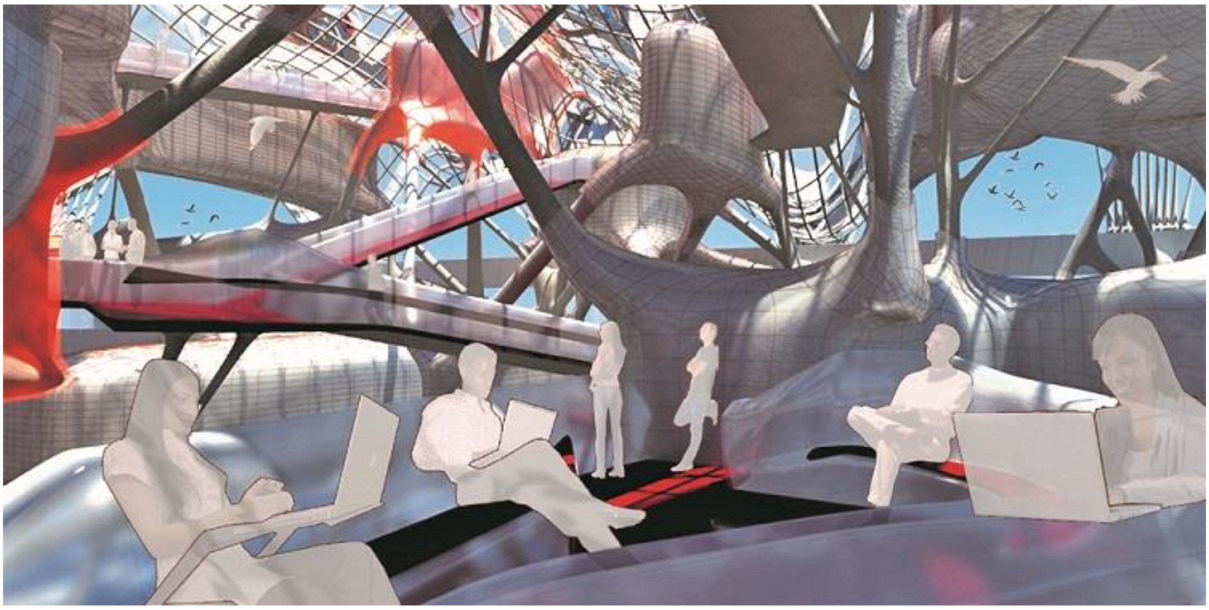
Department of Science, Information Technology and Innovation



Future of Office Space - Designer: Alexa Getting.

Collaborative workspace

Strategy and principles

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

Final

February 2017

V1.0.0

PUBLIC

Queensland Government

Document details

Security classification	PUBLIC		
Date of review of security classification	February 2017		
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
qgcio@qgcio.qld.gov.au

Acknowledgements

This version of the *Collaborative workspace for the future – Strategy and principles* 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

1 Acronyms 5

2 Introduction 6

2.1 Background 6

2.2 Purpose 7

3 Business environment and requirements 7

3.1 Business drivers/objectives 7

3.2 Technology trends 8

3.3 Vision 9

3.4 Principles 9

3.5 Assumptions 12

4 Future state 12

4.1 A new approach 12

4.2 Technology architecture 13

4.3 Applications and higher layers of the stack 14

4.4 Collaborative workspace features/attributes 16

4.5 Services architecture 20

4.6 Integration 40

4.7 Exclusions 42

5 Current state 42

5.1 Analysis 42

5.2 Audit recommendations 43

5.3 Changing demands 43

5.4 Constraints of the existing applications 44

5.5 Constraints of the existing networks 46

6 Dependencies 47

6.1 The 1WS as-a-service model 47

6.2 Project dependencies 48

7 High level deployment options 50

7.1 Occupancy 50

7.2 Option 1 – Network-as-a-service with logical agency separation 51

7.3 Option 2 – Network-as-a-service with logical agency separation + shared resources 52

7.4 Option 3 – Desktop-as-a-service + shared network 52
7.5 Option 4 – Collaboration centric 53
7.6 Matching options to agencies 54
Appendix A - Qld Government network services overview 56
Appendix B – Unified communications and collaboration 57
Appendix C – Myth busting Desktop-as-a-service 61

Figures

Figure 1 - Technology stack adopted for the 1WS project 13
Figure 2 - Application diversity across agencies 14
Figure 3 - Future ICT Platform 15
Figure 4 – Stepped change 21
Figure 5 - Services for collaborative workspaces of the future 22
Figure 6 – User workspace services 37
Figure 7 – Government AppStore 39
Figure 8 - Current state network visualisation 46
Figure 9 - Four primary deployment options for collaborative workspaces. 51
Figure 10 – Logical agency separation 52
Figure 11 – User workspace/DaaS + shared network 53

Tables

Table 1 - Technology principles 10
Table 2 – Operational principles 11
Table 3 – Implementation principles 12
Table 4 - Assumptions 12
Table 5 – Architectural alignment 16
Table 6 - Future office attributes 20
Table 7 – WWN service benefits 29
Table 8 – Room booking service benefits 31
Table 9 – Print and imaging service benefits 32
Table 10 – VCTC service benefits 35
Table 11 - Service ownership 41
Table 12 - Barriers to shifting ICT service paradigm 45
Table 13 - Current State network issues 47
Table 14 - Dependencies 50

1 Acronyms

An abridged list of acronyms used in this document is defined below. A comprehensive glossary of terms and definitions can be found on the QGCIO Glossary page (http://www.qgcio.qld.gov.au/products/glossary).

Acronym	Definition
CAC	Common Access Card
Building service provider	A person who provides building services for the Site and includes the owner or manager of the Site.
Integrator/ICT service provider	A person who provides ICT services for the Site and includes the integrator and subcontractors
CA	An entity that is responsible for the issuing of digital certificates.
MFD	Multi-function print and imaging devices
Core and underpinning services	• Wired and Wireless Network (WWN) including Guest network web content filtering • Print and Imaging (PAI) • Room Booking (RMB) • Federated Identity Management (FIM) being enabled integrated access to shared applications • Security Management (SEC) • APIs for future integration with Site facilities • Support Services and Maintenance Services • Contractor Help Desk.
SIP	Session Initiation Protocol (SIP)
Threat Risk Analysis (TRA) Controls	Security controls used to mitigate assessed threats and risks.
Block Patching	1-to-1 connections from switch to patch panel
IPTel/ VOIP	IP Telephony/ Voice over Internet Protocol
LAN/MAN	Local Area Network/ Metropolitan Area Network
Guest Network	The network used by specific End Users and Guests at the Site.
802.1X	Is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN
POE	Power over Ethernet
GovNet/ QGN	Queensland Government Network
QGIS	Queensland Government Internet Service
SSID	Service Set Identifier
UTP/Cat6e	A standardized twisted pair cable for Gigabit Ethernet
VLAN/VPN	Virtual Local Area Network/ Virtual Private Network
End User	An employee of a service recipient consuming the managed services provided
WLAN	Wireless Local Area Network

2 Introduction

2.1 Background

A new approach to ICT architecture and facilities management is required in larger multi-agency office buildings. The approach must provide consistent, high-quality services to agencies while also balancing the government's desire to achieve value-for-money for the State.

The key characteristics of office accommodation in the future is likely to be the provision of a more harmonious, integrated and flexible workplace. 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 catalyst for major change in the way ICT services will be delivered and consumed by tenanted agencies has been driven by the One William Street (1WS) implementation and associated learnings. It removes the current siloed state of agency ICT environments, where commodity ICT infrastructure and services are duplicated within each agency, as well as reducing the high level of technology diversity that inhibits the ability to share information and leverage economies of scale as appropriate.

The completion of a rigorous ICT service procurement led to the establishment of a panel of suitable ICT service integrators for future single and multi-tenant government buildings which was completed in August 2015. Consultation is occurring between Queensland Government Chief Information Office (QGCIO), Queensland Investment Corporation, Government Accommodation Group (Department of Housing and Public Works) and Commercial Group (Queensland Treasury), to leverage 1WS base building fit-out specifications, standards and contractual arrangements for broader adoption in future government building refurbishments.

The adaptive ICT technologies and services being deployed will offer tenants a greater level of mobility, flexibility, productivity and interagency integration. The positive impact will eventually be a seamless, standardised ICT environment for staff, with much less waste through repeated or redundant ICT services.

The future workplace must support either the same end-user computing environment as other agency premises, or one which will allow simple 'low touch' integration within those environments and not place undue support burden on agency staff or require significant end-user training.

ICT services delivered out of collaborative workspace environments will be procured and consumed by agencies on an 'as-a-service' basis. The expectation is one of transformational change enabled by the underpinning ICT environment acting as the 'bedrock' while business initiates change to embrace new ways of working through:

- modern activity based environments
- collaboration between staff, public and private sectors.

This Collaborative workspace ICT strategy and principles has been developed based on the 1WS State Blueprint and has been designed to be a repeatable architectural pattern intended to be applied to future multi-floor, single-agency and multi-agency government buildings.

2.2 Purpose

The purpose of this document is to translate the State's ICT business requirements and scope for future collaborative workspace environments into a high level services architecture.

The document will:

- articulate the expected outcome for take up of ICT services in single tenant and multi-tenant buildings[1]
- provide an 'umbrella' architectural document that can be referenced by agencies as they 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 procured through 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 into agency migration plans
- Offer a repeatable architectural pattern for implementation and/or migration of other multi-floor, single-agency and multi-agency buildings in the future.

3 Business environment and requirements

3.1 Business drivers/objectives

The Queensland Government's objectives for developing collaborative workspace environments are to:

- create a productive, harmonious environment that accommodates the Queensland Public Service by providing a cohesive interagency integrated workspace, encouraging collaboration and increasing productivity
- challenge the way the Queensland Government traditionally use digital technologies, by taking a more collaborative approach to how we work
- use technology to introduce complementary cross-agency processes and synergies achieving the best outcomes for the people of Queensland
- achieve economies of scale and value for money for the State
- work holistically, efficiently and effectively across agencies within a shared workspace
- make transitional steps in the ICT delivery models and network architecture to enact a number of recommendations and actions from both the Commission of Audit (February 2013) and the Whole of Government ICT strategy 2013-2017)

[1] This document is a revision of the 1WS State ICT Blueprint published in May 2014 which outlined a number of high level deployment options, tiered for core (common) and non-core (optional) services that could be taken up by agencies during their transition or over time.

- provide coordinated delivery of services and infrastructure, resulting in less waste and rework
- facilitate greater face-to-face interaction between government employees, improving communication and outcomes for the public service and customers.

3.2 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 cellular mobile phones, soft-phones and wireless IP telephony (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 (see appendix B, page 1) 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.

