref	Principle
OP1	Adopt an as-a-service delivery model. The Queensland Government will not own, operate or manage telecommunications networks and desktop environments.
OP2	The ICT architecture should be machinery of Government (MoG) proof (to the highest extent possible).

[3] http://www.gbca.org.au/green-star/

Ref	Principle
OP3	The ICT architecture should provide a boost in collaboration, productivity and agility within and across agencies and with customers, partners and suppliers.
OP4	Limited ICT support staff will exist on site. ICT Infrastructure should support user self-service (to the highest extent possible).
OP5	The future workplace premises should allow simple integration with agency environments and not place undue support burden on agency staff or require significant end-user training.
OP6	Agencies will pay for use of shared/common ICT and physical resources on a fixed or consumption basis. Metering and consumption reporting will be available based on individual usage of physical and virtual resources as well as cumulative reporting on overall agency usage. This will require an advanced billing system and will help to identify areas of wastage and assist users and agencies to modify their behaviours if needed.

Table 2 – Operational Principles

Implementation principles

The proposed implementation principles for 1WS are outlined below:

Ref	Principle
IP1	The ICT architecture will address the government's requirements for 1WS and provide a repeatable model for other multi-agency buildings in the future.
IP2	Increased sharing and reduced duplication of ICT infrastructure.
IP3	In the short term the government will consume an IP network (as-a-service) behind the government gateway. This network will link 1WS to all existing government networks and to the government Internet gateway.
IP4	The building owners/operators and/or Government will outsource the design, implementation and management of shared ICT infrastructure to a Systems Integrator and approved ICT service providers.
IP5	Choice of providers - Must be able to move between ICT service providers upon contract renewal. (Contractual arrangements will be established in such a way to promote minimal switching costs).
IP6	The Queensland Government is committed to maintaining a viable and competitive ICT industry in Queensland. This requirement will need to be considered as part of any product selection and sourcing/procurement decisions.

Table 3 – Implementation principles

2.5 Assumptions

The key assumptions that apply to the 1WS ICT program are:

Ref	Assumption
A1	Agencies support the need for a new approach to ICT delivery in the 1WS location, with increased sharing and reduced duplication of ICT infrastructure/services.
A2	Ministerial Services will have a standalone network.
A3	Agencies are to meet the costs of their transition to 1WS out of agency budgets by managing short term expenditure if it does not align with 1WS.
A4	Agencies will be operational on most or all of target ICT blueprint components prior to occupancy of 1WS.
A5	Occupancy will be immediately after construction completion; potentially May 2016.
A6	The occupants of 1WS will include as the base, all Queensland Government ministers and their immediate staff, all directors-general and their immediate staff; executive support for the directors-general including appropriate senior staff; and the following central agencies departmental staff: • DPC including PSC • DSDIP • QTT including QTC • DLGCRR, (yet to be confirmed). See Appendix B – Proposed Occupancy Plan Note: The proposed occupancy numbers will continue to move around as the design is resolved. At this stage, the estimate is 4,500 work points.

Table 4 - Assumptions

3 Future state

3.1 A new approach

The collaborative[4], flexible and creative workplace desired for the 1WS building needs to be supported by the underpinning IT environment.

Previous agency co-location efforts have typically resulted in per-agency IT infrastructure with limited sharing and significant duplication. This approach is not sustainable and will not address the desired objectives listed above for the 1WS site or for any similar sites in future. A new approach is required.

The world of ICT has changed enormously in the last few years. Expectations of staff, the community and partner organisations have also changed. As a consequence it is no longer adequate or even acceptable to continue to provide the same IT and networking services that have served government well for the last 20 years.

[4] Collaboration is a cultural and social construct which may be supported by technology. To put the term 'collaborative' in context with the proposed architecture for 1WS, please refer to Appendix C – Unified communications and collaboration.

It's time to commence step change in how people use ICT. The success of that step change depends on government rethinking its approach to network communications, security, identity management, mobility and the cloud. Much of this work is already underway.

The building's workplace design must not only support a flexible, collaborative and productive working environment for the Queensland Public Service it must also address the changing demands of Cloud computing and the State's reform program including ICT-as-a-service. The approach must provide consistent, high-quality service to agencies whilst also balancing the Governments desire to achieve value for money for the State.

3.2 Technology architecture

The ICT architecture of an agency can be depicted graphically as a stack. Each layer of the stack consumes the products of the layer below, which also integrates and abstracts the products of all layers below it. At the highest level of abstraction, an agency is responsible for the delivery of a set of government services which are highly specific to that agency. Descending through the layers, the level of agency specificity reduces and the level of commoditisation increases. The lower layers (see Figure 1) are where shared commoditised services are relevant for multi-tenant buildings.

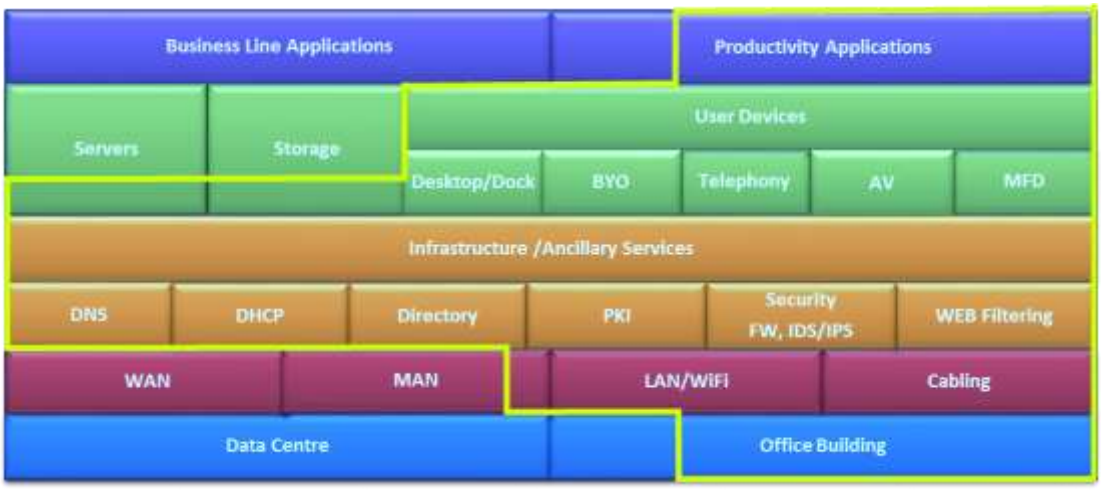


Figure 1 - Technology stack for the 1WS project

It is proposed that, the services outlined in yellow in Figure 1- Technology stack for the 1WS project, form part of the target architecture that agencies should be aligning to. The components presented above are not a "one in, all in" scenario; i.e. not all agencies need to agree to the same model. Some agencies may for example take up an as-a-service/cloud model for productivity applications and their associated server and storage requirements while others may have valid business reasons (subject to contestability) to retain these services in-house.

3.3 Applications and higher layers of the stack

Government services, business processes, information sets, and applications are generally specific to an agency's function and cannot be shared across different agencies. Where there is commonality (e.g. payroll, finance), these systems are delivered by a shared service entity/cluster to all client agencies, and apart from connectivity have no relevance to any particular building such as 1WS.

The following information reflects the agency environment in relation to applications, information sets and software:

1. Platforms and middleware that are open to sharing
2. Potential commodity software, applications, services:
    - Office suite
    - Email
    - Collaboration
    - CRM
    - Finance/HR
    - Records
    - Utility apps – 'corporate', training, procurement, time etc.
3. Cloud-based services/managed service.

The diversity of agency environments is depicted in the diagram below:

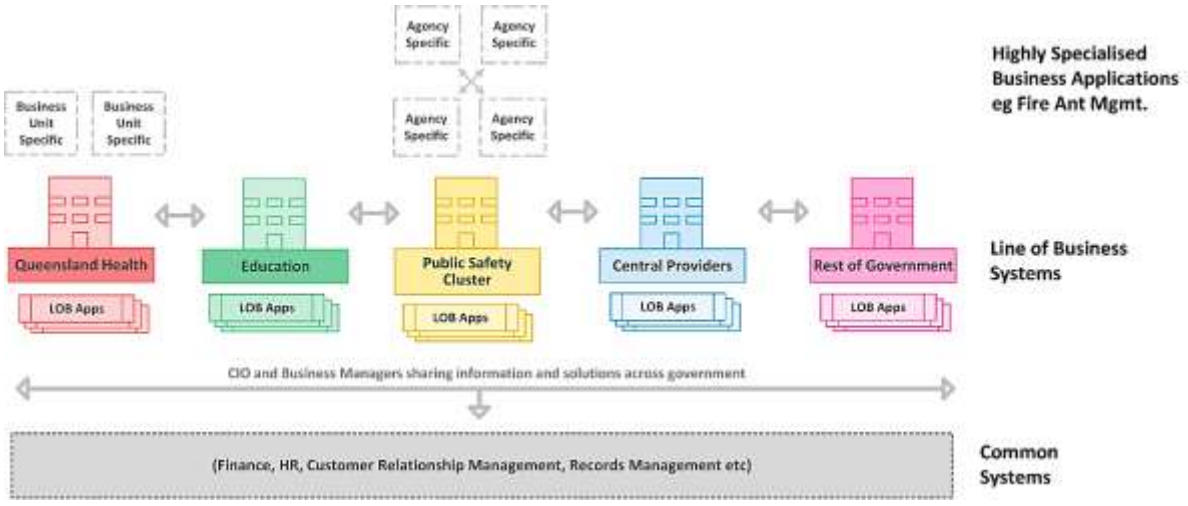


Figure 2 - Application diversity across agencies

Agency applications and information stores are hosted off-site in the Government primary data centres or agency data centre facilities. They are delivered via the agency's data network to multiple agency locations.

Where only an estimated 20-25 staff (i.e. DG, DDGs and support staff) are to be accommodated in 1WS, connectivity to an 'Office Suite' may be the primary

requirement. Under this model Desktop-as-a-Service (DaaS) and cloud based services may prove to be a more flexible approach[5].

Agencies who are migrating 100% of their staff to the 1WS location are not encumbered with the requirement to consider integration/interaction with other agency staff on a legacy ICT environment. They are in a good position to think of a new approach to ICT delivery.

The figure below depicts the target ICT platform:

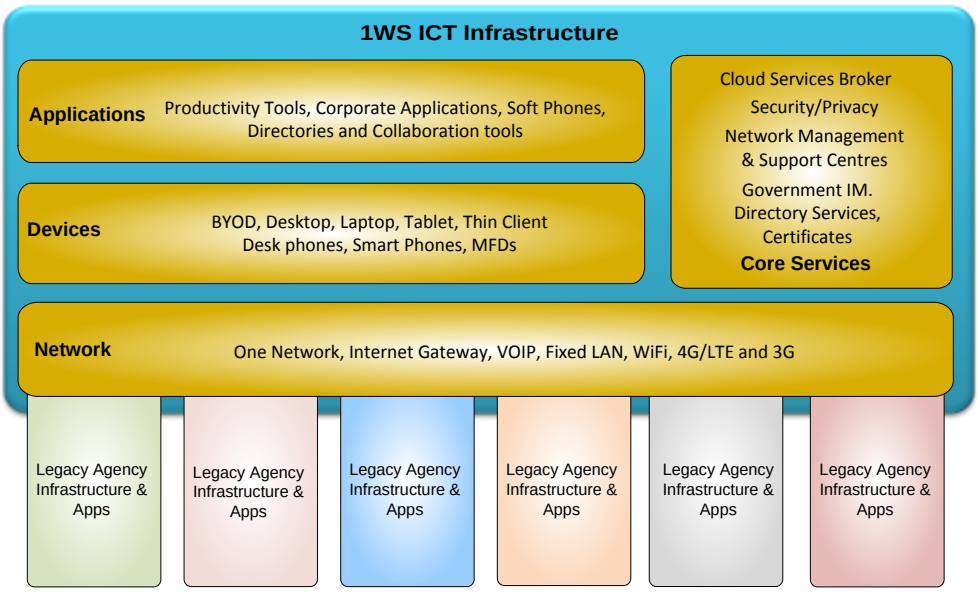


Figure 3 - Future ICT Platform

3.4 Future office features/attributes

It should be noted that many of the following attributes should be adopted as a component of the minimal baseline architecture while others align to the longer term goals of a fully collaborative environment. Many of these attributes have been identified and agreed by agencies as key underpinning requirements for 1WS.

[5] Feedback from agencies suggests that cost, time and organisational change will be an impediment to this approach and as such they consider it a longer term strategy.

