ALGIM INFO

Association of Local Government Information Management Inc

Mobility in Local Government

2012 and Beyond

Author	Damien Toman Director and Independent Consultant ICT Training & Consulting International Ltd icttci.webs.com
Sponsor	ALGIM
Date	November 2012

CONTENTS

Please Note:

1. Any views expressed in this document are the views of the author and not necessarily the views of ALGIM, ALGIM executives or members.

2. This document is designed to be viewed on a Tablet or Personal Computer rather than for printing (diagrams extend close to the edge of the page for maximum legibility).

3. Please email damien.toman@xtra.co.nz with corrections or suggestions for updates. At least one update is planned.

4. Any updates will be available on the author's web site,
   Downloads section: http://icttci.webs.com/
   and on the ALGIM web site.

1. Introduction

All ALGIM members, i.e. all Local Government organisations in New Zealand, were called, to enquire about their current and planned mobile systems environments. Around half made the short time requested available, to discuss their status and plans. Some others responded with information after an email request was sent to all organisations. Their valuable input to this document is appreciated.

Laptops have been the standard in-the-field application access tools for many years. In recent times, Smartphones and Tablets have presented other attractive options, with Global Positioning Systems, long battery life, intuitive touch-screen interfaces, built-in cameras and instant-on capabilities. As more consumers invest in these devices for their own use, organisations are under increasing pressure to allow access to business systems through these devices. Users realise they can be more productive. They typically do not want to carry duplicated business and personal devices. New Zealand is far from the forefront in this trend, but some Local Government organisations are already embracing the opportunities that these new tools offer. They are adapting their networks, security solutions and application access systems, to take advantage of these developments, improve productivity, while satisfying staff preferences and demands. This trend will continue, it will accelerate, and it will become increasingly important for all Local Government organisations and their employees. Even the House of Lords, in England, which may not be seen as one of the most go-ahead organisations, has approved the use of iPads and other Tablets. The USA Government also supports Bring Your Own Device (BYOD) and has issued a toolkit to help other agencies.

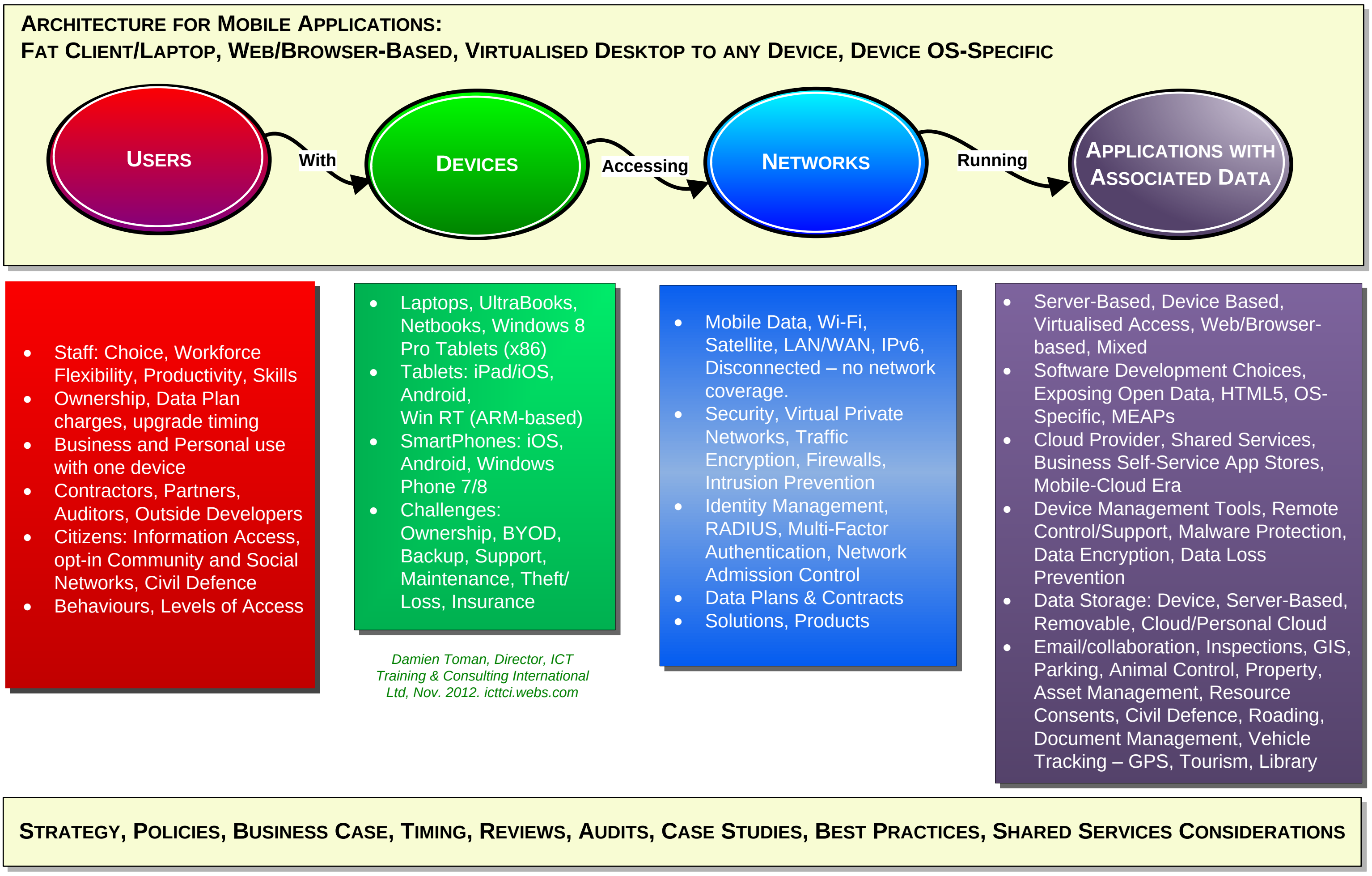
This White Paper aims to help all Local Government organisations in New Zealand understand what is happening and provide some examples. It will help explain the scope and solution options available. It will also provide some sample documentation, and solutions to consider, that can help Local Government organisations gain traction along this accelerating growth path.

As we will discover in this paper, these new devices can not only provide access to existing web-based applications through browsers, but Tablets can also provide full desktop access to all existing applications through Virtualisation solutions available today, over both Mobile Data networks and Wireless Local-Area-Networks (Wi-Fi). Some solution providers also offer applications that are designed specifically for these latest devices, providing off-line, non-connected, access to sub-sets of downloaded data, while in the field - various inspections forms, animal control and ownership, being examples. The latest web development environment, HTML5, also offers the opportunity to be device-independent for many future applications, and supports offline/disconnected use.

This paper will investigate all of these interesting developments, the associated challenges, the risks, the policies and documentation that might be required to support progress down these inevitable paths to a more productive and user-satisfying way to work. It explores additional down-stream options for work/life balance choices and cost reductions, while also providing more comprehensive Disaster Recovery, Business Continuity and Civil Defence responses.

2. Overview of Key Consideration Areas for Mobility in Local Government

This diagrammatic table presents an overview of key considerations for implementing Mobility solutions in Local Government organisations.



ARCHITECTURE FOR MOBILE APPLICATIONS:
FAT CLIENT/LAPTOP, WEB/BROWSER-BASED, VIRTUALISED DESKTOP TO ANY DEVICE, DEVICE OS-SPECIFIC

- Staff: Choice, Workforce Flexibility, Productivity, Skills
- Ownership, Data Plan charges, upgrade timing
- Business and Personal use with one device
- Contractors, Partners, Auditors, Outside Developers
- Citizens: Information Access, opt-in Community and Social Networks, Civil Defence
- Behaviours, Levels of Access

- Laptops, UltraBooks, Netbooks, Windows 8 Pro Tablets (x86)
- Tablets: iPad/iOS, Android, Win RT (ARM-based)
- SmartPhones: iOS, Android, Windows Phone 7/8
- Challenges: Ownership, BYOD, Backup, Support, Maintenance, Theft/ Loss, Insurance

Damien Toman, Director, ICT Training & Consulting International Ltd, Nov. 2012. icttci.webs.com

- Mobile Data, Wi-Fi, Satellite, LAN/WAN, IPv6, Disconnected – no network coverage.
- Security, Virtual Private Networks, Traffic Encryption, Firewalls, Intrusion Prevention
- Identity Management, RADIUS, Multi-Factor Authentication, Network Admission Control
- Data Plans & Contracts
- Solutions, Products

- Server-Based, Device Based, Virtualised Access, Web/Browser-based, Mixed
- Software Development Choices, Exposing Open Data, HTML5, OS-Specific, MEAPs
- Cloud Provider, Shared Services, Business Self-Service App Stores, Mobile-Cloud Era
- Device Management Tools, Remote Control/Support, Malware Protection, Data Encryption, Data Loss Prevention
- Data Storage: Device, Server-Based, Removable, Cloud/Personal Cloud
- Email/collaboration, Inspections, GIS, Parking, Animal Control, Property, Asset Management, Resource Consents, Civil Defence, Roading, Document Management, Vehicle Tracking – GPS, Tourism, Library

STRATEGY, POLICIES, BUSINESS CASE, TIMING, REVIEWS, AUDITS, CASE STUDIES, BEST PRACTICES, SHARED SERVICES CONSIDERATIONS

We will look at these areas in more detail, their specific challenges, and solution options. We will look at where some Local Government organisations are today and where some are aiming. We will also look at supporting policies and solution options.