3.3 Vision

A key characteristic of future office development will be the provision of a more flexible and harmonious 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 very nature of the way we conduct our day to day business will be a catalyst for a shift to a less-process and more-creative set of job responsibilities supported by ever evolving technologies. To enable this transformation, the workplace characteristics highlighted above need to be enabled by the underpinning IT environment acting as the 'bedrock' while 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'.

3.4 Principles

There are a range of technology, operational and implementation principles that will guide the ICT solution and services for future collaborative office environments.

Technology principles

The proposed technology design principles are outlined below:

Ref	Principle
TP1	Adopt open/common 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.

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

Ref	Principle
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 Green Star[3] vision for future buildings.
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 and the cloud first strategy should be applied.
TP8	The architecture must support a high level of staff mobility (anywhere, anytime, on any device connectivity) – a capability fundamental to the One Network[4] initiative.

Table 1 - Technology principles

Operational principles

The proposed operational principles 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 proof (to the highest extent possible).
OP3	The ICT architecture should provide a boost in collaboration, productivity and agility within and across agencies. This will ultimately embrace 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). Support as-a-service model should be considered where feasible.
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 help to identify areas of wastage and assist users and agencies to modify their behaviours if needed.
OP7	Be provided by the Contractor that is accredited with ISO 27001.

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

[4] The One Network initiative comprised a DSITIA ICT Renewal and QGCIO concept brief and market sounding to explore the barriers to success and options available in achieving anywhere, anytime on any device connectivity to cloud and agency applications.

Ref	Principle
OP8	Be centrally managed by the Customer's Contract Manager, including performance management, capacity planning, and issue resolution.

Table 2 – Operational principles

Implementation principles

The proposed implementation principles are outlined below:

Ref	Principle
IP1	The ICT architecture will address the government's requirements for collaborative workspaces and provide a repeatable model for other single and multi-agency green and/or brown field buildings in the future. At a practical level, this document is aimed at balancing the need to interface with the current ICT systems of agencies, while enabling the maximum benefit to be achieved for tenants of the building from the advances in both technology and service delivery models.
IP2	Increased sharing and reduced duplication of ICT infrastructure.
IP3	The government will consume an IP network (as-a-service) behind the government gateway. This network will link buildings adopting this architecture to all existing government networks and to the government Internet gateway[5].
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.
IP7	Be scalable (up and down) for the site and, where possible, for future multi-tenant customer buildings
IP8	Be 'Evergreen', where underpinning technologies are kept up to date and upgraded as appropriate over the contract period such that all services remain N-1 or as agreed

[5] In alignment with the Internet Protocol (IPv4) addressing standard and consumption of GovNet services, Queensland Government Network (QGN) connectivity was chosen as the most efficient, cost effective and scalable means of connecting multi-tenant buildings to agency data centre infrastructure (including Internet). Currently all agencies have an extranet presence within the GovNet/QGN core allowing migration into 1WS and other Governments buildings to be accomplished in a seamless manner and without additional expense.

Ref	Principle
IP9	Be designed and delivered in accordance with the following Codes, Policies, Guidelines and Standards: • Information standard: Information security (IS18) • Queensland Government Authentication Framework (QGAF) • Queensland Government information security classification framework (QGISCF).

Table 3 – Implementation principles

3.5 Assumptions

The key assumptions that apply to future office tenancies are:

Ref	Assumption
A1	Agencies support the need for a new approach to ICT delivery in future office locations, with increased sharing and reduced duplication of ICT infrastructure/ services.
A2	While the benefits of collaboration, mobility and efficiencies gained through sharing and economical use of resources are not able to be converted to a financial metric, they are considered outcomes of the holistic approach that will enable and enhance the features of the workplace design.
A3	Agencies are to meet the costs of their transition to future office locations out of agency budgets by managing short term expenditure if it does not align with the new tenancy take-up of services.
A4	Agencies will be operational on most or all of target ICT components prior to occupancy in the new tenancy[6].

Table 4 - Assumptions

4 Future state

4.1 A new approach

The collaborative[7], flexible and creative workplace desired for all Queensland Government buildings 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 collaborative workspace of the future or for any similar sites. A new way of working culture needs to be embedded across government, supported by a new approach

[6] All agencies that transitioned into 1WS are operational on the core and underpinning components of this document. As such future service integration work for buildings adopting this architecture will be minimal.

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

and underpinning infrastructure that enables innovative, harmonious collaboration between agencies.

The world of ICT has changed enormously in the last few years and will continue to evolve at an increasing rate. 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.

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 government's desire to achieve value for money for the State.

4.2 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 below) are where shared commoditised services are relevant for multi-tenant buildings.

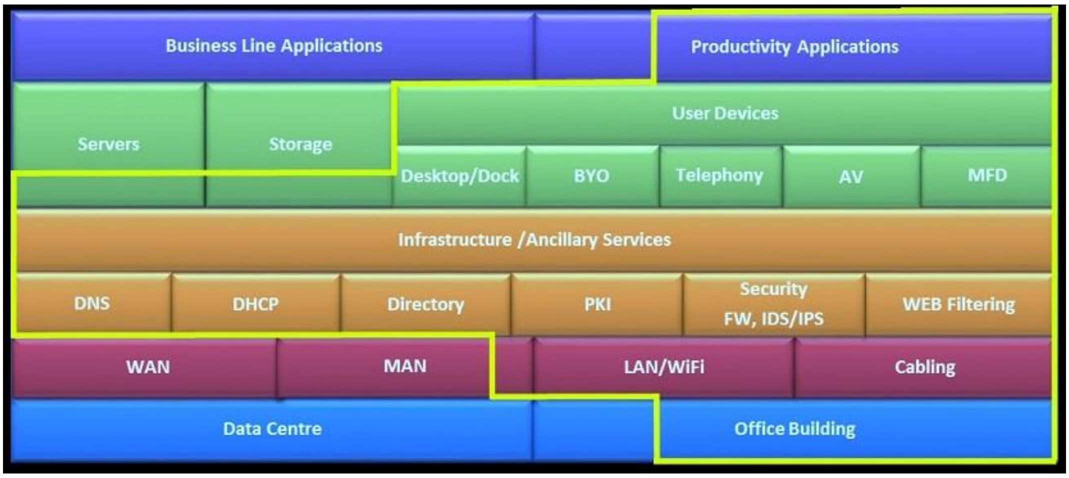


Figure 1 - Technology stack adopted for the 1WS project

It is proposed that, the services outlined in yellow in figure 1- Technology stack adopted 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 value for money) to retain these services in-house.

4.3 Applications and higher layers of the stack

Government services, business processes, information sets, and applications are generally specific to an agency's function and limited capability to share across agencies currently exists. 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.

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
   - customer relationship management (CRM)
   - finance/human resources
   - records
   - utility apps – 'corporate', training, procurement, time etc.
3. cloud-based services/managed services.

The diversity of agency environments is depicted in figure 2 below:

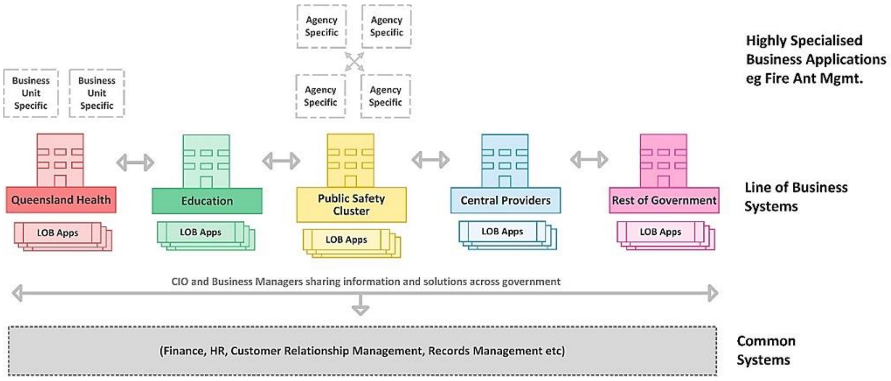


Figure 2 - Application diversity across agencies

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 a small number of staff are to be accommodated in future office tenancies, connectivity to an 'office suite' may be the primary requirement. Under this model user workspace/desktop-as-a-service (DaaS) and cloud based services may prove to be a more flexible approach[8].

Agencies who are migrating all or the majority of their staff to a future office 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.

Figure 3 below depicts the target ICT platform:

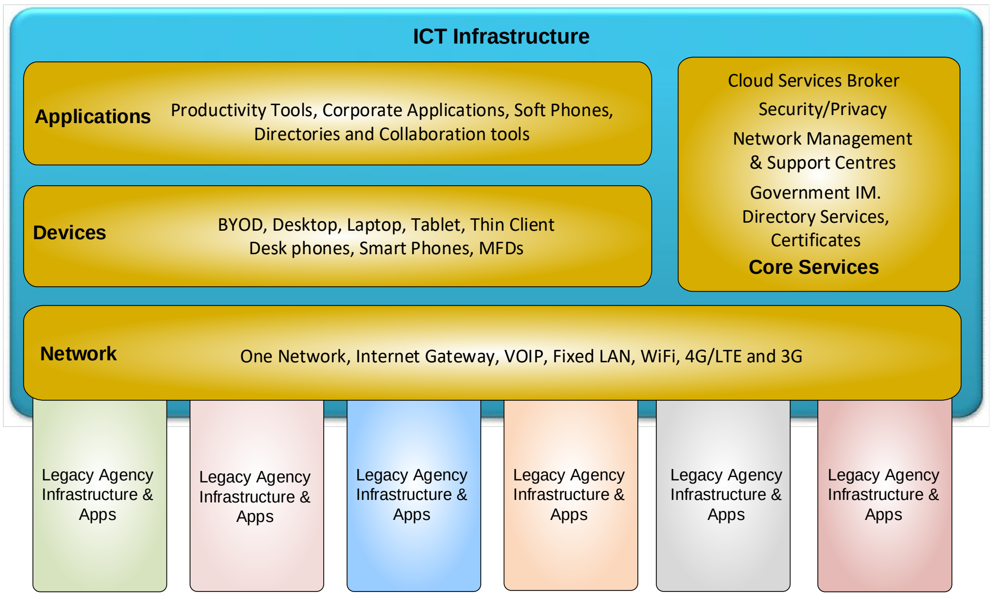

ICT Infrastructure
Applications
Productivity Tools, Corporate Applications, Soft Phones, Directories and Collaboration tools
Devices
BYOD, Desktop, Laptop, Tablet, Thin Client Desk phones, Smart Phones, MFDs
Cloud Services Broker
Security/Privacy
Network Management & Support Centres
Government IM. Directory Services, Certificates
Core Services
Network
One Network, Internet Gateway, VOIP, Fixed LAN, WiFi, 4G/LTE and 3G
Legacy Agency Infrastructure & Apps
Legacy Agency Infrastructure & Apps
Legacy Agency Infrastructure & Apps
Legacy Agency Infrastructure & Apps
Legacy Agency Infrastructure & Apps
Legacy Agency Infrastructure & Apps

Figure 3 - Future ICT Platform

[8] 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.