Specific office features should include:

Components	Attributes	Principle
Power	Standby generator and UPS power provision. Agencies should not be required to provide their own UPS infrastructure. Automatic power shutdown of equipment when not in use.	TP4, OP1, IP1
Horizontal and vertical cabling	It is proposed that cabling be delivered as-a-service. It should not be necessary for individual agencies to perform maintenance or moves/adds/changes to the building cabling arising from staff relocating within the building. Horizontal and vertical cabling will be hard wired between the basement and all data rooms. Horizontal cabling to support 1Gigabit fixed LAN – UTP copper structured cabling. One UTP outlet per work station is likely to be sufficient in most circumstances (due to the convergence of voice/data). Note – Cabling to meet the following standards: • Qld Government ICT cabling infrastructure policy • Qld Government ICT cabling infrastructure technical standard. (QGCIO are working with Ministerial Services to ensure physical security of cable patch panels is adopted to meet their requirements).	TP3, TP4, TP6, OP1, OP2, OP3, IP1, IP2.
Telephony	Traditional TDM/PSTN PBX Telephony will not be supported. There will be a fixed IP telephony service offering. Agencies may take up a hybrid model whereby the telephony services are an extension of their existing contract. Wireless 'follow-me' roaming will be a component of the service offering however depending on agency requirements soft client/UC integration may be required. In building repeaters for optimal 3G and 4G coverage should be negotiated by the building service provider with the carriers.	TP1,TP3, TP4,TP5, TP8, OP1, OP2, OP3, OP4, OP5, OP6, IP1, IP2, IP4, IP5, IP6.
PC's /end user devices	Office fit out considerations should include: • Compliance with the five star green rating of the building • The preferred desktop service will be a docking station, monitor (integrated HD video camera), keyboard, headphones and mouse with USB connectivity to laptops and BYOD devices.	TP2, TP5, TP8, OP1, OP2, OP3, OP4,

Components	Attributes	Principle
	• A shared pool of desktop PC's managed by a service provider may be an option for some agencies to book/use (This model could suit agencies that are able to deliver their full ICT environment in a secure way without requiring them to manage the end device e.g. thin Client/Web).	OP6, IP1, IP2, IP4, IP5, IP6.
Video conferencing	A model for the sharing of videoconferencing facilities amongst all agency tenants is preferred. In practical terms, this means ensuring that the Telephony, Unified Communications, video-conferencing etc. adopted by individual agencies provide a feature-rich collaboration experience not just within their own agency but also to other agencies, partners and the public. To achieve this the merits of a single supplier/whole-of-Government model requires further consideration.	TP1,TP3, TP4,TP5, TP8, OP1, OP2, OP3, OP4, OP5, OP6, IP1, IP2, IP4, IP5, IP6.
Printing	Consolidated multifunction devices (MFDs) in shared print rooms. Specialist printing devices i.e. large format printers, 3D printers and plotters in designated print rooms. A model for sharing of printing facilities amongst all agency tenants is preferred. This model could be supported by having printers on a shared network and use of common access card (CAC) or PIN printing (to identify user and tie into back-end service provider billing).	TP2, TP5, TP8, OP1, OP2, OP3, OP4, OP6, IP1, IP2, IP4, IP5, IP6.
Datacentre	It is proposed that there be no data centres in the building (apart from communications rooms holding on-site network equipment). Agency systems will remain in the data centres that exist when their staff move or in the whole-of Government datacentres at Polaris and 317 Edward St. The 24 x 7 operation of data centres has a serious impact on the efficiency ratings of the building and is unnecessary given the availability of ample data centre space already, and the progressive adoption of cloud computing services delivered via the Internet.	TP7.
Comms rooms	*Plant Room* -Dual basement services rooms of approximately 16m^2 are required for termination of carrier and metropolitan area network (MAN) services and with cable trays for distribution throughout the building. Dual diverse building entry should exist for delivery of carriage services.	TP3, TP4, TP6, OP1, OP2, OP3, IP1, IP2.

Components	Attributes	Principle
	Floor - A 16m^2 communications room is required on each floor. The room must be capable of housing appropriate 19 inch rack space with cable trays for distribution throughout the building. *Roof* - Antenna structural support infrastructure and a rooftop telecommunications room of approximately 16m^2 is required for termination of optional carrier, GWN and Government communication services with cable trays for distribution throughout the building. A telecommunications riser, preferably diverse risers with cable trays are required to connect all floors, to support inter-floor fibre optic cables, and potentially copper cables if required. All rooms must be secured, dust free, precision air conditioned and provide UPS power of approximately 5KVA. Note: Physical security and associated processes for cable patch panels must be adopted to meet Ministerial Services and agency requirements.	
Local area network	All desktops, portable devices, (MFDs: printing, scanning, etc.), and other equipment which require a data network connection will be provided connectivity via a single physical network (wired and wireless) to be deployed and managed by a nominated service provider. Optimal coverage of high bandwidth Wi-Fi will provide mobility for laptops/tablets etc. and act as a complement (not replacement) to fixed cabling. Building ceilings need to accommodate provision for wireless access points.	TP1,TP2, TP3,TP4, TP5,TP8, OP1, OP2, OP3, OP4, OP5, OP6, IP1, IP2, IP4, IP5, IP6.
Metropolitan area network (MAN) and Government Internet gateway	The connectivity between 1WS and the various agency datacentres should be provided by the Queensland Government Network (QGN) currently managed by CITEC. This is already an extensive network covering Brisbane CBD, Southbank, Fortitude Valley and Spring Hill. See: Project dependencies regarding possible service impacts resulting from CITECs future divestment.	TP1, TP3, TP8, OP2, OP3, OP4, OP5, OP6, IP1, IP2, IP3, IP4.
Meeting rooms & digital signage	Includes: • Presentation and conferencing facilities • Meeting rooms • Quiet rooms (for individuals/small meetings) • Collaboration areas	TP2, TP5, TP8, OP1, OP2, OP3,

Components	Attributes	Principle
	• Digital signage. Large screen monitors, digital signage, smart boards, video conferencing (whiteboard/presentation/network-connected) and inductive charging stations and/or USB ports for laptops, smart phones and tablets will be deployed and managed by the building service provider.	OP4, OP6, IP1, IP2, IP4, IP5, IP6.
Physical access	Physical access card security and virtual security should be merged where practical by utilising a common access card (CAC) solution – For example, building security card may also be able to be used for PIN swipe printing. It would be ideal if building/floor access and authorisation systems were consistent across Government buildings. Smart card based solutions can also integrate well with certain desktop computing devices whereby the smart card is inserted or swiped to activate an authenticated logon and user session. Having a single CAC that provides secure access to buildings and computing desktop devices would be beneficial. Use of emerging technologies (e.g. near field communications) where devices such as a person's mobile phone become the CAC.	OP1, OP2, OP3, OP5, OP6, IP1, IP2.

Table 5 - Future office attributes

3.5 Services architecture

It is important to note that this document outlines a target architecture best applied in a stepped change. The success of that step change depends on government rethinking its approach to network communications, security, identity management, mobility and the cloud. The short term adoption of all of the services nominated in this section would require substantial change to most end-user ICT environments. Undertaking this effort and dealing with integration back into the rest of the agency network/applications/users may not be cost-effective when only a small number of staff are located in 1WS.

"Some is better than none" philosophy should be applied. Adopting a limited amount of services would not preclude migration of these agencies to a full collaborative model at a later stage. The learnings gained from piloting collaborative services in 1WS will also inform the broader 'One Network' program and this model can then be considered for other agencies and other buildings.

Implementing a highly collaborative, shared ICT environment for some of the agencies in the building would mean that government would still have met its commitment/vision for the 1WS to demonstrate a model for future government working.

The diagram below depicts the substantial change required to move from the current state to a future as-a-service model:

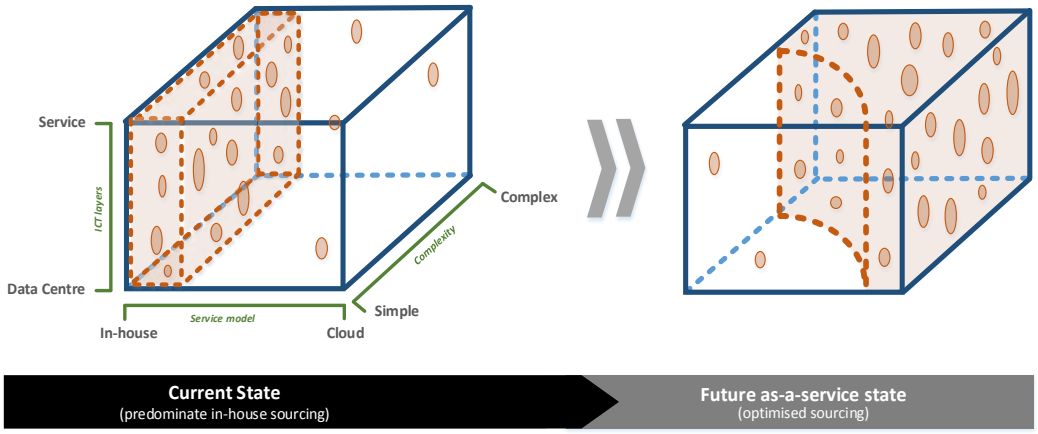


Figure 4 – Stepped change

The diagram on the following page (Services for 1WS) and the subsequent points summarise the existing and future services required for 1WS. Detail of the actual solutions, support models and their associated service attributes, KPIs SLAs and OLAs is a matter for further work to be undertaken. It is proposed that a working party consisting of the appropriate agency stakeholders representing their business requirements and transition plans and who in conjunction with ICT Strategic Sourcing and QGCIO will develop appropriate service requirements. Once developed these will be put to market under the current ICT Renewal Program guidelines.

It is expected that agencies will then trial and take up services based on their 1WS migration program in a stepped change, moving toward the target architecture and broader Government direction.

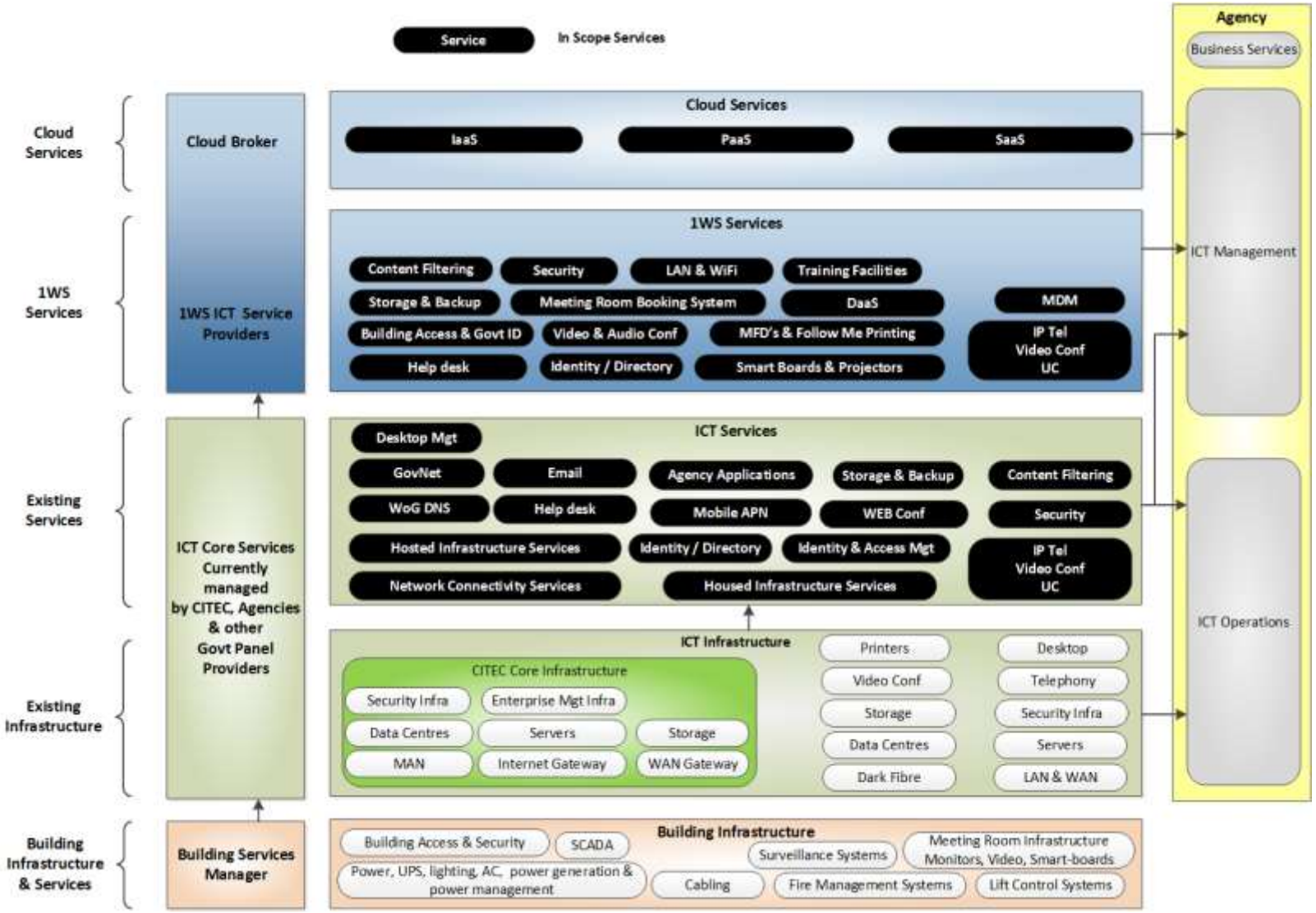


Figure 5 - Services for 1WS

Core and existing services

The core/existing services required for 1WS include:

1. *Identity federation* – The importance of Identity has been a common theme in discussions with agencies, analysts and vendors and has been evident in this government and other government cloud strategies. Identity is considered one of the key building blocks, along with network which needs to be in place to support a successful move to the cloud. It is also key to the cloud service brokerage approach and forms part an aggregation role.