Clearly, providing flexible mobile access to business applications will require continuous development of the organisation’s Mobility Strategy and end-to-end solutions. It will require evaluation of the potential business impact of mobility projects, the security requirements, the management tools and development environment for information systems.

> *“As mobile device usage continues to grow, support for some type of Bring-Your-Own-Device (BYOD) policy or approach will be mandatory for most organizations across Asia Pacific.” (End User Computing Trends In Asia Pacific In 2012 And 2013. From Desktop Virtualization, To User Experience Management) Michael Barnes Forrester Research, Inc.*

3. Strategy for Mobility

Local Government organisations today are looking to deliver more efficient and flexible working environments, with enhanced mobile solutions, that suit the changing needs of the business and also improve employee satisfaction and productivity.

When planning for change, and reviewing the organisations mobility strategy, here are some questions for consideration:

- How can mobile access to systems, in the field, improve productivity, and reduce transcription errors, avoiding the two-staged approach of paper-based forms and later data input?

  Need to consider Tablets, connected vs. disconnect use, web-based access, Virtual Desktop Access, developing specific front-end apps for Smartphones or Tablets, iOS vs. Android vs. Windows strategies or choices.

- What impact will providing field access to GIS systems, mapping, property systems, health inspections, asset management, animal control, roading management, tree management, civil defence, emergency services and document management have on the organisation's ability to serve the community better?

  In the following section we explore an approach to gaining user views, requirements and preferences. Research suggests that it opens up opportunities for innovation and smarter ways of working.

- How will employees feel if they are provided with smart new devices for business systems access in the field, allowing personal use of the device and providing a more flexible and productive working environment?

  In later sections we quote feedback on employee, HR and organisation views on positive experiences.

- How might your teams and business partners communicate better, and be more efficient, with sophisticated real-time collaboration tools?

  New Plymouth District Council has already implemented Microsoft Lync to address this requirement – Case Study later.

- Can investments in these areas save costs in the medium term? Long term?

  Interesting views expressed later. It often depends on existing security infrastructure and application delivery architecture in place (e.g. existing Virtual Desktop Infrastructure if that is the chosen approach. Putting such solutions in place from scratch can require significant investment).

- Is there a clear understanding of where the priorities should be when moving to a more mobile systems environment?

The answers will come from the investigations of easy opportunities (like email and Calendar access initially) and user feedback from assessments on application priorities.

- Is it clear what roles would benefit most and gain the greatest productivity benefits from a more mobile approach?

  As previous.

- Does the management team have a clear vision of where the organisation is going with mobility, the projects that will take it there and the timeframe for delivery?

  Not the starting point. The vision should come after the analysis, investigations and user feedback.

- Are the resources and funding available to investigate, plan and deliver new solutions?

  Need to consider partners, suppliers, estimated savings and benefits, project management requirements.

- Does the organisation have a clear understanding of the risks presented; the policy changes required; the security solutions necessary and the ability to audit, maintain and deliver new mobile capability?

  See overview of Information Security Lifecycle Review Process for Mobility in later section with 6 steps including Risk Assessment. The Western Bay of Plenty District Council has developed a spreadsheet to cover high level risks.

- Do employees want to choose and own their own devices?

  Predicted to be the way business is going. Details later in this document. Queenstown Lakes District Council already going down this path.

- What are the Human Resource team's views on this?

  Typically HR is keen to go down this path to help retain and attract key personnel.

- Is the ICT team ready to deliver new mobile solutions?

  Partners and Service Providers will often be brought in to assist with design and implementation of solutions. Current project pipeline will affect timing.

- Are there new Legal issues to consider?

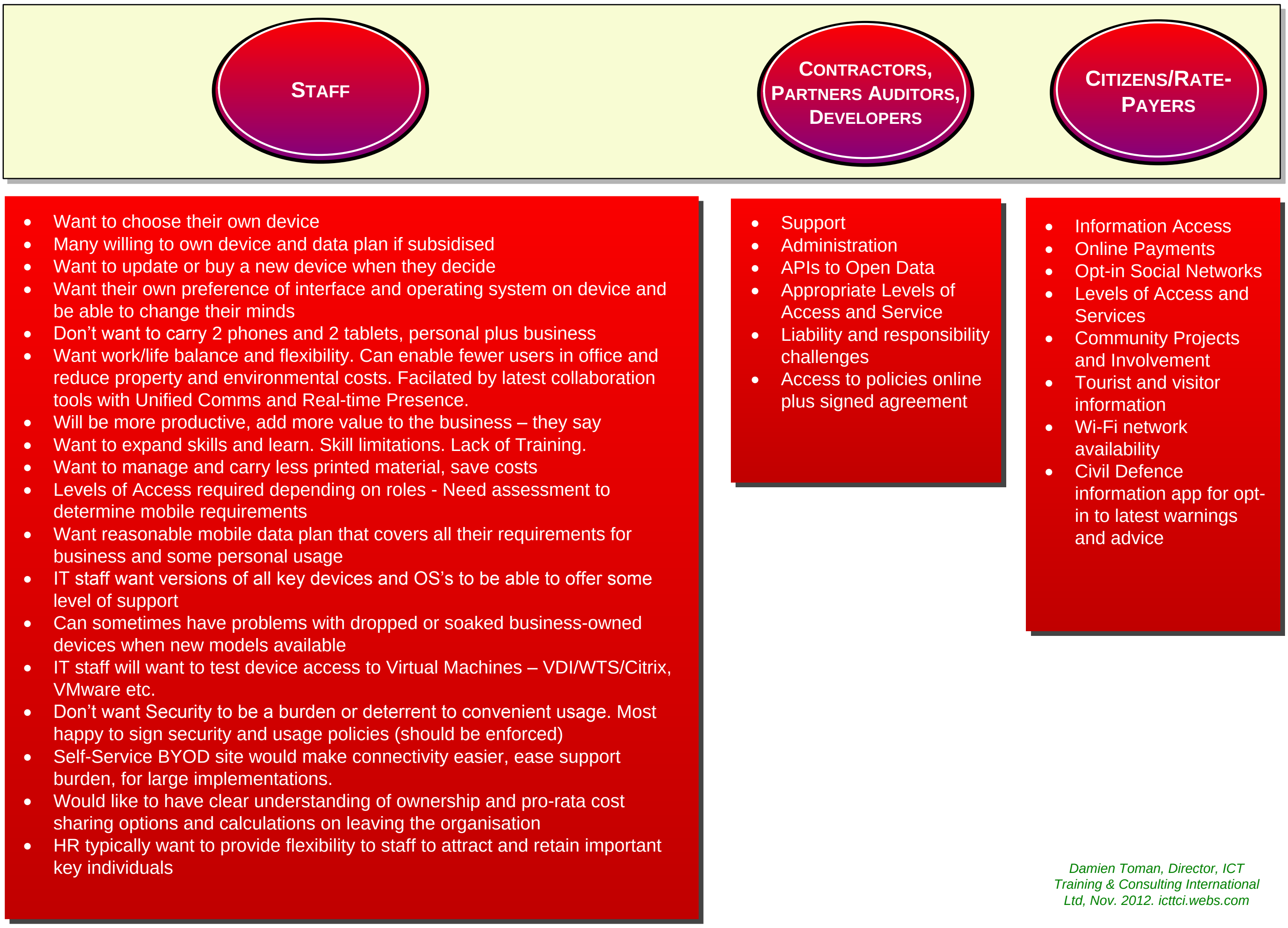
  Very important that the Legal team or advisors are involved especially when defining policies.

Each organisation will have its own answers, to these and many other questions, when looking at mobility strategy.

In the following sections, this paper will explore many areas that need to be looked at in detail. It will also provide some examples of approaches taken by Local Government organisations that are already on this journey. It will provide some suggestions, and guidance, on approaching the challenges and it will look at solution options available.

4. User Requirements, Preferences and Roles; Partners and Customers

Many types of mobile use-cases should be considered when planning for expanding your mobile access to Local Government information and systems.