4.4 Collaborative workspace features/attributes

The following table outlines alignment to the high level architectural themes and principles:

Technical	**Alignment**
As standard as possible	Standard service provider model
Security shift to ID, App, Endpoint	Identity and authorisation
Single LAN WLAN Shared infrastructure	VPN separated with shared services via home network Allows growth in shared products
Energy efficient	Less devices
Agile workspace	Services provided to the building
No building DC	Shared services via GovNet
Mobility centric	Anywhere anytime
Operational	**Alignment**
As-a-service	Easy to add new buildings
Machinery-of-government proof	Does not affect identity
Collaborative	Shared services accessed by GovNet
Self service	The network comes to you
Simple agency integration	Minimal change to agencies current environment and experience
Agency owns security	Agencies own their security posture with no uncontrolled assets in the path
Implementation	**Alignment**
Repeatable for multiple buildings	Architecture is pattern based
Sharing and deduplication	Allows growth in shared products
Network behind the Government gateways	Services accessed via GovNet
Outsourced	Completely
Easily transferred	Standard design and protocols
Competitive	Fast deployment into buildings

Table 5 – Architectural alignment

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.

Specific building features should include the following attributes:

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	Where appropriate, it is proposed that cabling be installed and maintained by the building service provider and patching done by the integrator. 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: • ICT cabling infrastructure policy • ICT cabling infrastructure technical standard.	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. 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, OP6, IP1, IP2, IP4, IP5, IP6.

Components	Attributes	Principle
	A shared pool of desktop PCs 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).	
Video conferencing	A model for the sharing of videoconferencing facilities among 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.
Data centre	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.
Communication rooms [9]	*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.

[9] Note: These are preferred specifications and may not apply to brownfield buildings.

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, Government Wireless Network (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 agency requirements. NB: For greenfield buildings these specifications apply however for refurbished buildings an audit will be required to determine suitability and appropriate trade-offs.	
Wired and wireless 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	There is no material requirement for duplication of networking infrastructure that comes at an unnecessary additional cost to government, in times of exercising fiscal responsibility. Scalability, resiliency, performance, availability and accessibility requirements can all be accommodated with a shared network that government has already invested in. From a whole-of-government perspective, agencies need to be seen to be making effective use of spare capacity before investing in duplicate assets and services.	TP1, TP3, TP8, OP2, OP3, OP4, OP5, OP6, IP1, IP2, IP3, IP4.

Components	Attributes	Principle
	Where practical the connectivity between future office tenancies and the various agency datacentres should be provided by the Queensland Government Network (QGN) managed by CITEC. This is already an extensive network covering Brisbane CBD, Southbank, Fortitude Valley and Spring Hill.	
Meeting rooms and collaboration areas	Includes: • presentation and conferencing facilities • meeting rooms • quiet rooms (for individuals/small meetings) • collaboration areas • digital signage. Large screen monitors, team collaboration infrastructure, digital signage, video conferencing should all be network-connected. Provision for USB ports for laptops, smart phones and tablets should also be deployed by the building service provider.	TP2, TP5, TP8, OP1, OP2, OP3, OP4, OP6, IP1, IP2, IP4, IP5, IP6.
Physical access	Physical access card security and virtual security should be merged where practical by using 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 6 - Future office attributes

4.5 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 a future office tenancy.

‘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 using collaborative services in 1WS and future tenancies will be used to inform revisions of the *Collaborative workspace strategy and principles* (this document).

Figure 4 below depicts the substantial change required to move from the current state to a future as-a-service model:

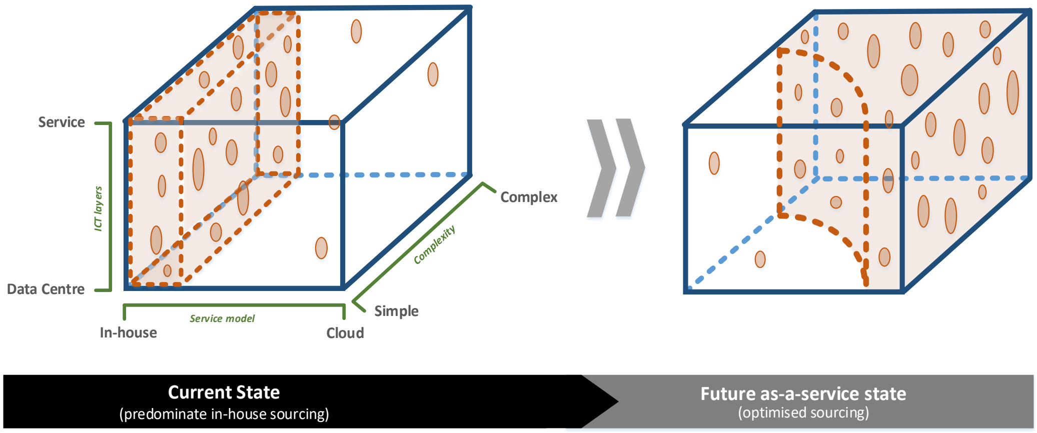


Figure 4 – Stepped change

Figure 5 on page 22 (Services for collaborative workspaces of the future) and the subsequent points summarise the existing and future services required. Detail of the actual solutions, support models and their associated service attributes, key performance indicators (KPIs), service level agreements (SLAs) and operational level agreements (OLAs) is detailed under the current panel arrangements. It is proposed agencies will take up services based on the learnings from the 1WS program in a stepped change, moving toward the target architecture and broader government direction.

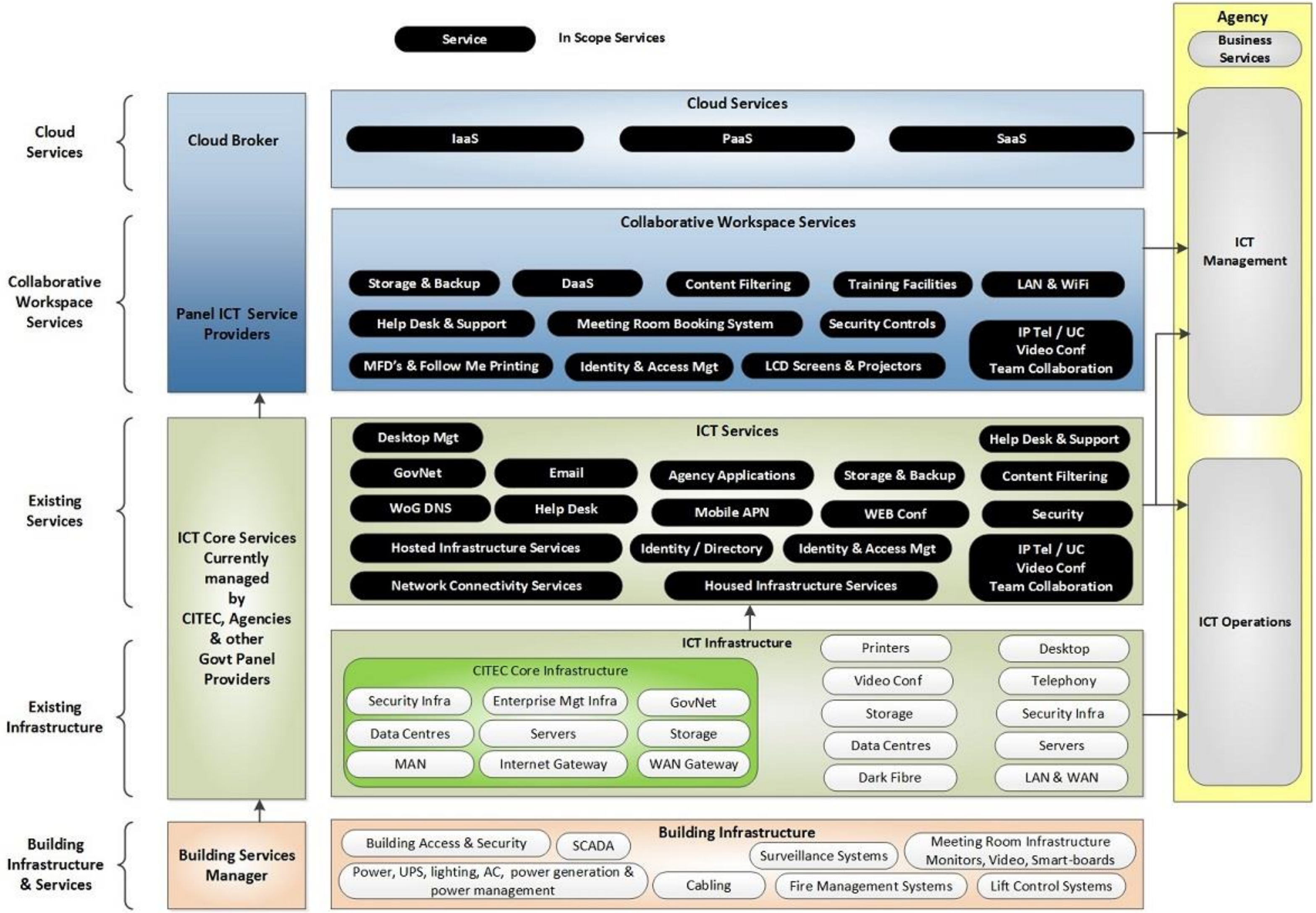


Figure 5 - Services for collaborative workspaces of the future

Underpinning and existing services

The underpinning services environment provides the necessary infrastructure, compute and security components to effectively support the provision and delivery of each service across the specified platforms and locations.

The underpinning service environment is comprised of the following components which support the services environment:

- compute platform
- data centre network infrastructure and telecommunications connectivity
- security controls
- monitoring and reporting
- identity services
- network operations and security operations centres.

Compute platform – Cloud based compute platform to facilitate all host resourcing requirements for each service deliverable.

Data centre network infrastructure - Network infrastructure to enable inter-service connectivity within the service datacentres and customer connectivity to enable customer consumption of each service deliverable. Exceptions include:

(i) Connectivity to the One Government Network and Internet Gateway - The MAN connectivity should provide dual trunk, high-speed (10Gbps) data connections between future office buildings, GovNet, the Government Internet Gateway and the tenant agencies' network core. Agencies will not install their own MAN services to the building.[10] If agencies terminate their own dark fibre or telecommunication services in multi-tenant buildings the following impacts become apparent:

  - government incurs greater capital and recurrent cost of duplicate physical infrastructure at reduced levels of usage efficiency (creating unnecessary spare capacity)
  - no scalability of solution to other buildings – physical fibre links and carrier services would need to be run into all government buildings tenanted by agencies
  - life cycle management and support of network infrastructure (e.g. configuration, fault, incident etc.) becomes more complex
  - machinery-of-government changes become increasingly more expensive.