   As individual Queensland Government agencies currently provide and manage their own identity capabilities, identities are not portable across agency boundaries, nor guaranteed to be unique or trusted across government. Without a shared identity framework or capability, duplication and disconnectedness will remain an inhibitor to effective and efficient service delivery.

   A central 'identity broker' is required to broker access to 1WSs common/shared applications and services from existing agency identity stores.

   For Option 2 (see deployment options), the following identity related requirements have been identified:

   - Device authentication and authorisation to support dynamic network VLAN allocation (802.1x) for wireless or wired devices e.g. placement of an agency managed device into the appropriate agency corporate network. This process should be seamless for an end user point of view
   - Authentication and authorisation using existing agency username/password credentials and identities to support access to the building's shared:
     - follow-me printing service
     - resource booking systems
     - visitor/guest registration systems.
   - Integration with building access management systems to support the use of CAC cards for printing
   - Self-service enrolment for guest access to filtered Internet and local printing or conferencing facilities.

   For Option 3 (see deployment options), the following identity related requirements have been identified:

   - Authentication and authorisation using existing agency username/password credentials and identities to support access to agency specific hosted virtual desktops
   - Integration with building access management systems to support the use of CAC cards for touch-on/touch-off authentication to agency specific hosted virtual desktops
   - Strong two factor authentication for remote access to agency specific hosted virtual desktops.

2. *Identity credential card access management (CAC authorisation)* - The building's identity store which controls building access may be provided in two ways:
   a) An independent Identity system is established and run by the building owner. The building owner would be responsible for enrolling/revoking staff in the identity store. The identity store would not be integrated with agency authentication systems, and may require users to sign-in to the building, then sign-in to their home agency systems.
   b) A federated Identity store is created based on one-way trust connections from each of the participating agencies' identity directories. Software is available which performs this task automatically and transparently. As the identity information is drawn dynamically from existing agency directories, no specific maintenance is required by the building owner. This is the preferred option.
3. *Connectivity to the One Government Network and Internet Gateway* - The MAN connectivity should provide dual trunk, high-speed (10Gbps) data connections between 1WS, Govnet, the Government Internet Gateway and the tenant agencies' network core. Agencies will not install their own MAN services to the building.

   Internet security controls and content filtering will remain under agency control where only an estimated 20-25 staff (i.e. DG, DDGs and support staff) are in scope. For agencies with full 1WS tenancy it is envisaged that security controls may remain under their control or be provisioned as-a-service with the flexibility to utilise a single common rule-set rather than per agency controls.
4. *Whole-of-Government Domain Name Services (DNS)* – DNS lookups are currently provided to agencies as a whole-of-Government service via core CITEC infrastructure. The current CITEC Internet and internal DNS domain consists of redundant servers deployed across the Brisbane and Polaris data centres. They are located in the Internet demilitarised zone (DMZ) domain. The DNS servers are deployed in a hierarchical design, with the authoritative name servers and forwarders responding to sub-domains and provide the following functions:
   - Internet DNS provides the forwarding of public domain name queries
   - Intranet DNS provides the forwarding of network traffic between agencies while containing it within government networks
   - Agency intranet and internal DNS would resolve other government departments and Internet by using the intranet DNS
   - Each agency is responsible for managing their own DNS entries.

   The Queensland Government domain qld.gov.au is administered by CITEC with the domain registration services provided by NetRegistry. The domain name provider, (Govnet Operations) administers requests for new domains. The request approval process adheres to both state and federal policy guidelines. Govnet Operations provides technical and administrative assistance for existing domain names. Agencies are authoritative for their own domains i.e. <agency>.qld.gov.au. Agencies can create sub domains as required.

   In the interim this service will stay in place. See: Project dependencies regarding possible service impacts resulting from CITECs future divestment.

5. *Network operations centre/security operations centre* - Where only an estimated 20-25 staff are in scope, it is proposed that these functions be provided by the agencies, but handoff and tight integration will need to be set up for issues relating to the building NaaS, MAN and Internet services.

   Current feedback from the agencies suggest that security services will initially remain under their control. Moving forward, the most appropriate way to address security operations will depend on how many as-a-service security controls are taken up.

1WS ICT service provider services

Proposed 1WS ICT service provider services include:

1. *LAN, including wired and wireless, DHCP and RADIUS* - LAN connectivity should be self-service for users. Implications include:
   a) Saturation patching – all floor outlets are patched to LAN switches
   b) Single UTP port per workstation PC/Laptop to be daisy chained off the phone
   c) 10/100/1G LAN switch connectivity
   d) Auto-sensing Power over Ethernet (POE), 802.1x support including dynamic VLAN
   e) 802.11ac equipped Wireless with capacity for 2.5 WLAN client devices per person; higher capacity in meeting/conference rooms and collaboration areas
   f) Guest registration to provide access to common services and Internet.

   Where only an estimated 20-25 staff are in scope, logical segregation provisioned via static VLAN assignment may be the most cost-effective solution in the first instance, as this would require minimal integration back into the rest of the agency network/applications/users. Adopting this model would not preclude migration to a dynamic architecture at a later stage.

   Agencies with full 1WS tenancy should strongly consider migration onto the same shared network as above. However the underpinning configuration would be agency agnostic and just provide high-speed connectivity to the Internet and/or a common government network (One Network).[6]

   This model will provide a single consistent approach that is in line with the 'One Network' vision. In the rare circumstance that additional security is required; it would be possible for the user/device to initiate an encrypted Virtual Private Network (VPN) to the home agency's systems. The adoption of logical segregation should be a fall-back position.

[6] The rationale for this approach is that agencies already need to adopt an ICT delivery model which provides secure connectivity to users from a variety of device types and locations outside the perimeter of their network, and so adopting this model as the standard approach (rather than a specific remote access solution) will provide a single consistent model for ICT delivery across an agency. This approach requires security models that are designed around the end-user computing device and user identity, and not around network segregation. Under this model the network will primarily become the conduit for connectivity (e.g. the 'Internet')

It would not be feasible or cost effective to support a large number of variants although a hybrid model may be feasible. Determination of the network layer architecture (Layer 2 vs. Layer 3) and supporting shared infrastructure (e.g. shared DHCP and RADIUS servers, Bonjour Gateways, etc.) will require further consideration during the design phase.

2. *Connectivity to the following services is required*:

   a) *A meeting room booking system* - this system can be a shared cloud based service or utilise agencies email appointment/calendaring applications, although visibility across individual systems may be problematic. In practical terms, this means ensuring that the ICT solutions adopted by individual agencies provide a feature-rich collaboration experience not just within their own agency but also to other agencies, partners and the public. To achieve this the merits of a single supplier/whole-of-Government model requires further consideration.

      Dynamic allocation of building wide conference rooms, meeting rooms, quiet rooms, and collaboration areas leads to improved utilisation. This also provides increased visibility into how the Governments real estate is being over or under-utilised.

      In selecting a booking system the architecture should include integration of collaboration and digital media to deliver a comprehensive set of features in areas of reservation, check-in, personalisation and administration capable of metering and billing space usage and services consumed. The solution should also be flexible and extensible to allow for varying degrees of integration with diverse building systems i.e. lighting and cooling.

      Where only an estimated 20-25 staff are in scope the floor plan design has a more fixed office style with limited sharing of meeting room and conferencing facilities. To support this model agency calendaring systems may be the most cost-effective solution in the near term. Adopting this model would not preclude migration to the shared service at a later stage.

      For agencies with full 1WS tenancy, a model for booking, sharing and easy identification of meeting room facilities amongst all agency tenants is key to achieving collaboration. A role based booking system will be a shared common service available to all authenticated users. Preferably it will be a Web based application capable of notifying agency calendaring platforms or a resource booking system utilising the most common government calendaring platforms i.e. Office 365/Exchange.

   b) *Follow-me printing and MFDs* – will be provided in an as-a-service construct and will allow users to print to a shared print queue, roam and release their print job from any enabled output device. This model will be supported by having printers on a shared network and using of common access card (CAC) or PIN printing which enables identification of the user and tie-in to back-end service provider billing.

Depending on integration requirements, printing may be linked with the building access and management system, a federated identity provider or agency active directories.

To maximise security agencies should also have the ability to restrict device access and user privileges, safeguarding devices and ensuring users only have access to the functions relevant for their job role. Restrictions can be made to copy, print, email, fax and scan and applied per user, output device or department.

All activity can be tracked and reporting tools will give an accurate picture on costs and activity, on a per user, device or department basis. Agencies are then able to make fact-based decisions to optimize the printing environment or allocate costs to departments, business units or clients.

Note – Ministerial Services will be adopting their own printer environments but this will not preclude ministers or their staff printing from the shared guest network.

c) *A file collaboration system/s* – the target architecture must facilitate connections between the public and private sectors and encourage cross-sector interaction. This will develop innovative, high quality, collaborative activities that improve efficiency in the use of government services and the pooling of knowledge, expertise and resources.

The shorter term goal and an immediate requirement for agencies moving to 1WS is to provide an interface between agency systems enabling the sharing and collaboration of intra-agency documents.

Public cloud file sharing services are becoming popular because they make collaboration simple enabling quick and easy to synchronisation of data between devices and people. For Government, however, public cloud file sharing services are not suitable for government information classified as “Protected” and may be problematic for a number of reasons:

- Storing critical business assets with third parties requires security controls to be matched to data classifications
- Duplicating data that already lives on agency infrastructure adds complexity and risk.

Apart from addressing some or all of the issues above the requirement is for a full-featured platform that allows agencies to manage projects, share documents and form groups around projects, departments or specific activities. The platform must be able to create private groups to help employees interact with each other and the public.

The solution should offer its entire feature stack anywhere, anytime on any device. Security features should include:

- Enterprise directory integration
- Data encryption (in-transit and at-rest)

- Role based access control (agency, department, group and user level based on need)
- Granular permission models for sharing, offline viewing, third-party app access, emailing and printing on a per document basis.

If used in conjunction with mobile device management (MDM), the ability to continuously monitor devices for compliance and revoke access for noncompliant devices will allow restrictions and policies to be more easily administrated. Available restrictions may include offline viewing restrictions; preventing cut/copy/paste, printing and emailing; and 'open in' restrictions to prevent content from opening in third-party applications.

It is expected that file collaboration services will be provided as a component of the DaaS catalogue, Email as-a-service provider or another offering.

d) *Cloud brokered services* - a cloud-first approach advocates that cloud-based provision of ICT solutions and ICT shared services will, over time, become the default approach for government agencies. Agencies will progressively adapt their ICT portfolio to take advantage of the benefits of Cloud Computing, considering first the use of cloud-based services. Not all workloads are suitable for cloud – and this necessitates a hybrid approach.

While the direct consumption of a single cloud service by a line-of-business group or agency can be achieved in a relatively simplistic manner, as consumption expands to include multiple services across multiple providers, managing the various commercial (e.g. agreements, billing and support) and technical (e.g. security, management, integration and provisioning) requirements become a substantial challenge and does not scale efficiently.

Cloud service brokerage offers a more coordinated approach and is increasingly being recognised by large enterprises and governments as a new service delivery model which is particularly important for successful cloud adoption. Agencies must consider moving to consolidate responsibility for this task, which is the cloud service brokerage role. The cloud service broker is responsible for aggregating, securing, integrating and simplifying the consumption of a diverse range of cloud services.

e) *Agency legacy applications* – access to agency legacy applications will be made available via virtual desktop containers. Not all legacy applications and infrastructure can be accessed from the cloud but they can be packaged and offered up in an as-a-service construct.

Where applications remain in house and where Web connectors, streaming or virtual connectivity i.e. CITRIX is not available, it is proposed that user/devices initiate an encrypted Virtual Private Network (VPN) to the home agency's systems.