Staff

- Want to choose their own device
- Many willing to own device and data plan if subsidised
- Want to update or buy a new device when they decide
- Want their own preference of interface and operating system on device and be able to change their minds
- Don't want to carry 2 phones and 2 tablets, personal plus business
- Want work/life balance and flexibility. Can enable fewer users in office and reduce property and environmental costs. Facilated by latest collaboration tools with Unified Comms and Real-time Presence.
- Will be more productive, add more value to the business – they say
- Want to expand skills and learn. Skill limitations. Lack of Training.
- Want to manage and carry less printed material, save costs
- Levels of Access required depending on roles - Need assessment to determine mobile requirements
- Want reasonable mobile data plan that covers all their requirements for business and some personal usage
- IT staff want versions of all key devices and OS's to be able to offer some level of support
- Can sometimes have problems with dropped or soaked business-owned devices when new models available
- IT staff will want to test device access to Virtual Machines – VDI/WTS/Citrix, VMware etc.
- Don't want Security to be a burden or deterrent to convenient usage. Most happy to sign security and usage policies (should be enforced)
- Self-Service BYOD site would make connectivity easier, ease support burden, for large implementations.
- Would like to have clear understanding of ownership and pro-rata cost sharing options and calculations on leaving the organisation
- HR typically want to provide flexibility to staff to attract and retain important key individuals

Contractors, Partners Auditors, Developers

- Support
- Administration
- APIs to Open Data
- Appropriate Levels of Access and Service
- Liability and responsibility challenges
- Access to policies online plus signed agreement

Citizens/Rate-Payers

- Information Access
- Online Payments
- Opt-in Social Networks
- Levels of Access and Services
- Community Projects and Involvement
- Tourist and visitor information
- Wi-Fi network availability
- Civil Defence information app for opt-in to latest warnings and advice

Damien Toman, Director, ICT Training & Consulting International Ltd, Nov. 2012. icttci.webs.com

The table above suggests areas for consideration to satisfy the demands of different classes of users, some specific requirements and individual user preferences. Determining the requirements and ideas of users is key to delivering successful mobile solutions.

The **Western Bay of Plenty District Council** has developed a sound approach for user position assessments for mobile technology. Its interview plan and detailed recording of feedback has helped capture, and provided analysis of, usage patterns with existing equipment; what new capability, functionality and application access would "help undertake work requirements more effectively or more efficiently" (in the field); and also captured other ideas raised by the interviewees. The CEO, GMs, Third Tiers, Field Staff and IT all contributed to the review.

Some comments from the Western Bay of Plenty District Council staff when asked about use of mobile devices:

- “The iPad and Smartphone have revolutionised the way I work. I’m 100% more productive!”
- “I access lots of documents by email (on iPad). My needs are vastly different than before. I could do away with my PC soon and therefore save costs” (Apps are available to allow access to Office documents, PDFs etc., and some provide annotation capability with a stylus).
- Many users stated that their Smartphones were used for emails, calendar, voice, TXTs, contacts, internet (including latest weather forecasts, Google Search and emergency services alerts), clock, camera, apps (Air NZ app mentioned by frequent travellers), GPS/Mapping (navigation applications like Google Maps), calculator, video, voice messages, hands-free voice when driving etc.
- Some users suggested that they could do without a desk phone if calls were all re-directed to the Smartphone.

When asked about mobile capability that would help them work more effectively and efficiently some user feedback was:

- “Mobile access to all corporate systems would be useful.”
- “Field staff require functionality to connect into systems to conduct business – issue notices, access inspection reports etc.”
- “Ability to link into telemetry with live streaming.”
- “Ability to interface with project managers and people.”
- “Would be good to have remote access via Citrix for access to full desktop and all information systems.”
- “Ideally we would have the same functionality available as a laptop.” (on a Tablet)
- “Would like access to the full Office suite, Objective, Ivy, Ozone. Tablet seems like a good option.”
- “From a safety point of view (for team) – ability to enable distress calls back to base would be good, with in-built GPS providing the precise location.”
- “GIS access out of the office would be good – allow to pull up plans and sign-off.”
- “Access to the building Codes, compliance documents, standards – would be useful.”
- “Ivy – to give good availability in the field to property boundaries and definitions.”
- “Once new browser access available for GIS we will need a tablet-sized screen to view it.”

- “From a whole-organisation point of view, it should be needs-based, not hierarchical. Functionality is what matters.”

- “The trend is for bigger organisations to not supply hardware anymore, but provide a subsidy to the workers instead.” Is this an option?

- “Our team should have a pool of devices for all to use.”

- “Photo and video capability are good for Court evidence.”

- “Ability to send instructions to contractors by writing on aerial photos.” “Ability to draw on maps – e.g. change a boundary line.” (Good candidates for Tablet with Wacom Digitiser screen and pen – Samsung).

- “Happy to pay technology cost 50:50 to acknowledge personal use aspect.”

- “Need to be able to carry on working offline in some areas and synchronise when back online.”

- “Ability to open a form and populate it e.g. when auditing performance of parks and reserves contract - then send back into Objective.”

- “Need to identify all implications before making changes e.g. HR Policies, Job Descriptions and Training needs.”

- “What about business continuity – working from home arrangements during disasters? Do the key people have the technology and connectivity required?”

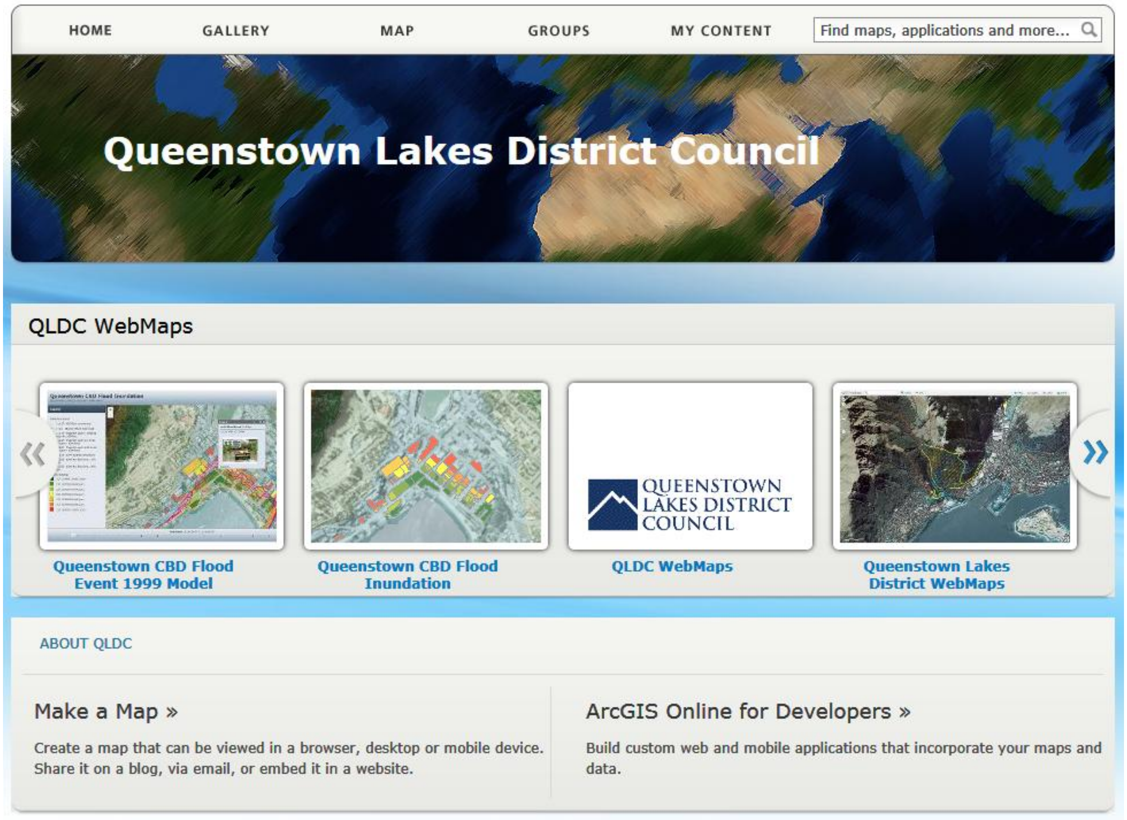
- “Check Pandemic Planning work previously done to identify ‘key’ positions able to work from home.”

- “Need to be highly flexible with our approach given the fast-changing nature of devices and the changes to mobile costs.”

The **Western Bay of Plenty District Council** has also developed a “Mobile Technology Management 2012 - Risk Management and Deployment Plan” in spreadsheet form, along with a well-defined process map for Mobile Technology Management and Deployment. These documents will likely be of significant value to other Councils following this mobility path. ALGIM can make these documents available to all ALGIM members.

The Council in this exercise focussed on internal users, which was a high priority first step. That work can pave the way to eventually investigating requirements and demands of partners, contractors, suppliers, auditors, external software developers and the growing demands of rate-payers, local businesses and other outside interests.

Queenstown Lakes District Council is a good example of how online services can be provided to external users. It provides online access to ArcGIS for Developers so they can build custom web and mobile applications that incorporate local maps and data. It also provides “Make a Map” to allow any visitor to its web site to create a map that can be viewed in a browser, desktop or mobile device, shared on a blog, sent via email, or embedded in a website.