(ii) Internet security controls and content filtering will remain under agency control where only a small number of staff are in scope. For agencies with full tenancy it is envisaged that security controls may remain under their control or be provisioned as-a-service with the flexibility to use a single common rule-set rather than per agency controls.

[10] In alignment with the Internet Protocol (IPv4) addressing standard and consumption of GovNet services, Queensland Government Network (QGN) connectivity was chosen as the most efficient, cost effective and scalable means of connecting single and multi-tenant buildings to agency data centre infrastructure (including Internet). Currently all agencies have an extranet presence within the QGN core allowing migration into 1WS and other Governments buildings to be accomplished in a seamless manner and without additional expense.

(iii) 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.

Security controls - Security controls to ensure the ongoing security of the service environment as a whole. This includes appropriate security incident and event monitoring to provide visibility of security events as they occur. Current feedback from the agencies suggest that agency security services will remain under their control.

Monitoring and reporting - Appropriate monitoring and reporting functionality has been included to provide reports for both the underpinning services environment and each service that is supported by the underpinning services environment. The included monitoring and reporting capability will be made available to customers of the service through regular standard report that will be generated and distributed to all customers of the service.

Identity federation –The importance of identity has been a common theme in discussions with agencies, analysts and vendors and is reflected in this government and other government cloud strategies. Identity management is a key element in achieving successful service delivery, from a user acceptance and security point of view. 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 common/shared applications and services from existing agency identity stores. See Federated Identity Management Service.

For Option 2 (see section 7, High level deployment options), the following identity related requirements have been identified:

Device authentication and authorisation to support dynamic network VLAN allocation 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 the use of CAC's for print release)
- Resource booking systems
- Guest Wi-Fi access to filtered Internet.

For Option 3 (see section 7, High level 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
- strong two factor authentication for remote access to agency specific hosted virtual desktops.

Network operations centre/security operations centre - Where only a small number of 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 service provider help desk.

Collaborative workspace as-a-service

The expected benefits to the State of establishing these services with an 'as- a-service' construct delivery model are that it will:

- provide the benefits of common technologies to agencies needing to invest in the infrastructure required or take on the risk of operating the infrastructure
- provide a utility reporting and billing model, enabling agencies to scale costs up and down according to need without being constrained by assets
- increase standardisation of IT infrastructure across government and reduce duplication
- result in a single procurement process rather than each individual agency undertaking their own process
- provide a repeatable model for other multi-floor, multi-agency buildings.

Listed below are the core services which should be adopted to provide the benefits of a standardised utility model allowing the State to be fully mobile between buildings without incurring expensive machinery-of-government costs. The proposed optional services are available as catalogue items and should be taken up in alignment with Section 7 - High level deployment options.

Proposed core collaborative workspace ICT service provider services

These services include but are not limited to the following:

1. *Maintenance and support services*

The service provider will provide maintenance and support services as an integral part of the each of the services to the extent that availability and performance are not impacted.

(a) Maintenance services may include (but are not limited to):

  (i) installation and testing of all updates, patches, bug fixes, and software enhancements/improvements as released by manufacturers

  (ii) all patches, updates, bug fixes, enhancements, and/or corrections to the service/s will be installed and implemented within 10 business days of release, unless otherwise agreed by the parties

  (iii) feedback and/or recommendations to the customer, where possible, to reduce the number and frequency of support issues.

(b) The service provider will provide the following support services:

  (i) Operational assistance and technical support to ensure the services comply with the customer's requirements and the contract specifications (including but not limited to):

  - help desk personnel to respond to issues and Incidents within the agreed response and resolution times
  - diagnosis of issues and priority incidents
  - temporary fixes or workarounds within the agreed timeframes.

2. *Wired and wireless network (WWN) service*

The wired and wireless network (WWN) service provides seamless connectivity for occupants to their agency's home networks and lays the foundation for all other services.

The service uses greenfield-constructed network architecture—designed to address modern mobility needs—and is delivered via a single wired and wireless network infrastructure throughout the building

The service provider will:

- Configure the site to provide connectivity to the Queensland Government Network (QGN) as per the customer's requirements including,10GB dual path network links and to provide connectivity to vertical multi-mode fibre and saturation patch horizontal CAT6e cabling which is installed into the site.
- Provision the network in a manner that end users are able to readily 'roam' across floors including in foyers and commercial environments of the site within scope
- Apply 802.1X controls using machine certificates provided by the customer. Together, these enable end users to readily connect to the WWN service without the need for further configuration, whilst still being able to seamlessly and securely access technology, applications and services for which they have been authorised.

- Include DNS forwarding, DHCP relay and NTP services for both building tenants and integrator services
- Accommodate for multiple network functions and multiple levels of segregation within the tenant environments by utilising logical network overlays and VPN technology to deliver required segregation and separation of each service recipient network
- Separate logical network functions can be created on a per agency basis, based on the following use:
  - data networks
  - voice networks
  - utility/support networks.
- Provide quality of service (QoS) features such as per-VLAN and protocol-based prioritisation, as well as flexible QoS assignments, for, granular control
- Provide a wireless network to supplement the wired network and support Layer 3 roaming and collaborative activities. This requires:
  - the provision of 2.5 wireless connections per end user
  - meeting rooms, video conference rooms and team collaboration spaces having greater device density
  - native support for BYOD and traffic.
- Be responsible for all aspects of physical and logical security as nominated in the applicable CSA Cloud Controls Matrix and the TRA controls identified during the service design
- Be capable of scaling by variation to meet the customer's requirements which may include:
  - increases in the number of intended end users and devices
  - increases in the number of floors initially provisioned for the services
  - any other requirements associated with emerging network technologies and functionality that may be required by the customer.

Where only a small number of staff are in scope, logical segregation provisioned via dynamic 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 flat network architecture at a later stage.

Agencies with full 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)[11].

[11] 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')

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.

The QGN acts as a backbone integrating the logical areas and providing users with seamless connectivity to all services.

A guest user will only receive access to the guest wireless network. For guest users, a captive portal will allow self-registration using an email address and mobile phone. Credentials will be sent to the mobile phone for entry into the captive portal. Upon acceptance of the terms and conditions, plus the acceptable use policy, individuals will be permitted access to the guest networks.

The following services are available for guests:

- internet content filtering
- video conferencing and team collaboration
- room booking services (with authentication).

Internet content filtering forms part of the WWN service and is used where sponsored internet access is required to be provided to end users using unmanaged devices, as well as to site guests.

The State (Cyber Security Unit, Queensland Government Chief Information Office (QGCIO)) will provide to the ICT service provider its black and white lists so that the service is enforced in order to provide a duty of care for the user and serves to support the end user's commitment to the government's code of conduct. The service will be provided under an 'acceptable use policy' that will be decided by QGCIO and mutually agreed among all participating agencies for any 'Business as Usual (BAU)' changes as per the ITIL based change management system.

The WWN service is dependent on federated identity management (FIM) service.

Service offering	Benefit
Saturated patching of single PoE Unshielded Twisted Pair (UTP) port per workstation	Ability for any agency to use any available port in the building – no additional port configuration necessary.
Proactive network management	Track assets, monitor performance and optimise throughput and latency.
Seamless network connectivity	Government staff visiting a building can connect back to their agency network using agency issued laptops, causing minimal impact to staff workflows.
Wireless network connectivity	Supplement wired network and support roaming and collaborative activities.

Service offering	Benefit
Guest wireless network with internet connectivity through the Government MAN	Separation of network from registered users while still allowing guests internet access.

Table 7 – WWN service benefits

3. Federated identity management service

Identity management in an IT infrastructure is the cornerstone of successful shared service delivery, from both a user acceptance and a security point of view. An identity management regime that facilitates and improves the user experience by reducing the need to enter credentials more than once to access the same or different applications is likely to be more acceptable than a service that either requires users to remember multiple credentials or to provide the same credential many times.

Federated identity management (FIM) solutions solve the identity dilemma by providing the following benefits:

- single unified view of agencies identities across multiple sources
- ease of management - does not add another management layer
- real-time verification of credentials to ensure that identity store changes are reflected as soon as they are performed.

The service provider will perform and deliver the services in accordance with any industry standard for identity management and identity federation.

Users will not have to remember a new credential in order to access the services. In addition, the current agency identity stores are used as the ‘source of truth’, thereby not changing the way the agencies do their business today.

The FIM service will comprise:

- single sign-on (SSO) authentication from managed devices
- reduced sign-on authentication for remote access via an agency username and a password
- a central and consolidated (aggregated) directory of identities and attribute data, this is commonly called a virtual directory.
- access controls and related security and identity management components configured to provide continuous level of service.

4. Room booking service

This system can be a shared cloud based service or use 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 is preferred.

Dynamic allocation of building wide conference rooms, meeting rooms, quiet rooms, and collaboration areas leads to improved use. 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 a comprehensive set of features in areas of reservation, check-in, personalisation and administration The solution should be 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. HVAC.

Where only a small number of staff are in scope with limited sharing of meeting room and conferencing facilities, agency calendaring system 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 tenancy, a model for booking, sharing and easy identification of meeting room facilities among 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 cloud based application capable of notifying agency calendaring platforms or a resource booking system using the most common government calendaring platforms i.e. Office 365/Exchange.

Employees must be able to consume the services from within a building, from agencies outside of a building and from the internet. An employee can access the service from any mobile or computer that is compatible with the mobile app or is capable of accessing the room booking URL via a web browser.

Service	Benefits
Booking or scheduling of spaces within a building.	Provides granular control over various booking parameters, thereby maximising the use of resources and space Real-time status update and conflict resolution.
Searching for specific room criteria e.g. room size, technology resources, location and in-room services.	
Displaying availability status of rooms and spaces.	
Ability to restrict access and/or visibility of meeting details and attendees for scheduled meetings (e.g. rooms on ministerial floors).	
Ability to disable reservation of selected rooms.	
Placing a room out of service notification when maintenance is required in the room.	
Automatic cancellation of room bookings if organiser does not check in.	

Service	Benefits
Interactive room booking panel features: Assigned to a single room Fixed wall or glass mounting of panel Assigned room reservation management of bookings Display of room and booking information	Supports ad-hoc user collaboration, increasing productivity and promoting a culture of activity-based working.
Mobile app for Apple iOS and Android.	An employee can create a booking from anywhere.
Service accessible from any agency and the internet.	Flexible and robust implementation.

Table 8 – Room booking service benefits

5. Print and imaging service

Agency staff will be able to access copy and secure print and scanning services via shared consolidated MFDs that are able to identify user and consumption. Printing services use the 'follow me printing' concept so that print jobs can be released on any printer and charged as-a-service to the consuming agency.

Ease of use is ensured for the end user as there is only one printer to select when sending a print job, regardless of user's device type, agency, document type or intended print location.

The printing and imaging service relies on:

- Federated identity management service (but not SSO)
- Wired and wireless network service.