3. *Desktop-as-a-Service, Desktop devices and peripherals* - because agencies have designed their corporate systems to operate on the products and versions specifically selected in their desktop stack standard operating environment: (SOE). If the ICT stack was placed alongside the Desktop stack, there are

interdependencies layer to-layer between the two, and there are also differences between agencies.

In order to increase workforce mobility, safeguard data based on its security classification and provide agency SOE autonomy and flexibility, desktop virtualisation can achieve all three. Virtual Desktop Infrastructure (VDI) is a desktop-centric service that hosts user desktop environments on remote servers and/or blade PCs, which are accessed over a network using a remote display protocol. A connection brokering service is used to connect users to their assigned desktop sessions. For users, this means they can access their desktop from any location, without being tied to a single client device. Since the resources are centralized, users moving between work locations can still access the same desktop environment with their applications and data. For IT administrators, this means a more centralized, efficient client environment that is easier to maintain and able to respond more quickly to the changing needs of the user and business.

There were two major technological advancements, introduced in 2013, that are making VDI much more attractive in many scenarios:

- The first is an advancement in storage technologies
- The second had to do with graphics.

These two technological advances, combined with Moore's Law continuously driving down the cost of server hardware, mean that VDI is an option for millions more users than it previously had been. See (Appendix D – Myth busting DaaS) for further detail.

Remote desktop virtualization can also be provided via a Cloud computing similar to that provided using a Software-as-a-Service model. This approach is usually referred to as Desktop-as-a-Service (DaaS). The DaaS provider will typically take full responsibility for hosting and maintaining the compute, storage and access infrastructure, as well as applications and application software licenses needed to provide the desktop service in return for a fixed monthly fee.

Where only an estimated 20-25 staff are in scope; initially supporting individual agency SOEs may be the most cost-effective solution in the first instance. This however this would not preclude migration to a more collaborative architecture at a later stage.

In a more collaborative environment, support for thin client, fixed desktop PC's, laptops, Government issued tablets, smartphones etc. will be provided as-a-service (DaaS) connecting via conveniently located cable ports or wireless. It is expected that this solution will deliver a rich experience at all levels including user, application and device. Benefits include:

- Aid of migration to modern SOE environments such as Windows 7 and Windows 8
- Support for mobile employees, contractors and BYOD initiatives
- Ability for IT divisions to provide improved flexibility so that not everyone has to be on the same version of software
- Cheaper and more robust than individual VDI only

- Frees up capital.

A user/device will authenticate to the shared network with an identity and password (or a CAC should the extra cost be justifiable). Once authenticated the user will dynamically connect to a common 'look and feel' government or agency context-specific portal. A role based SOE/Virtual Desktop can be presented allowing a single workspace and connectivity to collaboration file systems, agency file systems, streamed apps, cloud based apps and VPN's where required. This will make it easy for users to access widely dispersed information on any device. It is expected that KPIs will be based around user experience and the portal will deliver provisioning, reporting, service management and billing functions.

4. *Government issued tablets and mobile devices utilising MDM* – agencies will have a choice to utilise their own MDM systems or to procure as-a-service. It is expected that this service may be provided as a component of the DaaS catalogue or another offering.
5. *BYOD support for limited apps* - "bring your own device" (BYOD) connectivity will be supported to limited apps i.e. Internet, cloud email and office productivity suites or access to Agency Citrix platforms. BYOD devices will connect on-net and off-net via a browser or client, and may be managed by a MDM service. It is expected that this service may be provided as a component of the DaaS catalogue, Email as-a-service provider or another offering.
6. *VOIP and softphones* – there will be a fixed IP telephony service offering for agencies that wish to utilise it. Likely attributes include the following:
   - A single managed enterprise/carrier grade IP telephony service provided for the building
   - Pre-existing and proven market service offering
   - An "all-inclusive" per-user/device cost model with limited/no usage based variations
   - A range of fixed endpoints to support different user types, from basic headset/handset through to executive video-calling capability
   - Tight integration with existing telephony/unified communication (UC) environments in agency networks
   - Support for rich unified communications and collaboration (UCC) within and across agencies
   - Flexibility, in terms of underlying architecture to "future-proof" agency choices. For example the ability to change some or all agency users to a different IP telephony/UC solution whilst maintaining telephone number, or to integrate with industry leading UCC solutions
   - Support for mobile device integration (device type and mobile operating system agnostic)
   - Single number contact will provide the ability to dial a single number for a user that can be linked to multiple different devices (office, home, mobile) plus intelligent routing of same. This means people need to only know a single number to contact a person, and the person can take the call on the device of their choice, and handoff between devices if required

- Calendar integration and configurable call preferences will automatically direct call to voice mail when user is on holidays and only allow calls in meetings from nominated individuals
- Common voicemail box (between mobile, desk phone, email).

Agencies that do not wish to take up the 1WS offering can utilise their pre-existing IP telephony offering, assuming that said offering meets the other ICT requirements of the building such as zero or minimal on-site footprint required for IP PBX.

Note – Careful consideration to the supplier of the IP Telephony service will need to be given since it is likely to have more broad reaching considerations for UCC across government. Certain solution components may need to be supported beyond just 1WS and the procurement approach to market will need to consider this broader scope.

7. *Room audio and video conferencing* – in room monitors/screens will be provisioned and managed by the building service provider and should have ample HDMI and USB ports to allow WiFi, WiDi and Airplay screen mirroring. (Note – Some of these features may be integrated directly into monitors without requiring connectivity to external devices).

   A model for sharing of videoconferencing facilities amongst all agency tenants is preferred. For video conferencing it would not be feasible/cost effective to support a large number of variants in the building and may require that a minimal number of accredited/interoperating solutions be adopted. This may also be applicable to the broader whole-of-Government.

   It is important to ensure that the Telephony, Unified Communications, video-conferencing solution adopted for the building provide a feature-rich collaboration experience not just within an agency but also to other agencies. Given the tight integration between IP Telephony solutions (particularly video calling endpoints) and the room-based video conferencing solutions, selection of the videoconferencing solution will need to be done in parallel. Additionally, there may prove to be merit in choosing a single service provider for both IPTel and Videoconferencing requirements.

8. *Service Management and Help desk* – it is proposed that level 1 help desk support for 1WS be provided by the agencies existing IT help desk. A level 2 help desk will be provided by the Building ICT service provider who will have tight process integration and access to the following support staff:

   - Building service provider teams
   - Vendor/ICT service provider teams
   - Contract manager
   - Billing manager
   - Agency level 2 ICT helpdesk support teams.

   Service catalogues & Government storefront - Queensland Government's longer term vision is for the development of a Storefront/"AppStore" for Government that will support the sourcing of a wide range of mass-market ICT services from

Industry. Initially it is expected that as-a service providers for 1WS will offer their products through service catalogues. The diagram below depicts this model:

Figure 6 – Government AppStore

The sharing and re-use of common ICT services, solutions and components will introduce a number of integration issues that must be addressed. The table below summarises some of the 1WS service ownership and associated integration implications:

Service	Building SP	1WS ICT SP	Agency Services	Other SPs	Rational/implication
Power and AC	✓				Individual power and AC management settings will need to be negotiated with the building infrastructure service provider from a standard set of service offerings
Data cabling	✓	✓			Saturation patching of all outlets will belong to the LAN service provider. Note: Physical security controls will need to be implemented so that patching for ministerial services can accommodate MoG changes.
Building access	✓	✓	✓		A CAC system will require business processes to be setup between the various service providers and may require a federated trust model to be set up between the identity directories.
Meeting room booking system				✓	Integration with calendaring on different platforms will require federation of resource presence information. Visibility across individual systems is problematic

Service	Building SP	1WS ICT SP	Agency Services	Other SPs	Rational/implication
					therefore an initial WEB based system may be the most appropriate.
Monitors/ displays, smart boards and projectors		✓			Smart boards and projectors may be replaced by wide screen monitors and glass walls that can be photographed. If so these will be provided by the 1WS building SP.
Digital signage		✓			Integration will be required to building systems, meeting room booking systems and agency content.
Telephony		✓	✓	✓	Dependencies lie in current agency TIPT contracts and tight integration with Lync and Cisco UC services. UC services will also be tightly linked to video and audio conferencing systems and may also be linked to room booking systems.
PC's /end user devices		✓	✓		Federation of agency identity directory systems is essential to support the re-use of existing agency credentials and single sign-on to agency corporate environments. Business processes will be required between all associated service providers.
Video/audio conferencing		✓	✓		Room based displays and HD cameras/codec's will be managed by the 1WS ICT SP. Tight integration will be required between UC service providers to ensure interoperable services.
Printing		✓			Follow me printing will be delivered as-a-service with business processes to be set up for billing and role based identity. Access will be via CAC or PIN.
Training facilities		✓			Training room facilities and infrastructure will be provides as-a-service by the 1WS ICT SP. Connectivity to course material will be set-up by the trainer via guest Internet access or VPN.
Web filtering			✓	✓	Cloud based as-a-service WEB filtering will be multi-tenanted. Business processes based around individual 'white listing' will need to be set up between each agency and the cloud service provider.

Service	Building SP	1WS ICT SP	Agency Services	Other SPs	Rational/implication
					In the first instance most agencies have indicated a preference to maintain their own security and web filtering controls however guest access for the building will still require WEB filtering.
Local area network		✓			LAN and Wi-Fi services will be offered by the 1WS ICT SP. Interfaces to horizontal and vertical cabling, MAN and WAN will require tight integration.
Metropolitan area network (MAN)			✓		Resilient MAN services will be provided as core infrastructure by CITEC. Basement router interfaces and LAN connectivity by the 1WS ICT SP will require tight integration.
Internet, Govnet and WoG DNS			✓		To be provided as-a-service utilising CITEC Network Connectivity Services. Contestability may require an alternate solution. Transition business cases should capture this.
MDM		✓	✓		An optional MDM Service will be provided by the 1WS ICT SP. Business processes and tight integration between the agencies and the service provider will be required to administer policy requirements.
Help desk	✓	✓	✓	✓	Agencies will provide Level 1 help desk facilities. A level 2 help desk will be provided by the 1WS ICT SP. Business processes will be required for hand off, be it to an agency help desk or service provider help desk.

Table 6 - Service ownership

For further detail regarding the proposed uptake of services for 1WS see High Level Deployment Options.

3.6 Exclusions

Building management services

Building management systems components, include:

- Fire management systems (FMS)
- SCADA
- Lift Control Systems (LCS)
- Security Systems (except where likely BMS linkages have been previously noted)
- UPS, water, lighting, A/C and power generation.

It should be noted that some components of the Audio Visual fit-out may also be assessed as out-of-scope. However detailed examination of the selected AV system will be required to ensure that the delineation between included/excluded scope elements is both understood and agreed.

Ministerial services

The floor-plan design for Ministerial/DG areas has limited open-plan areas and much more fixed office style. This fact combined with the style of working in these areas means that there is less requirement for a full collaborative/shared ICT environment.

While this does not preclude the Ministerial Services department from implementing some or all of the shared services proposed in this blueprint, they are continuing to work with the QGCIO to determine common touch points.

4 Current state

4.1 Analysis

Before defining the future state, and the optimal implementation strategy to achieve this goal, it is vital to understand the current and planned requirements from both a whole-of-Government perspective and specific agency requirements that will shape the future architecture.

This document will provide a high level overview of the Queensland Government's current state. The analysis of up-to-date information on agency ICT environments, identified challenges and risks with the current state will be addressed in the agency blueprints.

An understanding of the current state will influence the key themes, strategic directions and implementation options of the 1WS program.

4.2 Audit recommendations

The ICT Audit (2012) and Commission of Audit (2013) recommended significant changes to the business model for Government IT. In line with these recommendations, the Queensland Government is running a major reform program covering its IT systems and networks.

The ICT audit noted the following:

- Unnecessary diversity across infrastructure platforms impedes efforts towards economies of scale, drives the need for a wide range of technical experts to remain in-house and limits agility and integration
- There is significant opportunity for government to reduce cost and remove the distraction of having to manage commodity environments. However, if real value is to be delivered then adoption must be accompanied by a fierce determination to adopt without customisation whenever possible
- The government should move infrastructure to an "as-a-service" model – essentially moving the government out of the business of owning and running commodity infrastructure.

Based on the recommendations above a new approach to ICT architecture and facilities management is required across Government and in larger multi-agency office buildings.

4.3 Changing demands

Just like the advent of Client Server in the early 1990's it is time for a new business model for ICT in multi-tenant buildings. No longer is it acceptable to operate as a number of silos. Collaboration and partnering have become core competencies. Across most large organisations the existing network architecture, identity management and approaches to security are all struggling to come to terms with these changing demands.