HOME
GALLERY
MAP
GROUPS
MY CONTENT
Find maps, applications and more...
Queenstown Lakes District Council
QLDC WebMaps
Queenstown CBD Flood Event 1999 Model
Queenstown CBD Flood Inundation
QUEENSTOWN LAKES DISTRICT COUNCIL
QLDC WebMaps
Queenstown Lakes District WebMaps
ABOUT QLDC

Make a Map »

Create a map that can be viewed in a browser, desktop or mobile device. Share it on a blog, via email, or embed it in a website.

ArcGIS Online for Developers »

Build custom web and mobile applications that incorporate your maps and data.

> *“We recently signed up with the AoG mobile agreement. The AoG agreement provides a helpline, and a security suite under their Managed Mobility offering which we can apply to mobiles and tablets.*
>
> *Our parks department is using http://qldc.maps.arcgis.com/home/index.html on iPads to locate and add assets to our AMS.”*
> *(Kirsty Martin, Chief Information Officer (BCA), Queenstown Lakes District Council)*

This is impressive work by the Queenstown Lakes District Council and just shows what can be achieved when the leaders of the organisation get together and tackle how they can develop their strategy to improve delivery of information and open up access for business and consumers as the technologies offer new and exciting opportunities.

Auckland Council Civil Defence has released free apps for iOS, Android and Windows devices, to provide public alerts of emergencies and natural disasters to around half a million people with Smartphones in the region.

> *"After registering their contact details within the app, Aucklanders will receive advance notification of impending disasters such as tsunamis and cyclones, as well as important advisories from civil defence authorities following major catastrophes such as earthquakes."*
> *"The apps allow Aucklanders to stay updated with accurate and timely information on vital information in their area such as road closures, floods, slips, and severe wind warnings."*

Napier City Council Library provides mobile access to some online databases – some via websites that are optimised for mobile devices and one via an app that can be downloaded and set up to use the library login. Napier also provides a free public Wi-Fi service, with Taradale planned to follow by the end of 2012. Napier Library also provides an eBook service which is supported on most mobile devices.

Hutt City Council is now providing easy to use online services to customers:

- Online payment for fines (parking, litter, dog)
- Re-register dogs and pay fees
- Pay for and renew food and trade waste licenses
- Search cemetery records

Trade waste inspections are now electronically processed on site on mobile devices and the results uploaded when the device is docked. This avoids the paper forms and opportunity for errors when data is keyed into the system. The solution involved Motion Computing F5v Windows Tablets and TechnologyOne's Ci Mobility module. A recommendation is to:

- Trial with "tech-savvy" staff
- Provide training and documentation to all users.

Porirua City Council Provides Electronic Access to Council Information

Early in 2012, elected members asked to be provided with secure electronic access to the Council's meeting documents on Tablets (iPads specifically mentioned).

There was no budget provisioned and this was not in the scheduled programme of work. There was an expectation of a fast implementation with a return on investment by:

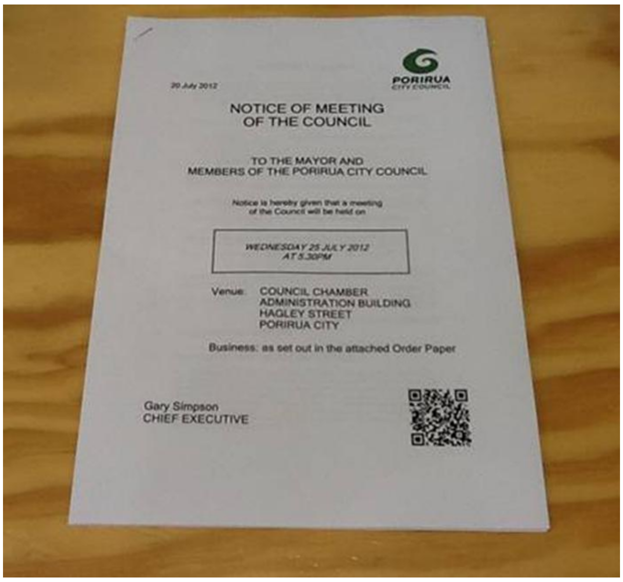
- Cost savings on printed material
- Greater productivity
- Enhanced remote access
- Better compliance with document management rules

- Other efficiencies in document management and communications

A Portal-Based Document Management solution was developed using Open Source software, built on a Virtualised Linux platform taking advantage of the VMware/ALGIM discount deal, and delivered over a Wi-Fi infrastructure.

To extend the value of this solution, QR (Quick Response - a type of matrix barcode) codes were placed on copies of public meeting agendas, encouraging open and democratic access. PCC has a high proportion of young citizens who, with Smartphones, can easily scan the QR codes for access to agendas and public notices. QR codes are also placed on many walkways to provide maps from the PCC web site. Web site stats show an encouraging uptake by the community. Users are also invited to visit the PCC Facebook site.

PDF documents are generated directly from the EDMS documents profiled for each meeting. 100% of all component documents of an agenda are captured into the EDMS. Public-excluded components are automatically removed and the remaining components are presented on the website for public viewing.



20 July 2012

PORIRUA CITY COUNCIL

NOTICE OF MEETING
OF THE COUNCIL

TO THE MAYOR AND
MEMBERS OF THE PORIRUA CITY COUNCIL

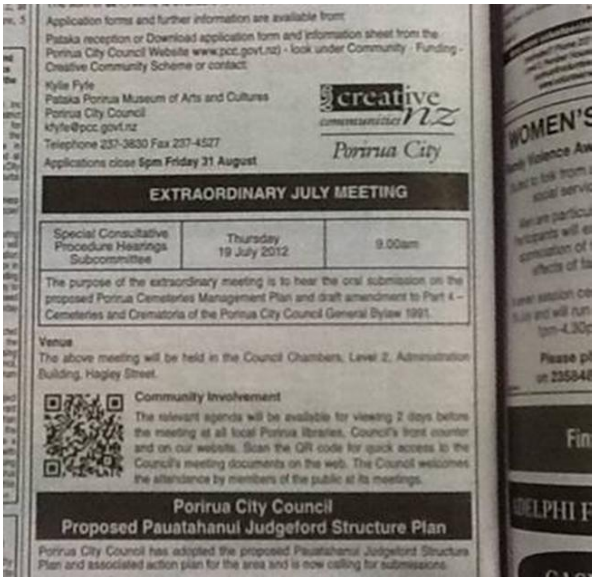
Notice is hereby given that a meeting
of the Council will be held on

WEDNESDAY 25 JULY 2012
AT 5.30PM

Venue: COUNCIL CHAMBER
ADMINISTRATION BUILDING
HAGLEY STREET
PORIRUA CITY

Business: as set out in the attached Order Paper

Gary Simpson
CHIEF EXECUTIVE



Application forms and further information are available from:

Pataka reception or Download application form and information sheet from the Porirua City Council Website www.pcc.govt.nz) - look under Community - Funding - Creative Community Scheme or contact:

Kylie Fyfe
Pataka Porirua Museum of Arts and Cultures
Porirua City Council
kfyfe@pcc.govt.nz
Telephone 237-3830 Fax 237-4527

Applications close **5pm Friday 31 August**

creative communities nz
Porirua City

EXTRAORDINARY JULY MEETING

Special Consultative Procedure Hearings Subcommittee	Thursday 19 July 2012	9.00am

The purpose of the extraordinary meeting is to hear the oral submission on the proposed Porirua Cemeteries Management Plan and draft amendment to Part 4 – Cemeteries and Crematoria of the Porirua City Council General Bylaw 1991.

Venue

The above meeting will be held in the Council Chambers, Level 2, Administration Building, Hagley Street.

Community Involvement

The relevant agenda will be available for viewing 2 days before the meeting at all local Porirua libraries, Council's front counter and on our website. Scan the QR code for quick access to the Council's meeting documents on the web. The Council welcomes the attendance by members of the public at its meetings.

Porirua City Council
Proposed Pauatahanui Judgeford Structure Plan

Porirua City Council has adopted the proposed Pauatahanui Judgeford Structure Plan and associated action plan for the area and is now calling for submissions.

QR codes appear on the page to encourage people to download the reports from the PCC web site. Hard copies of documents are distributed in libraries and the front counter.

> *"We believe in open democratic decision making – we WANT people to read our agendas and come to our meetings"*

Readers can scan the QR code to go to the web site to download specific documents of interest.

This project has created positive publicity for the Council and proved that Porirua City Council is "up with the play". Use of QR codes and iPads helps Porirua Council's image.

The project is paying for itself to the tune of $100,000 per year.

Training was provided for Councillors.

This Innovative approach has led to:

- Cost savings
- Efficiency improvements
- Improved service
- Increased use of Council's EDMS and compliance with document management policies
- Positive publicity for the Council

This project was a launching pad for taking the Council's information systems into the 21st century and making it more relevant to the younger population.