Print and imaging services are currently available via a panel arrangement to all agencies.

Service offering	Benefit
Print, copy, scan Printer defaults controlled universally by the PAI service; these defaults include duplex printing, black and white printing and colour printing that separates text from graphics so black ink can be used. Power saving features of MFDs	Simple to deploy and support for end users. One service for all Queensland Government occupants and authorised guests of 1WS.

Service offering	Benefit
Secure Printing Access to specific PAI facilities can be restricted if requested by the customer. Access can be based on user, group or basis of logical location.	The print and imaging service features a document routing engine, and encrypted communications and print queues to ensure security of the PAI service
Agency usage accounting	Provides detailed tracking and billing for agency-specific usage.
Follow-me printing is offered at all MFDs and users must authenticate using a combination of proximity, federated identity, personal identification or supplied or BYO access card.	Ensures ease of use as it requires only one printer to be added to the user's device.
Device monitoring A shared services website will provide searchable information including device name, device type, floor location and map layout.	Tracks print and image assets, monitors consumption and optimises supply and demand via reallocation of assets.
Scalable	Scalable provision of ongoing management and servicing of assets.

Table 9 – Print and imaging service benefits

6. *Service management and help desk*

It is proposed that level 1 help desk support for future office tenancies 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
- agency level 2 ICT helpdesk support teams.

Integration to ServiceNow should be the longer term objective. However, at a minimum the service should provide service desk email integration offering the ability to integrate tickets using email templates and include the following functionality:

- receipt of emails in defined format for ticket creation
- receipt of updates from the client, including comments, work notes, status info, attachments, etc.
- call flow process validation
- bi-annual checks on quality of email exchange.

Proposed **optional** collaborative workspace ICT service provider services include but are not limited to:

7. Video conferencing and team collaboration service

A model for sharing of videoconferencing facilities among 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.

Video conferencing and team collaboration where practical should be standardised across the building, thereby eliminating the need for re-training or learning a new system each time the service is used, irrespective of location.

Video conferencing services with video end points in selected meeting rooms are available for Queensland Government use. The room systems consist of high definition cameras and displays to ensure sharp picture quality. Audio performance is provided by matching speakers and microphones to room configuration.

The service uses industry standard infrastructure and is consistent throughout the building, thereby providing a common interface, features and functionality. This in turn provides benefits such as improved cross-platform collaboration, familiar interfaces irrespective of the room in which the service is being consumed, reduced training needs and increased service uptake. There are three classes of video-enabled meeting or conference room:

- Small 8 person room - Consists of a single high definition camera, two commercial 55’ flat panel displays with dedicated wall mounted speakers and a single ceiling microphone
- Medium 12 person room - Dual camera system with active speaker tracking technology, two commercial 55’ flat panel displays with dedicated wall mounted speakers and dual ceiling microphones
- Large 20 person room - Dual camera system with active speaker tracking technology, two commercial 75’ flat panel displays with dedicated wall mounted speakers and dual ceiling microphones.

Each room type will also consist of a single touch panel for control of the room video conferencing system.

The room systems are managed through a central infrastructure in the cloud platform. Bridging resources are available for ad hoc conferences, or those scheduled via the room booking service. The platform supports dialling the bridging resources or room systems directly via Microsoft Lync or Skype for Business. Agencies outside a building are able to dial the rooms using a unique address. External parties will also be able to dial the video conferencing services.

Team collaboration services will be enabled in certain general and video conferencing enabled rooms. A base and standard team collaboration offering is available as outlined below:

- Base - The base team collaboration system is ideal for (but not limited to) small rooms and huddle spaces and is designed for use in a single room.
- Standard - The standard presentation solution is suitable for any size meeting room or huddle space. The service supports four concurrent presenters on a

single room display, or five presenters using dual room displays. The service is optimised for touch-enabled room displays to enhance interaction. Current technology provides shared content can be presented across two displays, or multiple rooms in a single session.

Service	Benefit
The video conferencing platform adheres to industry standard, resulting in compatibility with the majority of third party conferencing systems. The solution is contactable from external parties using Session Initiation Protocol (SIP) addresses. Agencies and external organisations contact the building room systems using a unique SIP Uniform Resource Identifier (SIP URI). A video conference bridge only receives a unique SIP URI once a booking is confirmed. The video conferencing platform supports Microsoft Lync and Skype for Business clients calling the room systems or bridge. The room video systems are also able to dial Queensland Government employees using Lync or Skype for Business. Video conferencing facilities will be available for guests to call if included in scheduled or ad hoc call. Options are available to dedicate a bridge number for internet parties or guests to dial, or the room systems directly. Services available within video enabled rooms: • High definition video conferencing • Camera and displays as per the selected room classification • IP phone with handset • Audio telephony services also available from the video system.	Evergreen technology promoting collaboration between and within agencies and the State. Tight integration exists between the VCTC and the room booking service to ensure conferencing resources are scheduled when multiple video participants exist within a meeting.
Services available within general meeting rooms without video conferencing: • IP phone with handset • IP conference phone.	Promotes collaboration between and within agencies and the State.

Service	Benefit
Team collaboration systems allow devices to stream content simultaneously through a wireless to a display or as the presentation source in a video conference. The presentation of content to the team collaboration services is intuitive and easy to initiate. Native wireless presentation from all Apple iOS devices (i.e. iPhone, iPad, iPod and OS X) and Windows computers is supported. Apps and software to enable content sharing are available for most popular devices. Sharing of a collaboration session where single or multiple participants are displaying content on a display is available across multiple rooms and floors via the high-end team collaboration service. A participant is also able to present content from a device using the physical HDMI or DisplayPort connection on the table. Sharing using the team collaboration services will be available through the guest wireless networks for non-government employees to use. Services available within a team collaboration space: • High definition commercial-grade display • Choice of base or standard collaboration service • Speakers for audio playback • Touch-enabled displays are optional for all team collaboration services.	
Team collaboration capability and enabling technologies, e.g. streaming multiple devices on a large screen.	
Centralised contact directory for consistency across all rooms.	Easier to manage and maintain.
Service may include a full time on-site level 2 Engineer for video conferencing management.	Reduced response time for support requests, increasing efficiency.

Table 10 – VCTC service benefits

8. Voice over internet protocol (VOIP) service

To avoid the need for agencies to provide their own telephony services in shared areas there will be a fixed IP telephony service offering in all meeting rooms and collaboration space for agencies that wish to use 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 will use 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.

9. User workspace/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 centralised, 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 C – Myth busting DaaS) for further detail.

Remote desktop virtualisation can also be provided through 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.

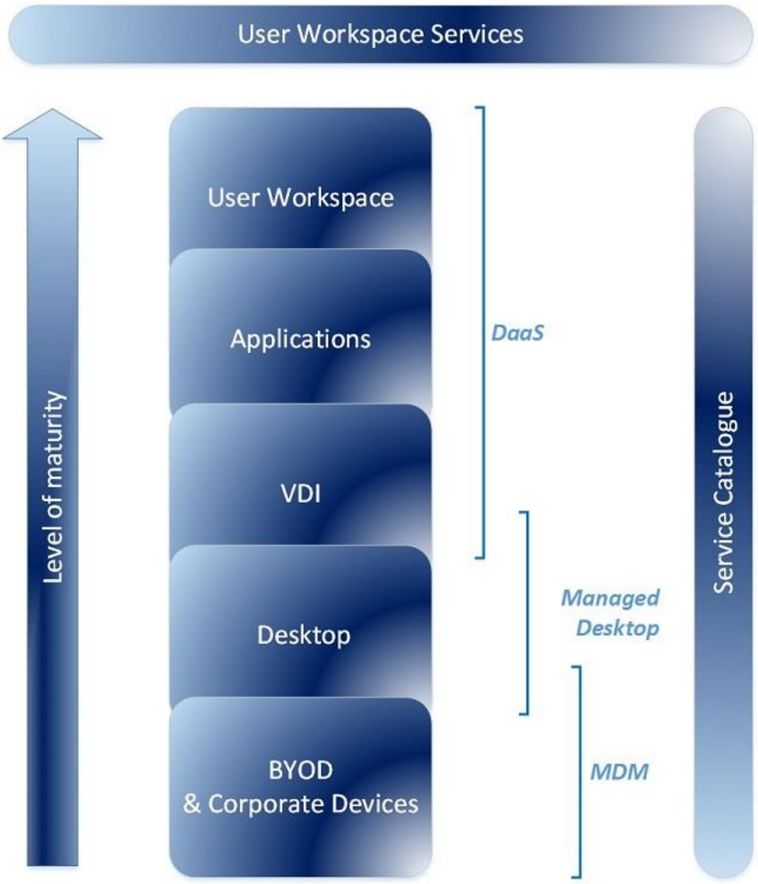


Figure 6 – User workspace services

Where only a small number of 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 SOE environments such as Windows 7 and Windows 10
- 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.

Optional user workspace services include but are not limited to the following:

- *SOE Design or Agency provided Template* – Agencies can use their existing SOE or they can use a provided template. Should an agency use their existing SOE a transition service will be required to suite the VDI environment.
- *Application Packaging* – Packaging services can be managed via a cloud based workflow tool to ensure the process is tracked from the package request to the UAT acceptance. Pre-packaged offerings will be made available via the service catalogue.
- *Virtual desktops and traditional desktops* – A wide range of options should be available around end user devices being provisioned with access to the solution.
- *Managed desktops* – As an option a distribution server can apply SOE images to devices as they are deployed for use. This service can also be used for delivering applications, updates, patches and security fixes.
- *Antivirus* – Agencies have various options to secure the desktops from virus threats. Should agencies have an existing investment they can choose to extend that service to the virtual desktops. Should agencies want to use a new product they can select this from the catalogue.
- *Government issued tablets and mobile devices using mobile device management (MDM)* – agencies will have a choice to use 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.
- *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.

- *Software asset management and software rationalisation (SAM)* – SAM management is a critical component of any agencies IT and business strategy. A number of optional SAM services can be offered. By identifying unused applications and remaining deployments against the licence entitlement the software rationalisation process can produce one of the most substantial returns on investment as part of a complete SAM service.
- *Transition services* – Onsite support will be available via the catalogue and can range from simple break fix call outs to a fully outsources service.
- *End of life services* – This optional service will manage the disposal/end of lease process for all IT asset types.

Exclusions from the user workspace service:

- agencies are responsible for all Windows Desktop Operating system licencing
- agencies are responsible for all application licencing.