The issue is therefore not that there are multiple networks, multiple types of users or devices to contend with (this is reality). The problem lies in the limited interoperability between networks and the tight tethering of users and devices to a given network. Under this architecture the network is the vehicle to deal with the inability of applications to operate in a hostile environment. A user's access to applications and the security of those applications is solely determined by the network (or network perimeter).

Under this model, the network itself is used as a broad security perimeter such that the users, devices and applications are co-located within the network, behind the firewall. Everything outside the firewall is therefore considered untrusted. Everything behind the firewall must be tightly controlled and managed so as to keep the network "secure".

An overview of the Queensland Government's current state network and support arrangements can be found in Appendix A - Qld Government network services overview.

4.4 Constraints of the existing applications

Traditionally agency ICT divisions have been the in-house provider of ICT services. However, with cloud adoption and the corresponding outsourcing of common and commodity ICT capabilities, their role and mindset must shift from producing and managing assets to acting as a broker of ICT services from external suppliers to satisfy business needs.

Agencies are to have a minimal ICT footprint, and should be brokering, investing in and leveraging a network of ready-made capabilities to assemble and deliver innovative, business led ICT solutions.

The Queensland Government cannot move directly to an Internet based network and will not be able to do so for a number of years. However the most significant constraint is driven by the government's legacy applications. A large number of applications cannot operate in an environment that is considered hostile (i.e. the open Internet). These applications are designed to operate in the 'so called' safe environment behind agency firewalls.

The following table summarises some of the barriers to becoming brokers of ICT capabilities:

Barriers to shifting ICT service paradigm	
Agencies are not ready to take advantage of Cloud-Internet-Mobile-Social	Cloud-Internet-Mobile-Social paradigms have gone from a good idea to industrial strength in less than the replacement cycle for a desktop. The speed of this maturity cycle has caught the industry napping. Only the most alert organisations are cloud and mobile ready – and most of these are greenfield. Very few mature organisations have been agile enough to take advantage of this new paradigm. Lack of agility is also exacerbated by the inertia of older IT investments. For example, many desktops and servers have a replacement cycle of 3-5 years. Those purchased a year ago still have a working life of up to four years.
Readiness of ICT Industry	Moving to a new ICT business model built around ICT-as-a-service will require a significant change in capability across the local and international ICT industry. While many industry leaders argue they are cloud ready a number of questions remain about industry capability. These include: • Ubiquity of capability across the full range of ICT skills required for an organisation to migrate to a cloud based ICT business model • Level of commitment to outdated approaches across the ICT industry, including reward systems, capital investments, outdated supply chains, etc. • Staff capability in new technologies and tools • Threat of the cloud business model on the existing profit making areas.
Scale and complexity of the change	Changing how IT works across an entity as big and complex as government while continuing to run all services and interactions with the community at 100% capacity is more than challenging.

Barriers to shifting ICT service paradigm	
	Adding to this complexity is the tight link between the success of business initiatives within agencies and the quality of their ICT networks. How much control agencies will be prepared to rapidly give up to a central initiative is a significant variable in the success of the initiative.
Legacy applications	Client Server is the dominant desktop architecture within the Queensland Government, with Microsoft Windows being the dominant desktop OS. By its nature this architecture constrains how people access the government's applications. Client-server architecture normally requires users to be in a government building serviced by the relevant government network. Many agencies driven by enterprise mobility requirements have implemented VPN gateways and Citrix portals in order to gain remote access to their applications. These disparate workarounds are complex and not scalable. While this is an impediment to the governments "Cloud First" approach and ever increasing mobile workforce, it is the only viable short to medium term solution for connectivity to legacy applications.

Table 7 - Barriers to shifting ICT service paradigm

4.5 Constraints of the existing networks

A per-agency approach to ICT across Queensland Government has resulted in extensive duplication of infrastructure by agencies. This duplication was not only in the area of network connectivity, but also with related services.

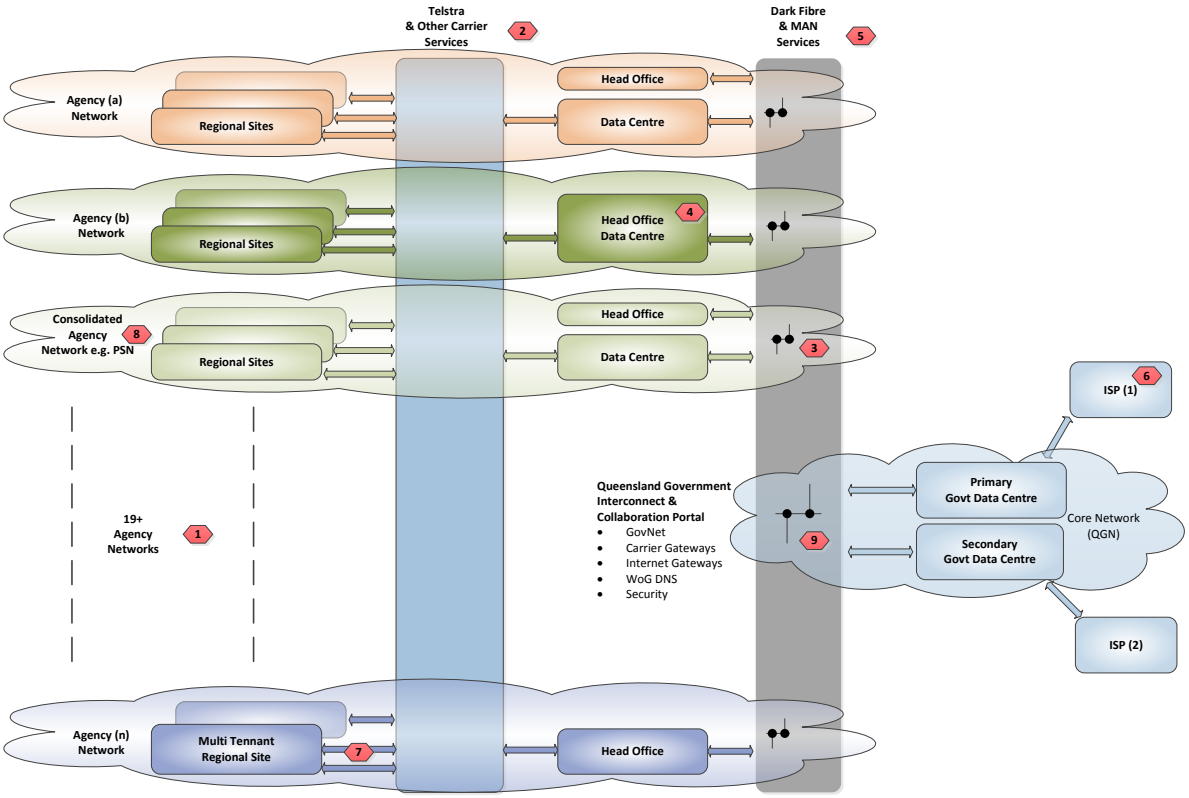


Figure 7 - Current state network visualisation

The following table highlights the constraints of the current state networks:

#	Issue	Problem Description
1	19+ disparate networks	Multiple disparate networks evolved from local agency requirements. Lack of standardised technologies and processes, constrain seamless service delivery and do not allow agencies to quickly obtain or divest services as changes occur.
2	Multitude of telecommunications accounts	Procurement approaches are substandard and relationships are difficult and expensive to administer. There is no responsibility for optimisation of the service during the contract period and no end-to-end control. This provides little motivation to improve service or reduce prices. Vendors consumption based models are complex and difficult to change limiting innovation for the vendor and government driving unwanted behavior within agencies.
3	Individual security regimes	Often driven by IS18 compliance and perimeter security models, agencies have implemented differing controls that inhibit accessing and sharing information across agency boundaries.

#	Issue	Problem Description
4	Duplicated facilities & services	There is extensive duplication of environments, carrier gateways, vendor arrangements, support contracts, network management, help-desk services and security services.
5	Duplication of dark fiber services	An abundant and cost effective supply of government owned dark fibre services in the CBD has driven poor behavior from agencies, resulting in a large amount of duplicated services, underuse of available capacity and poor utilisation of assets.
6	Centralised ISPs	While a consolidated ISP model has many advantages for government (particularly in the area of cyber security), it does have some disadvantages in areas where backhaul is limited or expensive.
7	Duplication of carrier access into multi-tenant buildings	Extensive duplication of access circuits into multi-tenanted buildings results in poor utilisation of available capacity, duplication and higher operating costs.
8	Cluster agency consolidation	Agency centric investment reduces duplication of environments and infrastructure for the cluster agencies only. Lack of standardised technologies and processes, constrain seamless service delivery across whole-of Government.
9	Underutilised core infrastructure	Underutilisation of existing physical infrastructure and available capacity results in duplication, higher operating costs and poor utilisation of assets. The future operating model of this strategic asset will determine its viability for both 1WS and the One Network.

Table 8 - Current State network issues

5 Dependencies

5.1 Project dependencies

In line with the One Network initiative and the Governments ICT reforms, the 1WS blueprint is part of an overall change to the business model of IT. This change is driven by industry maturity as much as changes in government policy. The change is characterised by a number of interconnecting initiatives that must be identified and synchronised.

Key to the management of dependencies is identification. Examples of dependencies for the 1WS and One Network initiative are summarised in the table below:

Dependencies	Description
Retirement/disposal of ICT assets	Moving to a service provider IaaS model for network connectivity in a building requires consideration/alignment of agency lifecycle management of network assets. Consider the 1WS location for example. According to the current schedule, agencies will take up residency in the building in 2016. It is proposed that LAN connectivity in that building will be delivered by a service provider. This would mean that agency LAN switching assets (for the relocating staff) would not be required and could be redeployed or retired. Where possible, agencies should look to avoid any investment in refreshing of these assets between now and their relocation to 1WS.
Sharing common resources	Sharing of Printing/Videoconferencing/Meeting Room resources – The model outlined above is that these resources would be provided as common services that agencies utilise and where appropriate, pay for on a consumption basis. This model will present some challenges to the traditional ICT security and cost allocation/billing approaches within government that need to be addressed. It is worth noting that this model may not necessarily be best fit for all circumstances. In situations where a single agency is taking up a long-term tenancy on a floor in a new building it may not make sense to implement a shared printing/conferencing model if there are no other agencies to share with.
Security	As outlined above, the proposed ICT environment for 1WS includes a single logical network. Traditional perimeter security boundaries that agencies have implemented between themselves and other agency networks will not exist. Whilst it is not necessarily a requirement, some agencies may wish to implement increased endpoint security, data encryption or traffic encryption in light of the open nature of the building network. In any event, agencies will most likely need an endpoint VPN solution to connect back to agency networks for any legacy application access requirements.
One Network	It is expected that the 1WS program may provide a catalyst for the One Network initiative. See the One Network discussion paper for actions. However neither have direct dependencies and the following components may occur in parallel or independently: • Implementation of a federated identity capability across participating One Network agencies. • Implementation of non-perimeter security approach. • Implementation of a cloud services broker and associated uptake of cloud services

Dependencies	Description
Government Interconnect and Collaboration portal	The stated direction of government to divest CITEC's role to the private sector may have impact on certain service components which currently exist. Use of Govnet (QGN) to achieve cross agency collaboration, the Metropolitan Area Network and the Polaris Data Centre may require a new approach.
Interim VLAN assignment	The dynamic assignment of agencies into separate VLAN's requires the establishment of a shared identity/authorisation model for Queensland Government. The architecture and governance of this model must align with the "One Network" initiative.
Procurement	The Government's ICT audit and Cloud Strategy is driving broad changes to ICT delivery in Queensland Government which affects the approach (to future office) outlined in this document. As an example, the government may determine that services such as desktop, telephony and unified communications could in some cases be sourced cost-effectively as commodity infrastructure services, and may then seek to drive use of more common services in some/all of these areas.

Table 9 - Dependencies

6 High level deployment options

6.1 Occupancy

ICT planning activities for the One William Street (1WS) location have changed considerably since the original concept. In particular:

- The number of agencies requiring some level of occupancy in the building has increased from 6 to 21
- The floor layout design has changed significantly on a number of floors
- The desired work style/practices of these new agencies varies from the original concept.

All of these variables plus any future Machinery of Government (MoG) changes need to be considered as part of the ICT blueprint/design for the building. This section highlights several high-level deployment options that should be considered for the building.

In considering the options outlined below, it is important that agencies remain mindful of the fact that the government has a stated intention for 1WS to be a showpiece of a new way of working and for the building to be *"modern, innovative and designed for a creative and adaptable workplace".* This vision should continue to guide thinking, and any approach that does not deliver on this promise should not be considered.

A summary of each option is provided below, followed by a deeper dive into the relative merits of each.

Note – it has already been determined that Ministerial Services will have a standalone network. This paper does not discuss any aspects of delivery for Ministerial Services staff.