The 2012 **Ericsson ConsumerLab report**, based on an online survey of 500 New Zealanders, found that 7% of New Zealanders currently own a Tablet device and 20% say they expect to own one within six months. That is massive growth.

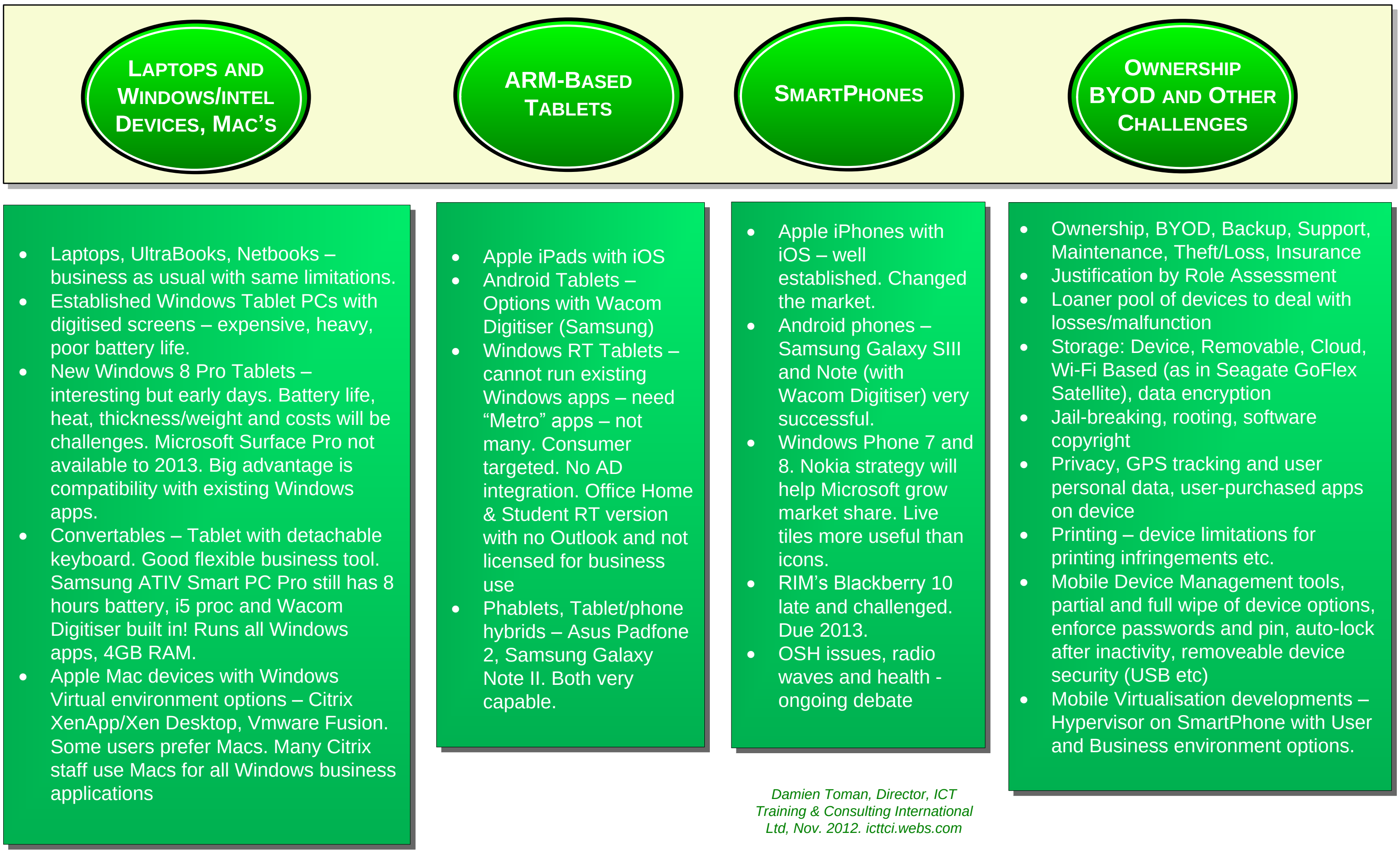
33% of New Zealanders already have Smartphones and this is also increasing very rapidly. As more and more of the population flock to these new methods of accessing information and using new applications to interact and discover what is happening in their area, or the place they are visiting, demands will increase and leading councils can potentially gain important benefits with more satisfied users, customers, businesses, visitors and tourists.

Those Councils that have already implemented, or plan to implement, free town/city-centre Wi-Fi access, can particularly add value to their community and visitors. Napier, Dunedin, Wellington and Hamilton are already in place.

> *With the aim of giving Napier the 'X factor' during the Rugby World Cup and beyond, local communications experts from Revolutionz Ltd. worked with Napier City Council to provide anyone with wireless capabilities on their Smartphone or laptop free 15-minute sessions while in the central city.*
>
> *"This means people can do everything from catch up on the daily news and sports results to check their emails and update their social networking status without leaving the hotwired area," Napier Mayor, Barbara Arnott says.*

5. Devices, Ownership and Policy Considerations for Mobility

Having assessed the user requirements for functionality in the field, it is then possible to look at the form factors and features of the devices available and make some decisions around suitability for purpose.



Laptops and Windows/Intel Devices, Mac's

- Laptops, UltraBooks, Netbooks – business as usual with same limitations.
- Established Windows Tablet PCs with digitised screens – expensive, heavy, poor battery life.
- New Windows 8 Pro Tablets – interesting but early days. Battery life, heat, thickness/weight and costs will be challenges. Microsoft Surface Pro not available to 2013. Big advantage is compatibility with existing Windows apps.
- Convertables – Tablet with detachable keyboard. Good flexible business tool. Samsung ATIV Smart PC Pro still has 8 hours battery, i5 proc and Wacom Digitiser built in! Runs all Windows apps, 4GB RAM.
- Apple Mac devices with Windows Virtual environment options – Citrix XenApp/Xen Desktop, Vmware Fusion. Some users prefer Macs. Many Citrix staff use Macs for all Windows business applications

ARM-Based Tablets

- Apple iPads with iOS
- Android Tablets – Options with Wacom Digitiser (Samsung)
- Windows RT Tablets – cannot run existing Windows apps – need "Metro" apps – not many. Consumer targeted. No AD integration. Office Home & Student RT version with no Outlook and not licensed for business use
- Phablets, Tablet/phone hybrids – Asus Padfone 2, Samsung Galaxy Note II. Both very capable.

SmartPhones

- Apple iPhones with iOS – well established. Changed the market.
- Android phones – Samsung Galaxy SIII and Note (with Wacom Digitiser) very successful.
- Windows Phone 7 and 8. Nokia strategy will help Microsoft grow market share. Live tiles more useful than icons.
- RIM's Blackberry 10 late and challenged. Due 2013.
- OSH issues, radio waves and health - ongoing debate

Ownership BYOD and Other Challenges

- Ownership, BYOD, Backup, Support, Maintenance, Theft/Loss, Insurance
- Justification by Role Assessment
- Loaner pool of devices to deal with losses/malfunction
- Storage: Device, Removable, Cloud, Wi-Fi Based (as in Seagate GoFlex Satellite), data encryption
- Jail-breaking, rooting, software copyright
- Privacy, GPS tracking and user personal data, user-purchased apps on device
- Printing – device limitations for printing infringements etc.
- Mobile Device Management tools, partial and full wipe of device options, enforce passwords and pin, auto-lock after inactivity, removeable device security (USB etc)
- Mobile Virtualisation developments – Hypervisor on SmartPhone with User and Business environment options.

Damien Toman, Director, ICT Training & Consulting International Ltd, Nov. 2012. icttci.webs.com

The table above highlights the variety of device hardware form-factors, operating systems and just some of the decisions around ownership, responsibilities and management that need to be made.

It will become increasingly challenging to stick to a pre-defined short-list of standard approved devices, and operating system environments, to ease the ICT support burden. HR departments, in particular, realise that the preferences of an important senior manager, could well be a factor in retaining his services. In many areas in New Zealand there are limited suitable candidates for key roles in Local Government.

The ICT support teams also feel the pressure of dealing with the inevitable problems that will arise, relating to the users and devices that they will have to tackle. Some will embrace the challenge as an exciting learning path for device integration and support. Some will be intimidated. Most will embrace the opportunity and want to be part of this exciting development. Some will want to demonstrate their ability to lead the way.

5.1. Device Choices for Mobility

When providing input to a wide variety of business applications, nothing beats the performance and productivity of a **powerful desktop computer**. It would have a very large screen (or two), powerful quad-core processor, a **64-bit Operating System** (e.g. Windows 7 or 8) that allows 16GB of RAM to be used, a powerful graphics card, and would be able to run a mix of 64-bit and 32-bit business applications. A full-sized keyboard and mouse combination is still the most productive method for providing input to many applications. The problem is, we often need mobility to be productive.

When working while out of the office, a compromise is typically required. The next most capable device is a large **laptop**. It will have a smaller screen, less RAM, but otherwise will be able to run the same applications.