10. Service catalogues and 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:

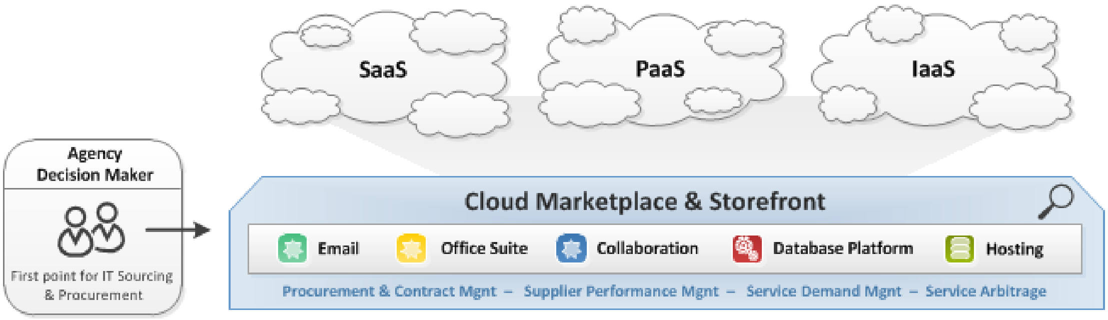

SaaS
PaaS
IaaS
Agency Decision Maker
First point for IT Sourcing & Procurement
Cloud Marketplace & Storefront
Email
Office Suite
Collaboration
Database Platform
Hosting
Procurement & Contract Mgnt – Supplier Performance Mgnt – Service Demand Mgnt – Service Arbitrage

Figure 7 – Government AppStore

4.6 Integration

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	Panel 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. Note: Learnings from 1WS and industry indicate early engagement is essential).
Data cabling	✓	✓			Saturation patching of all outlets will belong to the LAN service provider. Note: For refurbished buildings an audit will be required to determine suitability and appropriate trade-offs. Physical security controls may need to be implemented for some agencies
Meeting room booking system		✓			Integration with calendaring on different platforms will require federation of resource presence information. To simplify integration and to leverage economies of scale and it is recommended that a standardised platform be used across all buildings. NB: learnings from 1WS should be referenced.
Monitors/ displays, smart boards and projectors		✓			Smart boards and projectors should be replaced by wide screen monitors and glass walls that can be photographed. If so, these will be provided by the panel 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/codecs will be managed by the Panel ICT SP. Tight integration will be required between UC service providers to ensure interoperable services.
Printing and imaging		✓			Follow me printing and imaging will be delivered as-a-service from current panel arrangements 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 provided as-a-service by the Panel ICT SP. Connectivity to course material will be set-up by the trainer via guest Internet access or VPN.
Internet filtering			✓	✓	As-a-service internet filtering for the guest network will be multi-tenanted. 'Black listing and white listing' will need to be set up between QGCIO and the service provider. In the first instance most agencies have indicated a preference to maintain their own security and web filtering controls for their home network, however guest access for the building will still require internet filtering.
Local area network		✓			LAN and Wi-Fi services will be offered by the Panel 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 Panel ICT SP will require tight integration.
Internet, GovNet and whole-of-government DNS			✓		To be provided as-a-service using CITEC Network Connectivity Services. Contestability may require an alternate solution. Transition business cases should capture this.
Help desk	✓	✓	✓	✓	Agencies will provide level 1 help desk facilities. A level 2 help desk will be provided by the Panel ICT SP. Business processes will be required for hand off, be it to an agency help desk or service provider help desk.

Table 11 - Service ownership

Agencies should acknowledge that the 1WS architecture and associated panel arrangement are in place and that much of the backend integration work is now completed. As such integration work is repeatable/minimal for future tenancies should the collaborative workspace model be adopted.

The following components need to be considered:

- implementation of a federated identity capability across participating agencies
- implementation of Exchange Federation
- implementation of non-perimeter security approach with appropriate controls identified by a formal threat and risk assessment (TRA).

For further detail regarding the proposed uptake of services see section 7: High level deployment options.

4.7 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.

5 Current state

5.1 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 should be addressed in agency migration plans.

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

5.2 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 single and multi-agency office buildings.

5.3 Changing demands

Just like the advent of Client Server in the early 1990s 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.

5.4 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 not ready to take advantage of whole-of-government initiatives such as; as-a-service, cloud, internet, mobile, social	As-a-service, 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 some organisations napping while they pursue a more traditional approach. Only the most alert organisations are fully cloud and mobile ready – and most of these are greenfield. Very few governments have been agile enough to take advantage of this new paradigm in a multi-tenanted whole of government environment. 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 and in many cases contracts are renewed without market sounding.
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. • 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 shared/central initiative is a significant variable in the success of the initiative. (1WS is one such example of a successful initiative but ongoing take-up of similar constructs is struggling, particularly in brownfield environments)

Barriers to shifting ICT service paradigm	
Legacy applications	Client Server is the dominant desktop architecture within the Queensland Government, with Microsoft Windows being the dominant desktop OS, however the uptake of Office 365 is growing rapidly. By its nature client server architecture constrains how people access the government's applications. This 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 or use Microsoft Direct Access in order to gain remote access to their applications. These disparate workarounds are complex and expensive to scale up. While this is an impediment to the Government's 'Cloud First' and 'any-where, any-time, any-device' approach and ever increasing mobile workforce, it is the only viable short to medium term solution for connectivity to legacy applications. NB: The 1WS and Terrica Place implementations have overcome this impediment however take-up of this repeatable architectural building block is slow.

Table 12 - Barriers to shifting ICT service paradigm

5.5 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.

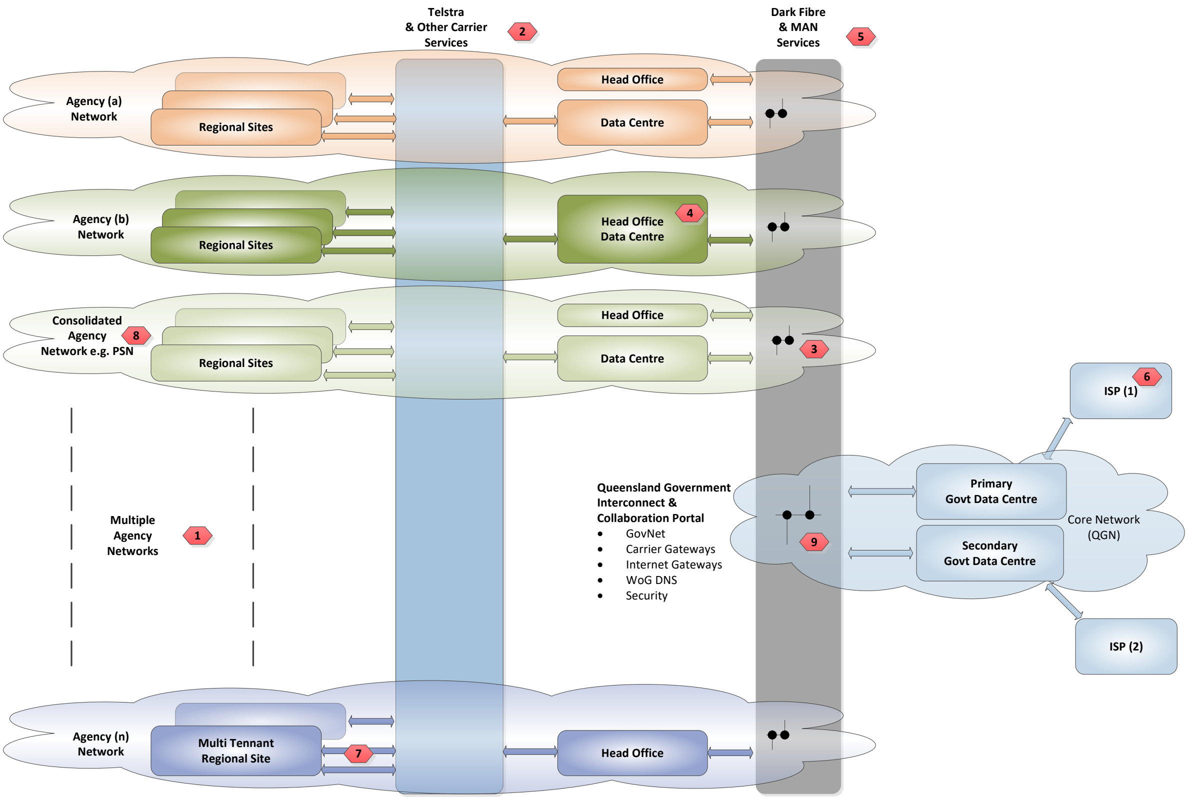


Figure 8 - Current state network visualisation

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

#	Issue	Problem Description
1	Multiple 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.

#	Issue	Problem Description
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.
4	Duplicated facilities and services	There is extensive duplication of environments, carrier gateways, vendor arrangements, support contracts, network management, help-desk services and security services across agencies.
5	Duplication of dark fiber services	An abundant and cost effective supply of dark fiber services in the CBD has resulted in a large amount of duplicated services, underuse of available government capacity and poor usage 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	With the exception of 1WS, extensive duplication of access circuits into multi-tenanted buildings results in poor usage of available capacity, duplication and higher operating costs.
8	1WS and Cluster agency consolidation	Agency centric investment reduces duplication of environments and infrastructure for 1WS and the cluster agencies only. Lack of standardised technologies and processes, constrain seamless service delivery across whole-of-government.
9	Underutilised core (GovNet/QGN) infrastructure	Underutilisation of existing physical infrastructure and available capacity results in duplication, higher operating costs and poor utilisation of assets.

Table 13 - Current State network issues

6 Dependencies

6.1 The 1WS as-a-service model

The 1WS precinct has proven to be a catalyst for transformational change in the way ICT services will be delivered and consumed by tenanted agencies.

It removes the current siloed state of agency ICT environments, where commodity ICT infrastructure and services are duplicated within each agency, as well as proliferating a high level of technology diversity that inhibits the ability to share information and leverage economies of scale.

The adaptive ICT technologies and services being deployed will offer tenants a greater level of mobility, flexibility and productivity than would otherwise be achievable if an agency siloed approach to ICT service delivery were taken.

Completion of service procurement leading to establishment of a panel of suitable Prime ICT Service integrators for future single and multi-tenant buildings was completed in September 2015. Dimension Data and Telstra will provide Core Services via the panel arrangement.

Core Services include:

- wired and wireless networking
- printing and imaging
- video conferencing and team collaboration
- room booking system
- appropriate underpinning security and identity management
- service management.

There has been strong business leadership from Directors-General and chief information officers to ensure migrating agencies adopt the new model and this will need to continue for all new and refurbished buildings going forward.