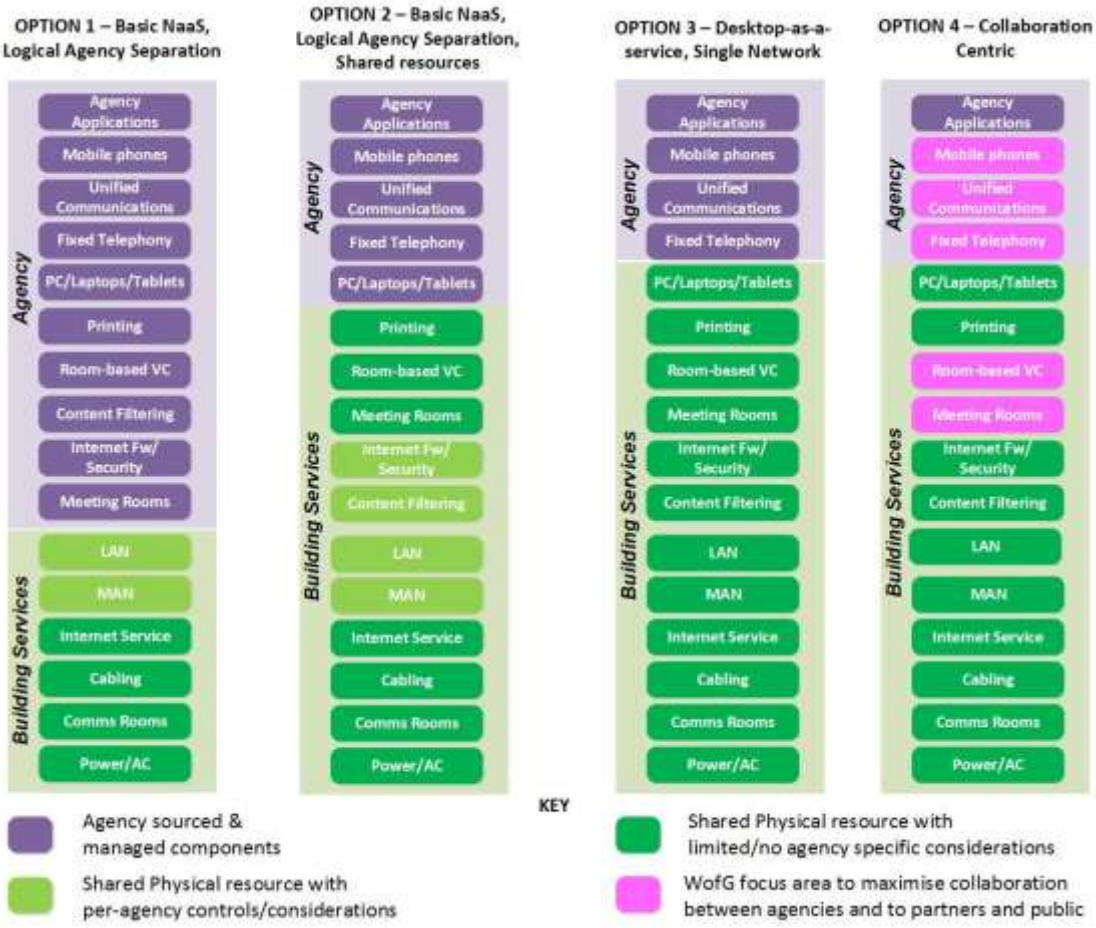


Figure 8 - Four primary deployment options for 1WS.

6.2 Option 1 – Network-as-a-service with logical agency separation

This option is the minimum baseline target for 1WS. Previous agency co-location efforts have typically resulted in per-agency network infrastructure with limited sharing and significant duplication. At a minimum the aim for 1WS must be to reduce this network duplication.

This option would involve the provision of a single physical network (wired and wireless) which will be deployed and managed by a nominated service provider (network-as-a-service). Logical agency segregation will be provided with VLANs/VPNs and trunked back to agency networks where necessary. VLAN assignment on the wired network may be pre-configured or allocated dynamically via 802.1x. Device authentication on the Wi-Fi network will require agency issued certificates providing dynamic VLAN assignment via 802.1x. Guest access will require self-enrolment.

There would be limited sharing of ICT/resources above the network layer. Agencies would relocate existing endpoint devices (PC, Printers etc.) from their current location to 1WS.

6.3 Option 2 – NaaS with logical agency separation + shared resources

As with option 1, a single physical network (wired and wireless) with logical VLAN segregation is deployed and managed by a nominated service provider. Follow-me printing, room based video conferencing, meeting rooms and their associated infrastructure (i.e. booking systems, white boards/projectors) will be shared common services. Digital signage, internet security controls and content filtering will be provisioned as-a-service with per-agency controls/considerations.

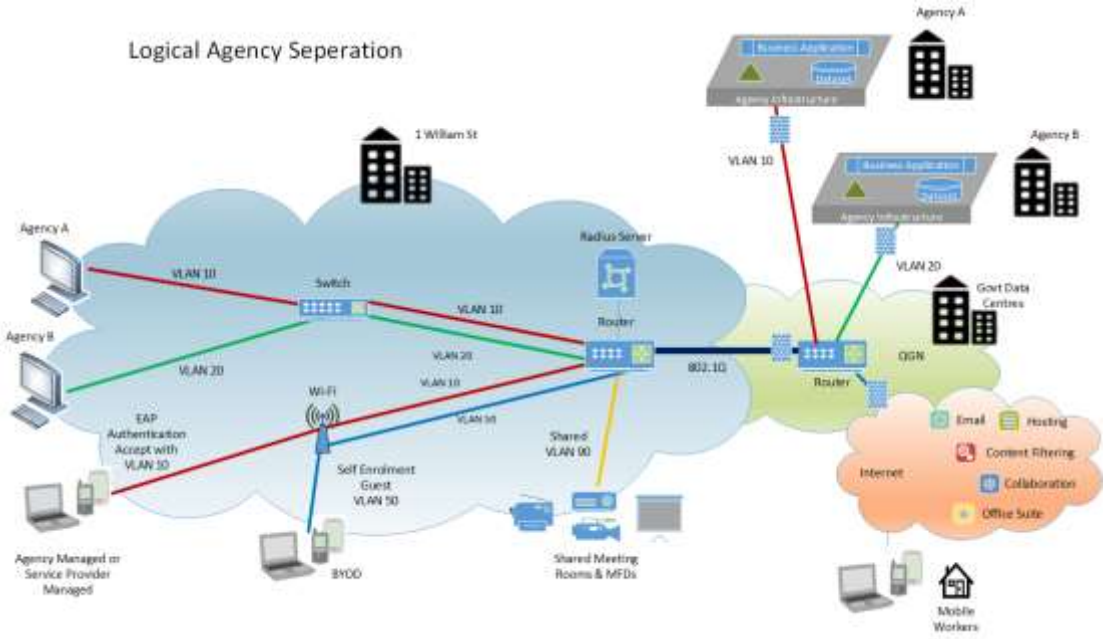


Figure 9 – Logical agency separation

6.4 Option 3 – Desktop-as-a-service + shared network

A single physical network (wired and wireless) is deployed and managed by a nominated service provider. Unlike options 1 & 2 the underpinning network would be agency agnostic and just provide high-speed connectivity to the Internet, a common government network and the ICT service provider. No logical agency segregation would be provided by the network within 1WS.

A role based virtual standard operating environment (SOE) for each agency can be presented, delivering a consistent and full-featured agency branded experience, yet allowing integration and connectivity to 1WS shared resources and collaboration facilities, file systems, legacy apps, cloud based apps and VPN's where required.

Under this model the limitations of network based perimeter security which restricts mobility is removed, providing anywhere, anytime, any device access based on

identity. Agencies will have access to a single workspace for files, applications and virtual SOE desktops, making it easy for users to access widely dispersed information on any device.

Follow-me printing, room based video conferencing, meeting rooms and their associated infrastructure will be shared common services. Digital signage, will be provisioned as-a-service with per-agency controls/considerations. Guest Internet security controls and content filtering will be provisioned as-a-service but it is envisaged that this could utilise a single common rule set for all agencies rather than per-agency controls.

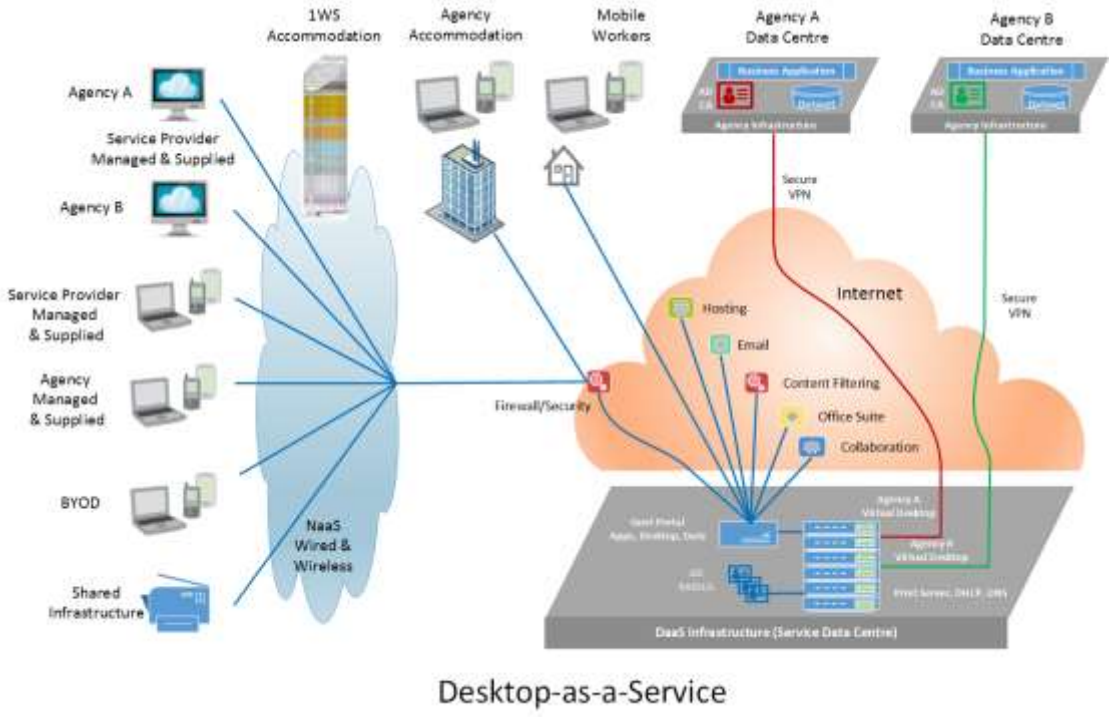


Figure 10 – DaaS + Shared Network

6.5 Option 4 – Collaboration centric

In alignment with the Queensland Governments objectives for 1WS the ICT environment needs to facilitate high levels of interpersonal communication for teams and project groups. To achieve this the model the 1WS environment would need to be architected around a collaboration centric environment that aligns with the One Government/One Stop Shop strategy for the public service, businesses and people of Queensland. See Appendix C -Unified communication and collaboration for further discussion regarding potential benefits.

Option 4 is the same as Option 3 except that there would be an additional focus on the components that are key to achieving collaboration (Telephony, Unified Communications, Meeting Rooms, Video-conferencing, shared EDRMS, Project Management, Sharepoint, Social Networking, etc.). In practical terms, this means ensuring that the ICT solutions adopted by individual agencies provide a feature-rich

collaboration experience not just within their own agency but also to other agencies, partners and the public. This may require that a minimal number of accredited/interoperating solutions be preferred for the building as well as the broader whole-of-Government. This option has more broad-reaching considerations than that of 1WS. It would need to consider whole-of-Government approach to collaboration.

6.6 Matching options to agencies

The following points should be noted:

- There are other variants besides the options presented above that could be considered.
- The options presented above are not a “one in, all in” scenario as not all agencies need to agree to the same model.

It would not be feasible/cost-effective to support many variants in the building. However a hybrid model that supports a couple of the options may be feasible.

Agencies with full 1WS tenancy

DPC, DSDIP and Treasury should strongly consider Option 3-4 as their target for 1WS. Option 2 should be their fall-back position. Option 1 should not be an option they consider.

The rationale for this suggested approach is as follows:

- These agencies are migrating 100% of their staff to the 1WS location so they are not encumbered with the requirement to consider integration/interaction with other agency staff on a legacy ICT environment. They are in a good position to think of a new approach to ICT delivery
- The floor-plan design for these agencies is open-plan and designed for collaborative, interactive working. Options 3-4 are the best options for supporting this work style
- The “some is better than none” philosophy should be applied. Implementing a highly collaborative, shared ICT environment for some of the agencies in the building would mean that government would still have met its commitment/vision for the 1WS to demonstrate a model for future government working. The ICT environment for these agencies could serve as a pilot for broader deployment.