Where weight, size and battery limitations are an issue, the recent **UltraBooks** are an attractive proposition as they also can run all the same Windows business applications.

Your requirements may go way beyond what these laptop-style devices can offer. The usage of mobile devices like **Tablets and Smartphones**, as stated by users in the previous section, demonstrates that these relatively recent device developments can add significant value to the productivity of mobile users. While these new smart devices also have some limitations, like not being able to run your existing Windows applications, they can still be used to access all your Windows applications and business systems by allowing them to access a secure **Virtual Desktop** back in your Data Centre or Computer Room. We will explore the architecture of this type of solution in a later section. **Apple Mac** portable computers can be used for running Windows applications by installing Citrix Receiver software to allow access to a Virtual Desktop in the computer room. VMware Fusion on the Mac **allows Windows applications to run inside a Virtual Machine on the Mac**. Many Citrix staff use Macs to access all their Windows business applications via Virtual Desktops.

So, can we really have it all ways? Have the features and functionality of the device (GPS, Camera, touch-screen, pen options, all-day battery life, instant on etc.) plus the same capability as a full desktop? Yes, it is possible, as long as you have network access (we will cover networking in the next section). Devices are a means of accessing applications and data – this approach provides access to more applications than any other.

For some use-cases, it may be a requirement to use particular applications when no network connectivity, of any type, is readily available. For these cases, applications have been developed that can allow capturing of data while disconnected, and have the ability to synchronise that data back to the business application server, when connectivity is available. This is an effective approach for form-filling in the field. Some of the development environments available allow customised forms to be developed quite quickly, to run them on the device which securely captures the data, and then talks back to the databases when connected.

With the added off-line data capture capability, some applications can also be created that allow sub-sets of database information to be downloaded and stored on the device to provide additional look-up information while disconnected. **With all of these options, a Tablet can do**

much more than any desktop or traditional laptop, while being much more portable and, for many, easier to use.

Some of the hybrid/convertible style devices can be a useful compromise. With some options, the phone becomes the computer, and docks in a tablet-style screen (Asus Padfone). Blue-tooth wireless keyboard options can also be added to most Tablets. Some of the latest tablets provide a keyboard built-in to the optional screen cover (Microsoft Surface).

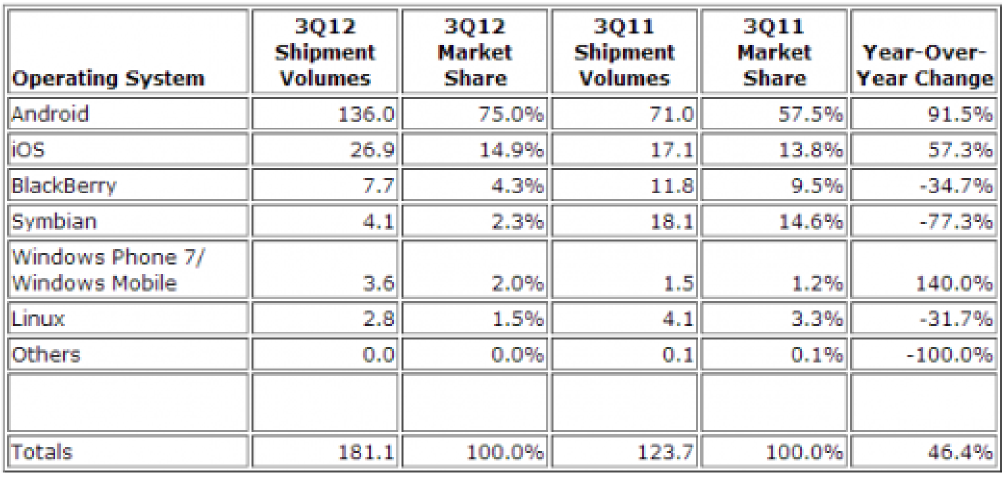
There are many things to consider when it comes to making your device choice. There is the suitability to the delivery of the required applications, the user role, the device form-factor, the operating system, the compatibility with the range of applications you use, cost, support, manageability, features, specifications etc.:

- The just-released **Windows RT** devices will not run existing Windows applications. They require applications to be developed to the new Microsoft Windows 8 "Modern" or "Metro" or "Windows Store" environment. This is because they use **ARM-architecture processors**, not the Intel x86 processors used by Windows 7 and Windows 8 Pro. Compared to iOS and Android, there are limited applications available for RT. The RT devices target consumers. They cannot be authenticated into an Active Directory Domain. The cut-down version of Microsoft Office RT does not come with Outlook and is not licensed for use in a business environment.

- The advantage of **Windows 8 Pro Tablet** devices is that they use Intel processors and can therefore run existing Windows applications and RT applications. Microsoft's Surface for Windows 8 Pro Tablet will not be available until early in 2013. The Samsung ATIV Smart PC Pro is a full 64-bit, Intel i5, Windows 8 Pro Tablet due mid. November 2012 for NZ$1699 excl. GST. HP's ElitePad is due in early 2013 and is likely to be Intel Atom based as are the Lenovo ThinkPad Tablet 2 and the Dell Latitude 10. Atom devices will be cheaper, have longer battery life, less memory and be less powerful than the Intel i3, i5 and i7 processor devices.
  Issues for many Windows 8 Pro Tablets will be cost, thickness, weight, heat and possibly battery life (though Samsung claims 8 hours is possible, even with the powerful i5 processor).

- The new **Secure Boot** feature of Windows 8 uses public-key infrastructure to protect the operating system from malware and will improve security which will be important for business users – it can also be turned off.

- **Android 4.2**, the latest, also has **improved security features** and has support for multiple users (useful for a pooled device). The new real-time scanning of apps keeps you aware of any suspicious behaviour and warns you of rogue apps that you might try to install. This is not typically an issue unless the device is “rooted”. Android is now the leading operating system for Smartphones. Latest IDC global Smartphone published figures:



Operating System	3Q12 Shipment Volumes	3Q12 Market Share	3Q11 Shipment Volumes	3Q11 Market Share	Year-Over-Year Change
Android	136.0	75.0%	71.0	57.5%	91.5%
iOS	26.9	14.9%	17.1	13.8%	57.3%
BlackBerry	7.7	4.3%	11.8	9.5%	-34.7%
Symbian	4.1	2.3%	18.1	14.6%	-77.3%
Windows Phone 7/ Windows Mobile	3.6	2.0%	1.5	1.2%	140.0%
Linux	2.8	1.5%	4.1	3.3%	-31.7%
Others	0.0	0.0%	0.1	0.1%	-100.0%
Totals	181.1	100.0%	123.7	100.0%	46.4%

- **Near Field Communication (NFC)** is supported on some of the Android devices and will become increasingly important for payments, transferring data between devices and providing access to information when the device is held closely (within 4cm) to an NFC sticker. This radio-frequency identification (RFID) standard can be very useful for providing up-to-date tourist information and reading asset tags (unpowered). For many applications, this will replace or be used alongside, QR codes. Apple devices do not yet support NFC. Google Wallet and Microsoft’s Windows Phone 8 both support NFC. An NFC payments system, for bus services, is already operating in Wellington. Auckland Transport and Telecom NZ are running an NFC pilot.

- The Google Maps app for Android is an excellent free turn-by-turn navigation system available on Tablets and Smartphones. Apple’s iOS 6 no longer has the Google Maps app and their attempt to replace it has been embarrassing. Sometimes these app limitations will determine the choice of devices.

- iOS from Apple runs on the iPhones and iPads. It is a slick operating system environment for running apps but can be frustrating for technically aware users as it does not provide file system access as standard and it has clunky ways to import files as related to apps. Having established the market for these devices, it is now very well embedded in business environments. Apple leads the way in Tablet sales with the iPad range. The iPads 3 and 4 have the best display available on any Tablet. The new Mini iPad does not have the same “retina” display resolution and may be too small for many users that plan to access Virtual Desktops to run Windows applications.

- Adding a Citrix Receiver or VMware View Client to any of these Tablets provides access to full Windows Virtual Desktops and applications (if you have the back-end servers in place – more on that architecture later).

- Look for devices like the Samsung Note range if you require the ability to write notes on maps and photos (as requested by a user in previous section) or annotate PDF documents. The built-in Wacom Digitiser Screens are pressure sensitive; the devices have built-in pens; they perform infinitely better than capacitive styli for standard touch screens (like the iPad).

- For most field Council workers, a comprehensive GPS system will be desirable. Look for devices that support both the USA's GPS and the Russian GLONASS systems. The iPad does and so do many of the Samsung devices. This improves accuracy and tracking performance. Be careful about choosing Wi-Fi only Tablets. Many do not have GPS and just use triangulation of Wi-Fi signals to try to track your location. They also cannot provide navigation if they cannot download mapping information while you travel. A way around this is to use an Android Phone's Wi-Fi Hotspot ability to allow the Wi-Fi Tablet to use the phone's mobile data link.