6.2 Project dependencies

In line with the 1WS Program the One Network initiative and the governments ICT reforms, the *Collaborative workspace strategy and principles* 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 possible dependencies for the Collaborative Workspace 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. It is proposed that LAN connectivity in a building would 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 future office tenancies.
Sharing common resources	Sharing of networking, 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

Dependencies	Description
	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 future office tenancies includes a single logical network. Traditional perimeter security boundaries that agencies have implemented between themselves and other agency networks will not exist. While 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 and backend integration	The One Network initiative (anywhere, anytime, and any device) components may occur in parallel or independently however it is advised that the One Network discussion paper be reviewed in addition to this document. Agencies should acknowledge that the 1WS architecture building blocks and much of the backend integration work is now complete or at least repeatable. The following components should to be considered: • implementation of a federated identity capability across participating agencies. • implementation of non-perimeter security approach with appropriate controls identified by a formal threat and risk assessment (TRA).
Government Interconnect and Internet Gateway	Use of GovNet (QGN) to achieve cross agency collaboration, the Metropolitan Area Network and the Government Data Centres are core to this architectural model. To use another service provider would be disruptive and very costly to implement.
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 developed for collaborative workspace environments is both suitable and scalable for whole-of-government.
Procurement	The Government's ICT audit, the Cloud First Strategy and the 1WS SOA are driving transformational change in the way ICT services will be delivered and consumed in Queensland Government. This change aligns the approach (to collaborative workspace environments) outlined in this document. As an example, the government may determine that services such as

Dependencies	Description
	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 14 - Dependencies

7 High level deployment options

7.1 Occupancy

ICT planning activities remain fluid for occupancy into future office buildings in particular:

- the number of agencies requiring occupancy in future buildings will change
- some tenancies will be single agency, some multi-tenant and some short term
- the floor layout design will change significantly across buildings and across floors
- the desired work style/practices of some agencies varies from the desired concept.

All of these variables plus any future machinery-of-government changes need to be considered as part of the ICT strategy and principles for the building. This section highlights several high-level deployment options that should be considered for collaborative workspace design.

In considering the options outlined below, it is important that agencies remain mindful of the fact that the government has a stated intention for future building tenancies.

> *'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'.*

This vision should continue to guide thinking, and any approach that does not deliver on this intention should not be considered.

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

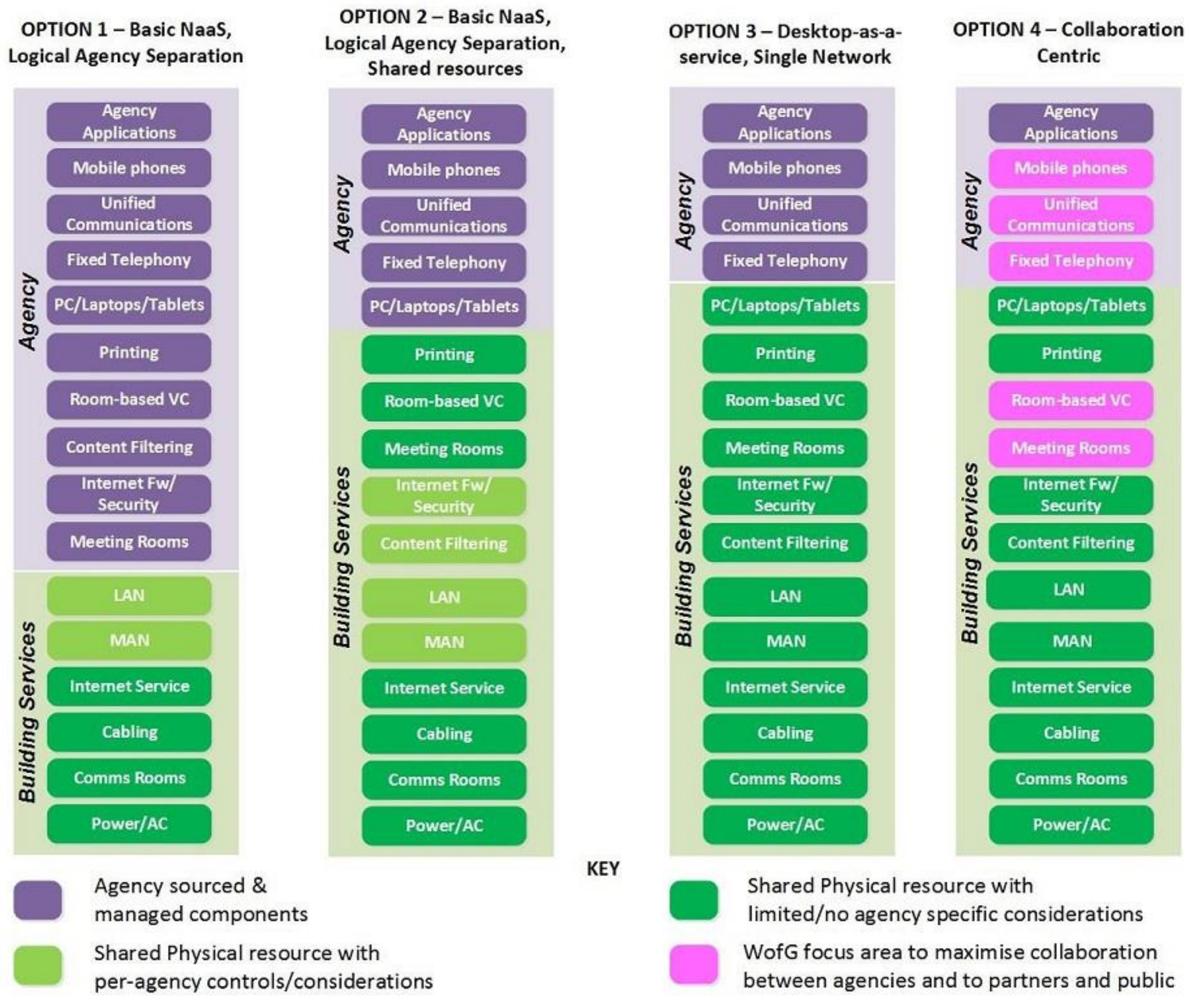


Figure 9 - Four primary deployment options for collaborative workspaces.

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

This option is the minimum baseline target for collaborative workspaces for the future. Previous agency co-location efforts have typically resulted in per-agency network infrastructure with limited sharing and significant duplication. At a minimum the aim 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 the new premises.

7.3 Option 2 – Network-as-a-service 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, video conferencing, team collaboration) will be shared common services. Digital signage, internet security controls and content filtering will be provisioned as-a-service with per-agency controls/considerations.

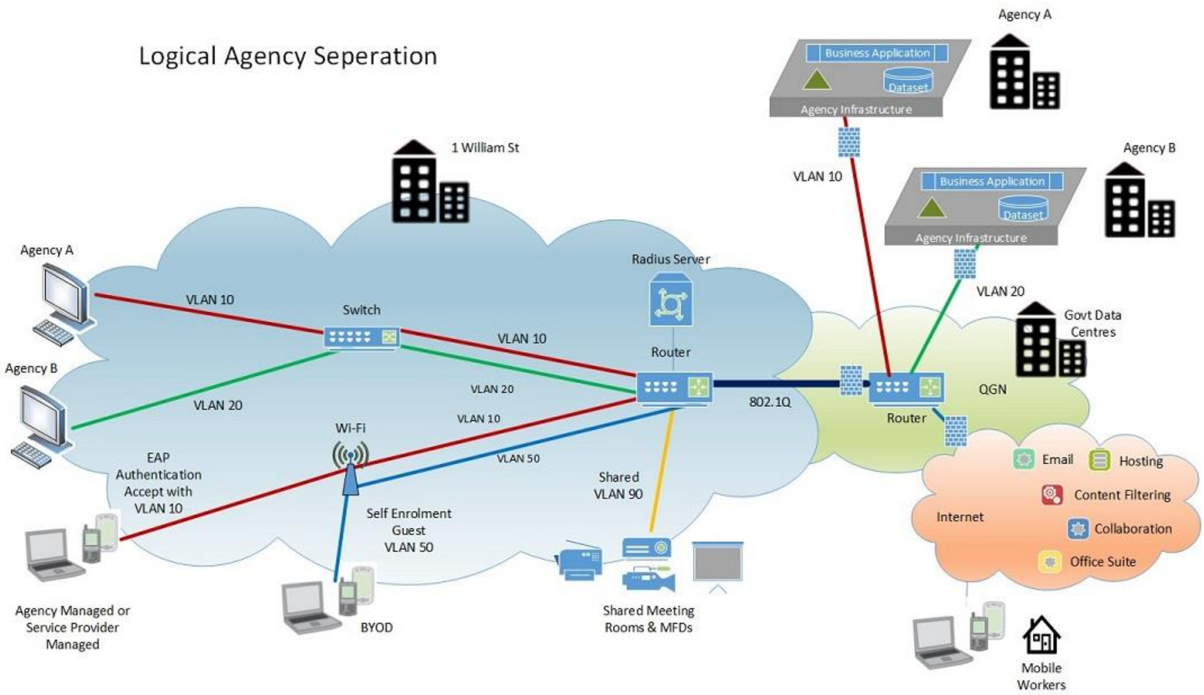


Figure 10 – Logical agency separation

7.4 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 and 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 future buildings.

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 the ICT Panel providers 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.

Print and imaging, room based video conferencing and team collaboration, 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.

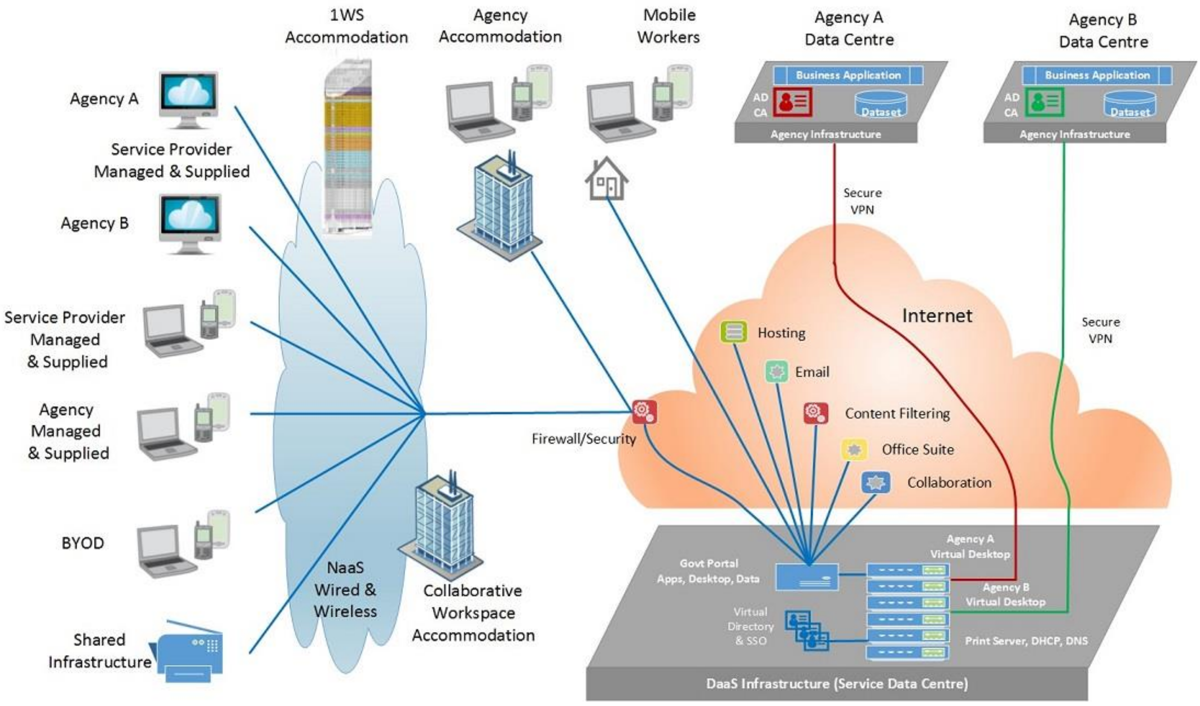


Figure 11 – User workspace/DaaS + shared network

7.5 Option 4 – Collaboration centric

In alignment with the Queensland Governments objectives for collaborative workspaces, ICT environments needs to facilitate high levels of interpersonal communication for teams and project groups. This option has more broad-reaching considerations than that of a single building. It would need to consider whole-of-government approach to collaboration. To achieve this the model, the building 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 and team collaboration). 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.