Other agencies with partial tenancy

Agencies other than those indicated above may consider Options 3-4 if they believe they are good fit for their requirements. Option 2, however may be the more realistic goal for these agencies in the first instance. Option 1 is a potential fall-back option. Agencies may also wish to consider an “Option 1.5” which adopts all of Option 1 and some but not all of the changes proposed in Option 2. For example, agencies may wish to share printers and meeting rooms but maintain separate Internet security/content filtering.

The rationale for this suggested approach is as follows:

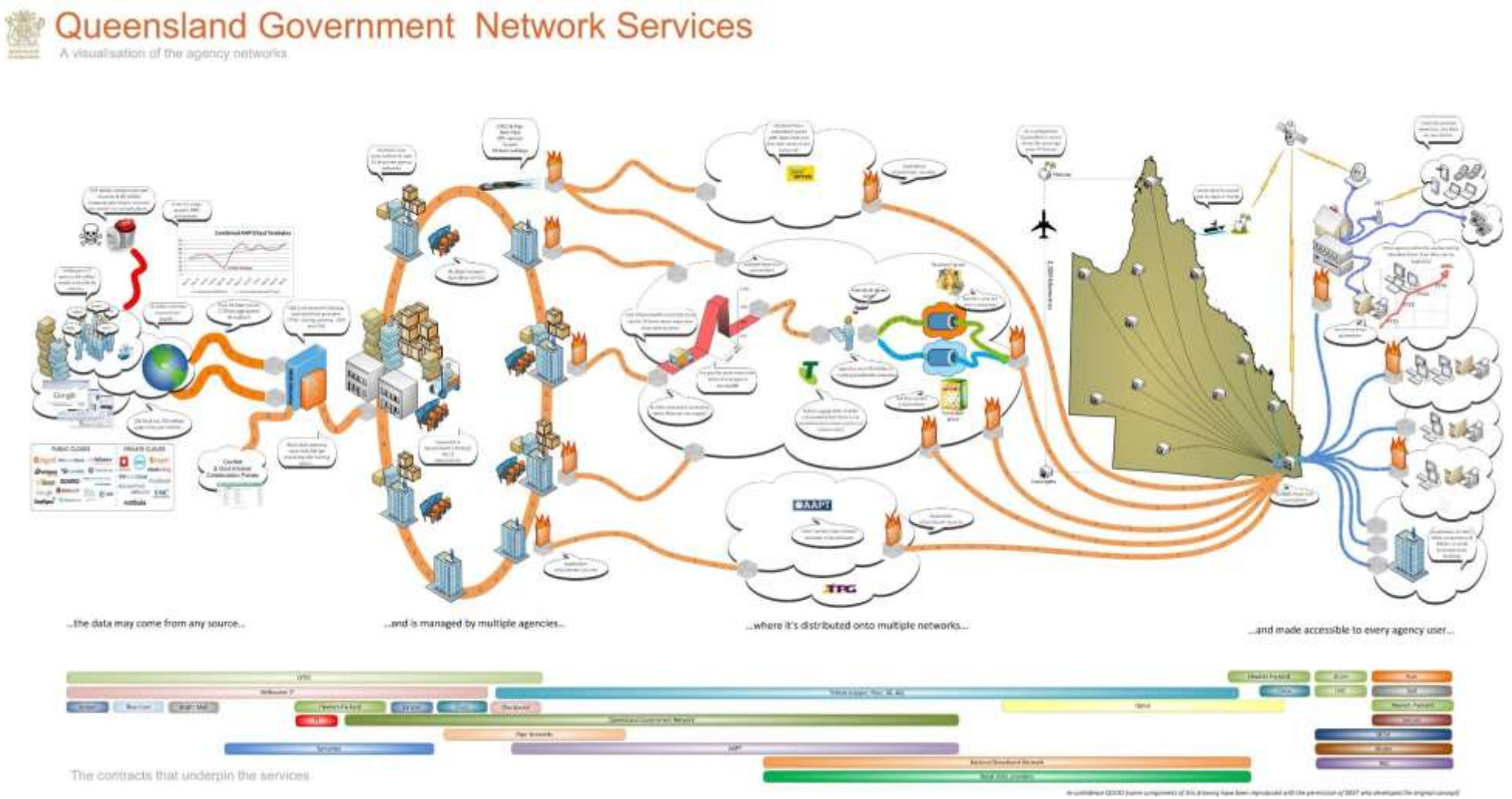
- These agencies are each migrating an estimated 30-40 staff per floor. Of that number, perhaps 10-15 are Ministerial staff which will be on a separate network.

Only an estimated 20-25 staff (i.e. DG, DDGs and support staff) are in scope of the ICT delivery options outlined in this document. Options 3-4 may require substantial change to end-user ICT environment (see note below). If that is the case, undertaking this effort and dealing with integration back into the rest of the agency network/applications/users may not be cost-effective for such a small number of staff

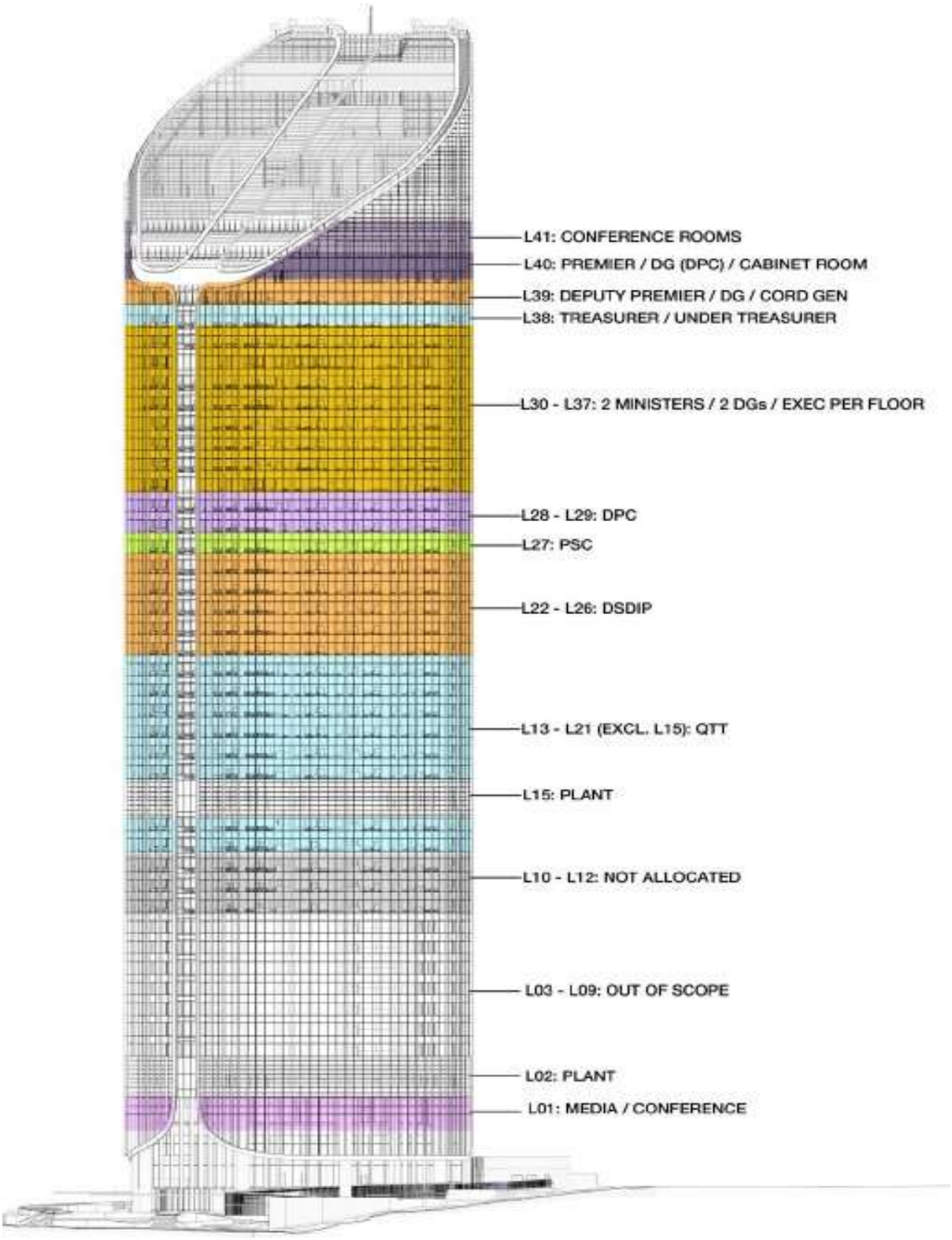
- The floor-plan design for these agencies has limited open-plan areas and much more fixed office style. This fact combined with the style of working in Ministerial/DG areas may mean that there is less requirement for the full collaborative/shared ICT environment.

Note: - A key factor in the decision to be made by these agencies will be the extent to which the Desktop-as-a-Service (DAAS) model can deliver a virtual SOE which provides a similar experience to that which they already have. If the DAAS architecture can provide a solution that is low impact on users/support staff and has simple integration back into agency ICT environments then Option 3 should be considered as a genuine option for these agencies.

Appendix A - Qld Government network services overview



Appendix B – Proposed tenant occupancy plan



Appendix C – Unified communications and collaboration

Enabling improved collaboration

Consideration needs to be given to the Unified Communication and Collaboration (UCC) solutions/approach adopted by agencies.

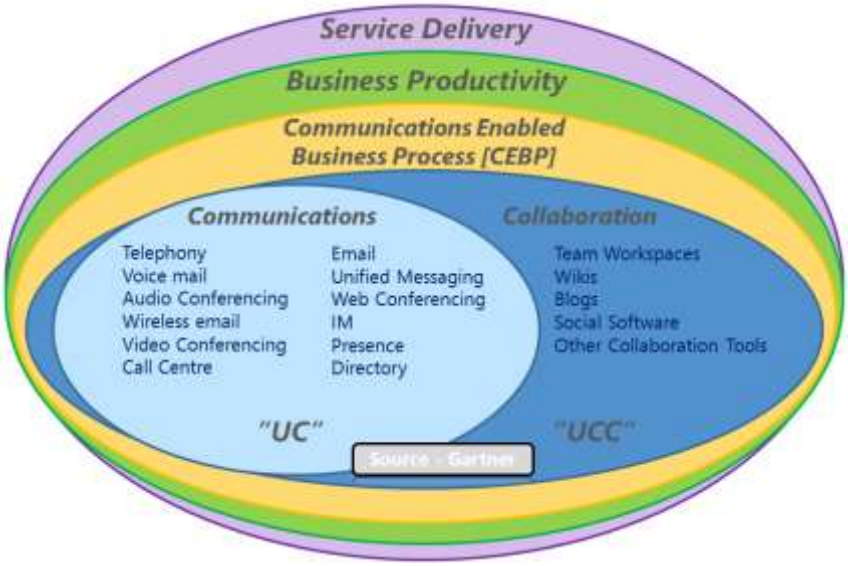
What is UCC?

Unified Communications (UC) is the integration of real-time communication services such as instant messaging (chat), presence information, telephony (including IP telephony), video conferencing, call control and speech recognition. All have non-real-time communication services such as unified messaging (integrated voicemail, e-mail, SMS and fax). UC is not a single product, but a set of products that provides a consistent unified user interface and user experience across multiple devices and media types.

Unified Communications (UC) evolved from two key technology areas: the telecommunications area, with roots in IP-PBXs, unified messaging and videoconferencing; and secondly, the email and desktop collaboration market, with roots in e-mail, IM and web conferencing.

As communications shifts to software, communication applications and components are more easily integrated with other applications. One important advantage of this type of integration is that applications can provide a context for the communications activity, and, as a result, individuals may be more productive if collaboration and communication functions are combined or integrated.

UC is increasingly being offered as part of, or integrated with a collaboration platform to form unified communications and collaboration (UCC) as depicted below:



UCC delivers important functionality in its own right and importantly is also a core enabling capability for the broader imperatives of business productivity and service delivery. Access to rich collaboration services across the extended enterprise is increasingly important to all organisations. It is a powerful and foundation enabler for driving efficiencies across internal operations and enriching the interaction with external stakeholders and clients.

Benefits of UCC

In simple terms, UCC integrates all the systems that a user might already be using and helps those systems work together in real time. This can drive benefits in a range of areas such as reduced travel/operating costs, improved customer service and improved productivity.