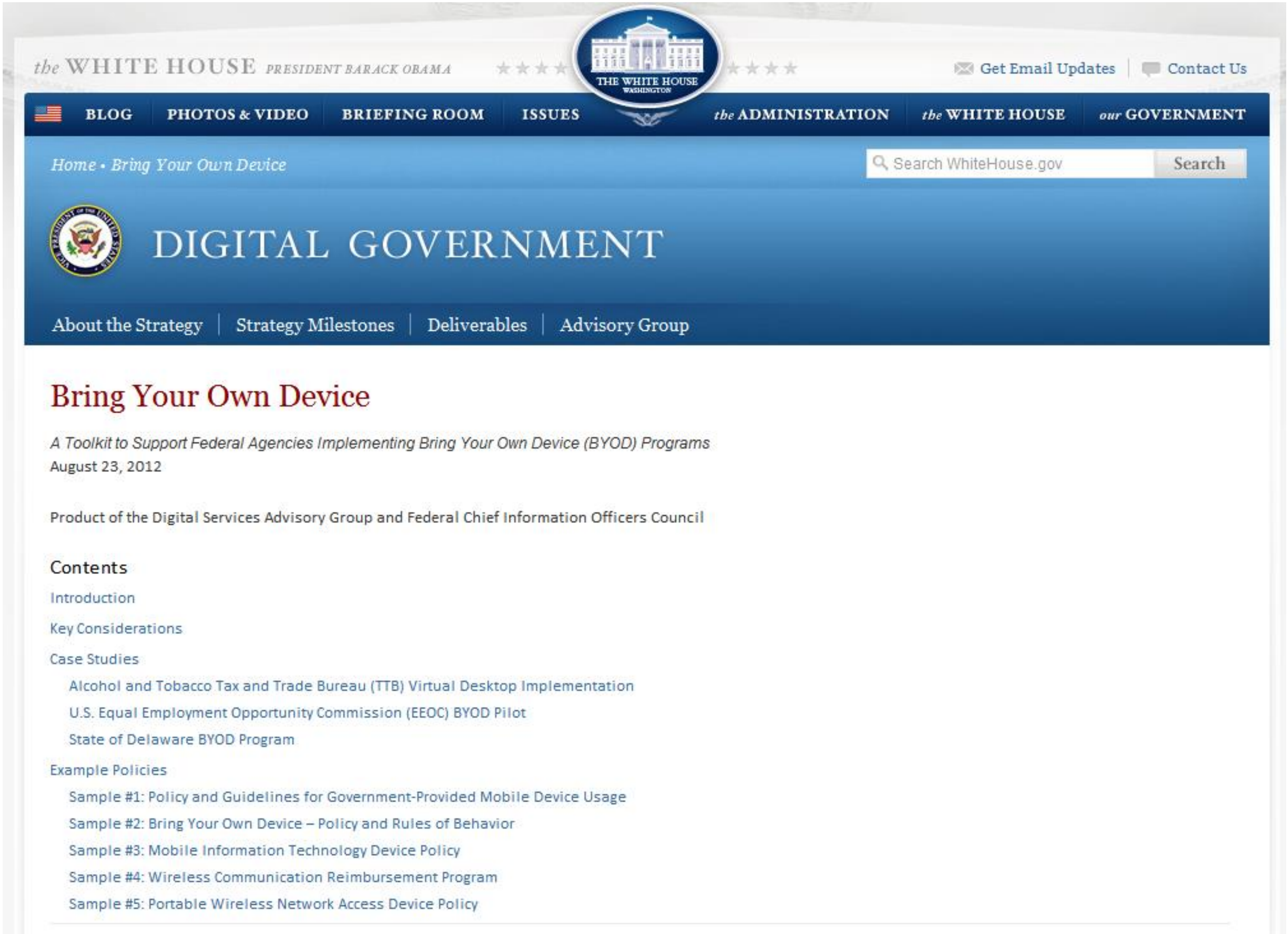
- Be aware that many of the Intel Atom processor devices only support 32-bit Windows and 32-bit applications and also therefore cannot use more than 3GBs of RAM. Intel i3, i5 and i7 devices do not have these limitations.

- Research in Motion's BlackBerry 10 Operating System release has been delayed till around March 2013. Once the leader in business mobile phones, RIM has many challenges including availability of apps for the platform and stiff competition from iOS, Android and Windows Phone 8.

5.2. BYOD (Bring Your Own Device) Considerations

Most Local Government organisations in New Zealand do not yet support a BYOD policy. Most are very interested but are concerned about security, support, manageability and privacy. This White Paper should help organisations become more aware of what needs to be considered in developing policies and solutions to support this BYOD wave that is growing rapidly and putting pressure on ICT departments to deliver. This is happening in all businesses, not just Local Government.

The USA Government has issued a BYOD toolkit to encourage and support Federal Agencies implementing BYOD programmes:



Bring Your Own Device

A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs
August 23, 2012

Product of the Digital Services Advisory Group and Federal Chief Information Officers Council

Contents

Gartner predicts (October 2012) that half of all non-PC devices will be purchased by employees in 2016. Also half of all business devices will be purchased by employees by the end of this decade. Gartner states that a new strategic role of “Chief Digital Officer” will be created and the leaders today will define the role.

Queenstown Lakes District Council funding BYOD

Queenstown Lakes District Council is one of the New Zealand organisations leading the way:

> *"We are funding people eligible for a smartphone with $500, rather than supplying a handset. This is renewed every 2 years. People can use that to buy a phone of their choice and, as they own it, they are also responsible for purchasing accessories or replacing it if it is lost or broken. This new policy has been successful, being cheaper for the organisation and providing the staff with the flexibility they have been asking for.*
>
> *We provide all our Councillors and senior managers with iPads (although we have a Samsung Galaxy Note and Galaxy S2 to explore alternatives). Both groups have agreed that by having a tablet they won't get hard copy agendas, and on the whole this is working well. Being so intuitive the tablets have a good take up rate. It also means that they have instant access to policies stored on their iPads."*
> *(Kirsty Martin, Chief Information Officer (BCA), Queenstown Lakes District Council)*

Southland District Council BYOD

Southland District Council has now developed its "Portable Data Device Guidelines" policy document to accommodate BYOD (ALGIM can provide a copy). This document also refers back to other existing policy documents covering Code of Conduct, Information Management, e-mail and Internet usage policies. The IM department maintains a list of approved "Standard" devices. They also allow device exceptions when justified and approved after a Business Case process (diagram in the document).

Most devices are owned and provided by the Council. A few iPad owners have been authorised to use their own devices over the Council Wi-Fi network. The IM team do not officially support user-owned devices but will provide assistance on a best effort basis when their workload permits. The devices all need to be registered and inspected. Permission must be granted to allow IM to install (e.g. anti-malware and Mobile Device Management software) or remove software to minimise any security risks. The user must agree to allow remote locking and possibly wiping the device clean if it is lost or stolen – which must be reported as soon as possible. If the user leaves the business, they need to submit the device for inspection and removal of any business connectivity tools or software provided by the Council.

Where connectivity to the Council network is required, access is provided through a secure Virtual Private Network and Thin Client software is used to present a Virtual Desktop with the required applications. This approach keeps all data securely in the Data Centre and not on the device. Any data or documents stored on the device need to be backed up by the user. "The Council reserves the right to audit all portable data devices that connect to the SDC network at any time."

Currently the Council does not offer any subsidy for the purchase of devices and any Mobile Data usage or software purchase will only be reimbursed if prior approval by a Group Manager has been granted.

New Zealand Local Government BYOD Status

Based on feedback from the Councils that have responded to this exercise, most do not yet embrace BYOD. Most are interested but not ready. Some are doing tests with a small number of keen users, mostly for email and calendar links to Exchange messaging servers.

Business Case Development for BYOD

Developing a sound business case for BYOD can be challenging, depending on the existing security infrastructure, the policy choices made and the application delivery options available.

> *"Gartner believes that we are likely to see highly successful BYOD programs in the coming years. Many businesses will expand beyond smartphones and tablets and embrace BYO for personal computers." Gartner, Aug 2012*

Key business case considerations:

1. User Productivity gains through more hours worked; better communications and team collaboration, especially when mobile; users having the device that suits them (often costing more than a business-supplied device). Users will often invest in and install their own purchased applications that they use to improve their business performance. More convenient access to web-based business applications could enhance productivity.

> *"Intel quotes productivity gains on the order of 2 million hours gained over a year, and that is just for an initial 10,000 user rollout" Wendy Carstairs, Cisco, July 2012"*

2. Attract and retain key staff; improve employee satisfaction and morale. Employees feel empowered.

3. Cost savings, depending on approach

   - User owns the device and data plan, with a device subsidy every 2 or 3 years at less than the cost of business-supplied devices plus data plans.

   - Flexible workplace, hot-desking and smaller offices or no need to expand. Options for some employee roles to work more days from home.