7.6 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 tenancy

Agencies with full occupancy should strongly consider Option 3-4 as their target. 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 a large amount or 100% of their staff to the new building 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 new building 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

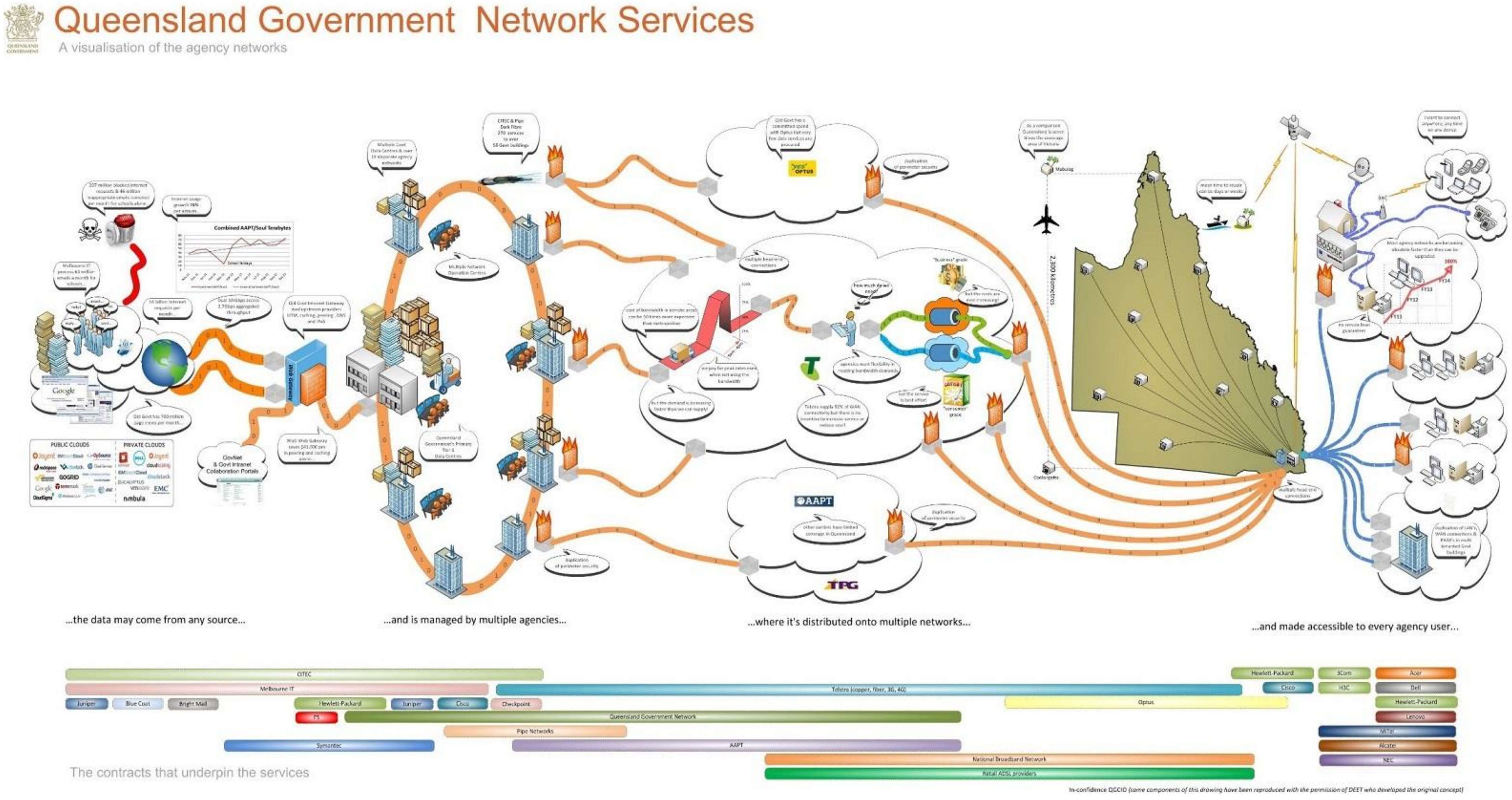
Agencies other than those indicated above may consider Options 3-4 if they believe they are good fit for their requirements. Option 2, however may be the more realistic goal for these agencies in the first instance. Option 1 is a potential fall-back option. Agencies may also wish to consider an ‘Option 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. 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 these 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 User workspace/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 user's/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


Queensland Government Network Services
A visualisation of the agency networks
207 million blocked internet requests & 46 million inappropriate emails removed per month for schools alone...
Internet usage growth 78% per annum...
Combined AAPT/Soul Terabytes
School holidays
Melbourne IT process 63 million emails a month for schools...
16 billion internet requests per month...
Dual 10 Gbps access 2.7Gbps aggregated throughput
Qld Govt Internet Gateway dual upstream providers UTM, caching, peering, DNS and IPv6
Google
Qld Govt has 700 million page views per month...
PUBLIC CLOUDS
PRIVATE CLOUDS
GOGRID
EUCALYPTUS
vmware
EMC
nimbula
Web Gateway
GovNet & Govt Intranet Collaboration Portals
Web Gateway saves $41,000 pm in peering and caching alone...
Multiple Govt Data Centres & over 19 disparate agency networks
CITEC & Pipe Dark Fibre 270 services to over 58 Govt buildings
Multiple Network Operation Centres
Queensland Government's Primary Tier 3 Data Centres
duplication of perimeter security
Qld Govt has a committed spend with Optus but very few data services are procured
"yes" OPTUS
duplication of perimeter security
multiple head-end connections
cost of bandwidth in remote areas can be 50 times more expensive than metropolitan
we pay for peak rates even when not using the bandwidth
but the demand is increasing faster than we can supply!
how much do we need?
agencies want flexibility in meeting bandwidth demands
Telstra supply 93% of WAN connectivity but there is no incentive to increase service or reduce cost!
"business" grade
but the costs are ever increasing!
but the service is best effort
"consumer" grade
AAPT
other carriers have limited coverage in Queensland
duplication of perimeter security
TPG
As a comparison Queensland is seven times the coverage area of Victoria
Mabuiag
2,300 kilometres
Coolangatta
mean time to repair can be days or weeks
multiple head-end connections
I want to connect anywhere, any time on any device
Most agency networks are becoming obsolete faster than they can be upgraded
100%
FY14
FY13
FY12
FY11
no service level guarantees
duplication of LAN's, WAN connections & PABX's in multi tenanted Govt buildings
...the data may come from any source...
...and is managed by multiple agencies...
...where it's distributed onto multiple networks...
...and made accessible to every agency user...
CITEC
Melbourne IT
Juniper
Blue Coat
Bright Mail
Hewlett-Packard
Juniper
Cisco
Checkpoint
F5
Queensland Government Network
Pipe Networks
Symantec
AAPT
Telstra (copper, fiber, 3G, 4G)
Optus
National Broadband Network
Retail ADSL providers
Hewlett-Packard
Cisco
3Com
H3C
Acer
Dell
Hewlett-Packard
Lenovo
Mitel
Alcatel
NEC
The contracts that underpin the services
In-confidence QGCIO (some components of this drawing have been reproduced with the permission of DEET who developed the original concept)

Appendix B – Unified communications and collaboration

Enabling improved collaboration

Consideration needs to be given to the unified communication and collaboration (UCC) solutions/approach adopted by agencies.

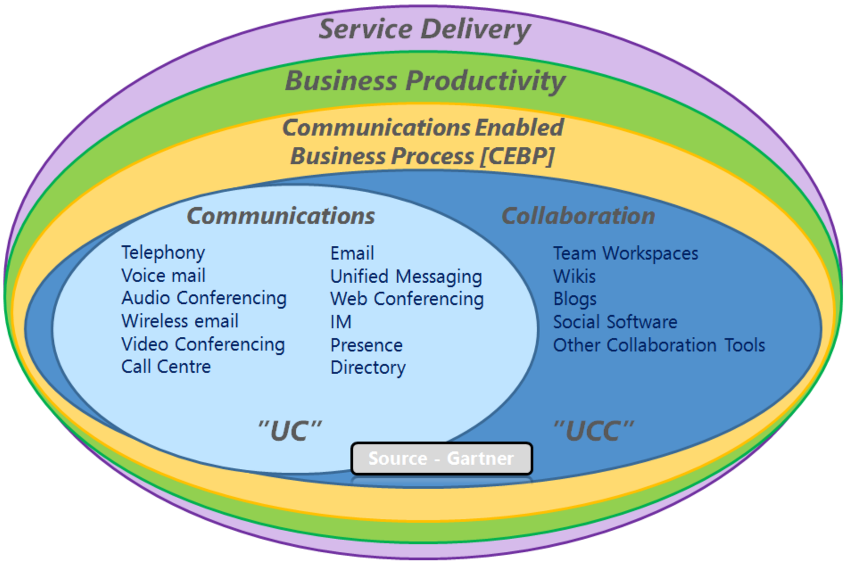
What is UCC?

(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.

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, information sharing 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, engage in 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 culture change required to implement this new way of working should not be underestimated and a robust change program should be undertaken to prepare staff for this transition.

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 but not be limited to 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 future office initiative

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

The following relate to the Collaborative Workspace and future office initiatives:

- The state vision/objective for the future buildings is to be modern, innovative and designed for a creative, harmonious and adaptable workplace. The intention is that they be 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-refurbished) areas of the agency will be critical.

Appendix C – Myth busting Desktop-as-a-service

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 organisations 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 datacentre. With DaaS, you can optimise performance by partnering with a proven cloud-hosted desktop provider. That way you can take advantage of global data centres 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 changed 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 usage 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 organisation 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.