Some example scenarios could include:

- Seamlessly collaboration between two people working on a project, even if they are in separate locations. One user could quickly locate the other by accessing an interactive directory, verify availability via presence, engagein an Instant Messaging(IM) chat session, and then escalating the session to a voice call, or even a video call and share content all through a single unified client interface
- An employee receives a call from a customer who wants answers. UCC could enable that worker to access a real-time list of available expert colleagues, then make a call that would reach the necessary person, enabling the employee to answer the customer faster, and eliminate rounds of back-and-forth emails and phone-tag
- High-level executives in the agency need to convene quickly for an urgent decision/ discussion. A multi-way video call using desktop video solution could be used to allow the executives to quickly address the issue with their peers from their own offices (or mobile in some cases) on the spot without needing to arrange and travel to a meeting
- Ability to establish a video call with multiple participants using any device type across any network and in any location and then add desktop/document sharing into the mix. This scenario allows true anywhere, anytime, and device collaboration
- Single number contact is the ability to dial a single number for a user that can be linked to multiple different devices (office, home, mobile) plus intelligent routing of same. This means people need to only know a single number to contact a person, and the person can take the call on the device of their choice, handing off between devices if required. A person could choose to participate in an early morning conference call initially via their home phone, then transition the call to their mobile whilst on the train to work, and then swap to video phone once they are in the office. All of this could be done seamlessly without impacting others in the conference. This flexibility increases availability and productivity of staff and also helps support improved work/life balance
- Contact Centre Integration – Contact centres are increasingly requiring seamless integration with back-office staff/systems throughout the organisation and beyond. Integration of contact centre systems with UCC solutions used more broadly in the organisation can potentially enable any expert in the agency to be incorporated in the customer service interaction via whatever mechanism (chat, voice, video) that suits the customer
- Calendar integration and configurable call preferences automatically direct calls to voice mail when a user is on holidays and only allow calls in meetings from nominated individuals
- Common voicemail box between mobile, desk phone and email

- UCC solutions provide capability to integrate/federate with other customers or the public. For example, the ability to see “presence” of your account executive at a service provider and then initiate a IM/video call is a possibility. Another example could be to enable a Skype video call from a member of the community to agency staff.

The case for a strategic whole-of-government approach

Many of the core ICT building blocks that enterprises rely upon already have a degree of embedded UCC capability and are continually being enhanced to provide additional UCC functionality over time. Consequently every product/service purchase, software upgrade, contract renewal and service provider selection that an organisation makes is potentially committing to a future UCC solution whether the organisation is aware of it or not.

The potential benefits to Queensland Government via effective use of UCC could be significant, but only if a holistic approach is adopted across government. There is considerable risk that a per-agency approach could lead to fragmented outcomes and undermine the ability to deliver improved collaboration and service delivery across government and to partners and public.

UCC remains at an early stage of market adoption and product maturity. While many of the vendors now offer a full suite of functionality, the capabilities and degree of integration within vendor’s portfolios varies. Standards support (e.g. SIP, XMPP) are critical for success in today’s multivendor environments however this alone is not enough to achieve genuine interoperability between different vendor solutions. Third party integration certification is required and even this requires ongoing strategic partnership between vendors. While there are vendor alliances emerging there is currently limited true interoperability between UC systems.

In order to achieve the sort of benefits outlined above it will mean that the ICT solutions adopted by individual agencies provide a feature-rich collaboration experience not just within their own agency but also to other agencies, partners and public.

The bottom line is that this may require that a minimal number of accredited/interoperating solutions be preferred across government. If this approach is not adopted and too many different solutions are implemented government then it is likely to perpetuate/create the following problems:

- Agencies will not be able to see calendar free/busy with other agencies, or at best may be able to integrate with some agencies but not others
- Agencies will not be able to see “presence” information outside of their own agency, or at best may be able to integrate with some agencies but not others
- The “One Stop Shop” solution for government will not be able to effectively integrate with agency back-office staff/systems in a feature-rich way, or at best will be able to do this for some agencies but not others
- Feature-rich video calling and desktop/document sharing will not be able to be cost-effectively achieved across government, or at best will be able to be done for some agencies but not others
- Feature-rich IM/video interactions extended to partners/public will not be able to be cost-effectively achieved across government, or at best will be able to be done for some agencies but not others

Relevance to the 1WS initiative

In reality, adopting a whole-of-Government approach to UCC is far more wide reaching that the 1WS initiative and it needs to be viewed as such. The 1WS initiative does however have the potential to be a catalyst for change across government.

The following relate to the 1WS initiative:

- The state vision/objective for the 1WS building is to be modern, innovative and designed for a creative and adaptable workplace. The intention is that it be a showpiece for a new way of working and facilitate high levels of interpersonal communication for teams and project groups. An effective implementation of UCC could be a key enabler of this goal
- All agencies will have some level of occupancy in the building and this is driving a need to consider areas for reduced duplication and increased sharing. ICT Implications of this include:
    - Shared video-conferencing systems
    - Potential (option) for single building telephony system
    - Shared video-conferencing/meeting room facilities
    - Potential Identity Management integration/federation
    - Tighter integration/federation of calendaring systems (for resourcing booking).

Outcomes explored in these areas are likely to be relevant in the broader whole-of-Government UCC discussion. The partial tenancy of a number of agencies means that ICT solutions such as UCC, that facilitate collaboration and communication with other (non 1WS) areas of the agency will be critical.

Appendix D – Myth busting DaaS

Reference:
NEC Corporation of America
www.necam.com
White Paper
Myth busting DaaS: Debunking the Top 10 Cloud-Hosted Virtual Desktop Myths

Summary

Desktops as a Service (DaaS) is the delivery of a virtual desktop offered as a hosted service offered by a service provider. DaaS has the potential to radically change the way desktops are purchased and managed. However, as is typical with such emerging, disruptive technologies, there is a good deal of confusion about what is and isn't possible with DaaS.

This paper exposes—and debunks—the top 10 DaaS myths, which range from supposed cost, user experience and security issues, to ease of use, licensing and integration limitations. It shows how, by consuming virtual desktops as a cloud-hosted service, businesses can deliver high-performing desktops to users on any device in minutes, easing IT management burdens and reducing the total cost of desktop ownership.

Myth #1: You can't do DaaS under Microsoft licensing

There has been a lot of noise recently about the difficulty or impossibility of offering DaaS to the market in a technically viable and cost-effective way given the challenges imposed by Microsoft licensing. Not only is it possible to offer DaaS successfully, but service providers are also moving on this opportunity and organizations are consuming it.

- For a full dedicated Windows 7 client desktop: The service provider runs dedicated servers for each customer and the end customer uses Microsoft VDA (virtual desktop access) licensing for the Windows desktops. If you already own Software Assurance on the end user device, it includes VDA and allows you to access the virtual desktop. A multi-tenant DaaS platform can still be leveraged for the management layer, reducing the costs of management, shared storage and networking.
- For a shared or dedicated Windows Server OS: Windows Servers can be licensed using SPLA (service provider license agreement). In this case, a service provider can rent a Windows Server to a customer on a monthly basis. A DaaS multi-tenant platform can provide the ability to partition a server and share it with multiple customers. This is done securely by providing separate datastores and VLANs per customer, allowing the service provider to achieve 100% fulfilment of compute resources.

Myth #2: Only shared session-based desktops can be used for DaaS

Many believe that you can only use a shared desktop technology like terminal services to deliver DaaS. This is true when looking at traditional VDI technology. However, VDI technology with true multi-tenancy, is capable of delivering full featured VDI desktops. A dedicated virtual desktop delivers a user experience that surpasses that of terminal services. This makes the DaaS user experience consistently strong regardless of how many people concurrently access their desktops.

A dedicated desktop allows users to work with their desktop in the same manner they work with their traditional physical PC. They can customize it and install applications. Even if shared desktop technologies could be rigged for DaaS, they would not be appropriate for

most users for the simple reason that they do not allow local installations. Commonly used online services, such as WebEx, Skype and Dropbox, would be off limits, rendering the solution ineffective.

Myth #3: DaaS is expensive like traditional VDI

It's true that Virtual Desktop Infrastructure (VDI) can be very expensive. In fact, that's one of its main drawbacks, especially the upfront cash/CAPEX investment. DaaS, however, is very different. Whereas traditional VDI requires purchasing and supporting new infrastructure, such as servers, networking and storage, DaaS has no upfront capital expenditures and lower ongoing OpEx. That's because rather than providing your own infrastructure, you're utilizing the service provider's environment. And, since you only pay for the resources you need, not only are the costs associated with DaaS predictable, you benefit from the buying power of large service providers.

On an ongoing basis, DaaS costs just a fraction of VDI to maintain. Provisioning efforts and related expenses are dramatically lower because there are no physical machines to rollout; you simply click on the DaaS portal to order and configure virtual desktops. Decommissioning is just as quick.

Myth #4: DaaS delivers poor user experience

The DaaS user experience is as good, if not better than, a rich client experience, and significantly better than a shared terminal services based desktop and VDI deployed onsite. One of the main user challenges of VDI is servicing a user who is physically far away from the VDI datacenter. With DaaS, you can optimize performance by partnering with a proven cloud-hosted desktop provider. That way you can take advantage of global data centers where proximity to users and world-class infrastructure results in sub-20 millisecond latency. These providers also allow you to choose best-fit protocols for task workers, graphics and video needs, and mix and match depending on the use case.

Myth #5: DaaS security is lacking

Some businesses are concerned that DaaS will put their data at risk. This is an unjustified fear. DaaS can be more secure than traditional PCs, where data resides locally and can easily be lost or stolen. With DaaS, each employee's data resides in the corporate data centre (see Myth #6) —not on the user's device and not offsite at the cloud hosting provider. Even if a user's device is lost, the data is protected. A high level of security is ensured by maintaining your corporate security features and policies (i.e. with firewalls and Active-Directory controls). No longer do you have to worry about viruses from local desktops infecting the corporate network.

Myth #6: DaaS won't work with your onsite IT assets

Many believe that because their desktop is now in the cloud, they can't access IT assets located onsite. DaaS is designed to securely work with virtually any IT asset. This includes resources that are onsite at your organization or offsite at your provider, such as shared storage, Active Directory and enterprise applications. DaaS providers can also integrate with other cloud services for an enhanced overall offering. Users will be able to use their cloud-hosted desktops exactly how they used their old physical PC.
White Paper

Myth #7: DaaS does not support consumerisation of IT

Not only is consumerisation of IT supported, but DaaS also makes it much easier to implement and manage. DaaS is ideal for “bring your own device” (BYOD) approaches, since employees can get their Windows desktops on whatever hardware they choose, including iPads, Androids and Macs.

With DaaS virtual desktops, users can easily segregate work from personal life without having to carry two devices. IT wins with DaaS too. Inside the virtual desktop, you can ensure secure, policy-controlled access to the corporate network. Everything outside the corporate virtual desktop can be at the discretion of the users, who support their own personal device and software.

Myth #8: Migrating users to DaaS is hard

It’s actually a lot easier than you think, especially when you compare migrating DaaS users to replacing a PC or laptop. Users can customize their desktops to look and feel exactly as they’d like. They can also install their own applications and data. And, because DaaS can connect to peripherals such as local and network printers and monitors, employees can use their desktops just as they have in the past. It’s simple, fast and requires little to no user training. A DaaS multi-tenant platform can provide the ability to partition a server and share it with multiple customers. This is done securely by providing separate data-stores and VLANs per customer, allowing the service provider to achieve 100% fulfilment of complete resources. DaaS also minimizes time-consuming, expensive help-desk support. Repairing a desktop is as easy as refreshing it with a new virtual machine (VM). There is no downtime, no lost productivity because of users waiting for desktop to be fixed, and no lost revenue.

Myth #9: DaaS requires lots of bandwidth

This is a misconception because people erroneously believe they will be downloading a ‘desktop’ every time they use DaaS. Average DSL is more than sufficient to accommodate DaaS. When you working, only the pixels that change are transmitted back to the endpoint. As a result, most of this downstream changes to the screen are pushed from the virtual desktop to the endpoint. This matches up well with how bandwidth is provisioned, as download bandwidth is usually on orders of magnitude greater than upload bandwidth. The average bandwidth utilization is around 100 kilobytes per session.

Myth #10: The disconnected use case is a deal-breaker

Cloud-hosted desktops, as well as traditional VDI, require the user’s device to be connected. However, this is not a big issue for businesses. In fact, Wi-Fi and 3G/4G has become so prevalent, we haven’t heard of any instances where this prevented an organization from adopting and reaping substantial benefits from cloud-hosted desktops. The reality is that most users don’t need continual or even frequent disconnected access. Many people who need to be connected generally want it at ad hoc times for email, and they can do that pretty easily with wireless and Wi-Fi, and devices like smartphones and iPads. The few users who do need continual connections can be provisioned with rich laptops.

Conclusion

DaaS is rapidly gaining momentum in businesses of all sizes because it delivers tremendous benefits compared to traditional VDI, terminal services and rich desktops. Although not intended to be the solution for every user in your organization, the fact that DaaS is so flexible, secure, manageable, inexpensive and high-performing, makes it ideal for the majority of workers.