Cost Challenges:

- Security solutions may need a major overhaul. (Though how secure are the business supplied laptops? Are all important data files on the hard disk encrypted?). May not be required if users are not granted access to the main network, server features and applications.

- New Mobile Device Management software may be required – depending on levels of access provided and policy choices.

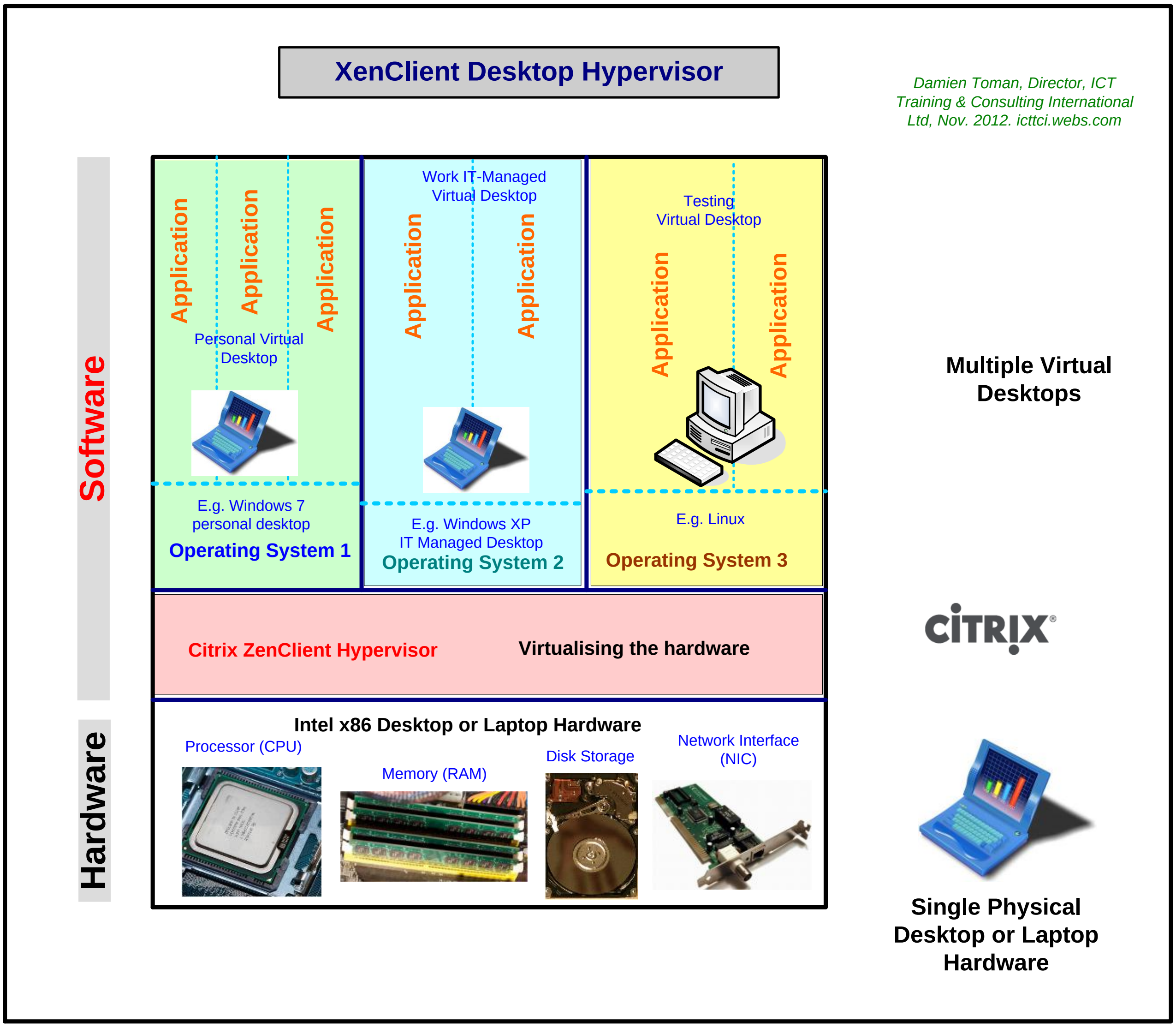
- The organisation may not have Virtual Desktop Infrastructure in place and may want to go that way.

- ICT Support demand may increase, leading to a requirement for more staff.

Virtualisation and Hypervisors for BYOD and Mobile Devices

Citrix XenClient

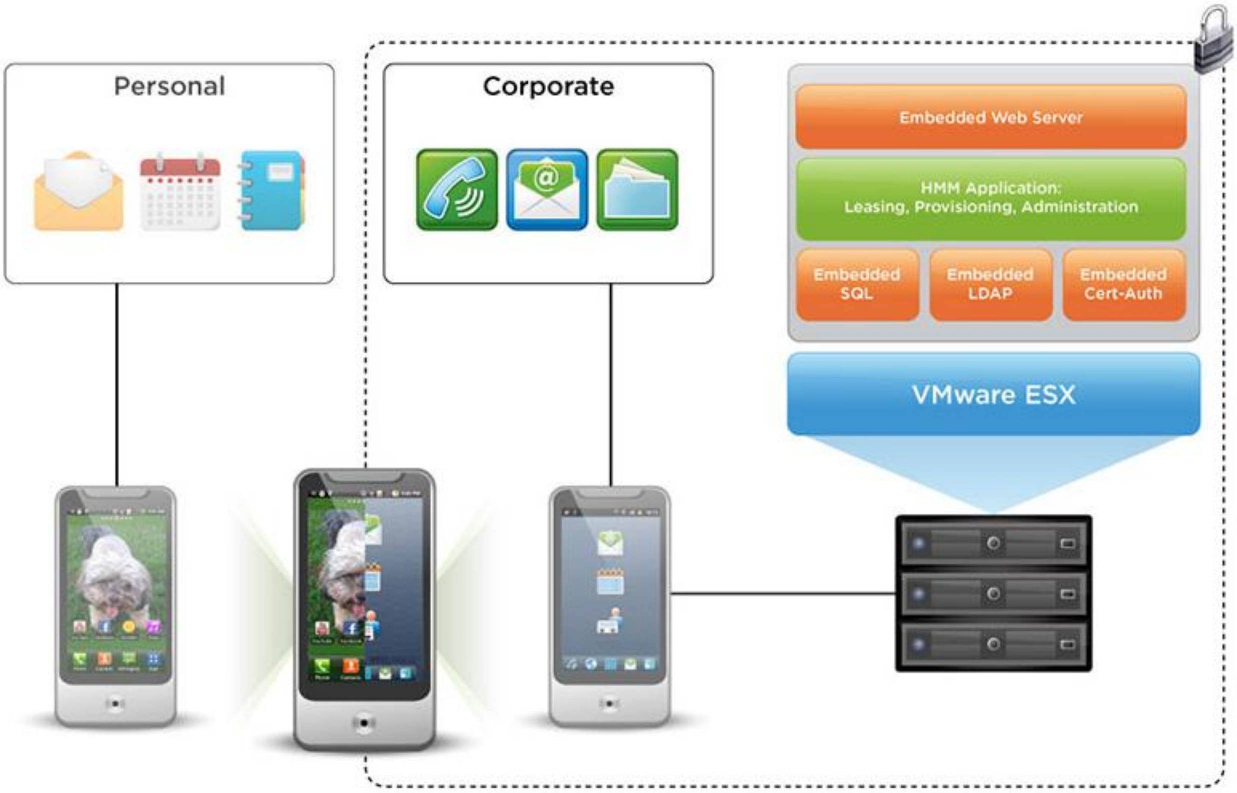
An interesting technology development to support BYOD for laptops is available from Citrix. XenClient provides a Hypervisor that runs on the laptop and allows multiple operating system instances to run simultaneously. This supports a user personal environment running alongside a business environment. The business image can be synchronised to a Virtual Desktop in the Data Centre. The image on the laptop can be encrypted. Losing your laptop then means that your desktop is still available as a Virtual Machine and your data is secure on the encrypted disk image on the lost device. It provides automated backup and remote wiping of the device. This technology initially only supported Intel vPro-based laptops (with hardware-assisted virtualisation) but has now opened up to hundreds more laptops – Citrix provides a list of current supported hardware. XenClient is included in some XenDesktop versions. The Town of Lincoln, Massachusetts, has implemented XenClient and greatly improved manageability of laptops.


XenClient Desktop Hypervisor
Damien Toman, Director, ICT Training & Consulting International Ltd, Nov. 2012. icttci.webs.com
Software
Hardware
Application
Application
Application
Personal Virtual Desktop
E.g. Windows 7 personal desktop
Operating System 1
Work IT-Managed Virtual Desktop
Application
Application
E.g. Windows XP IT Managed Desktop
Operating System 2
Testing Virtual Desktop
Application
Application
E.g. Linux
Operating System 3
Multiple Virtual Desktops
Citrix ZenClient Hypervisor
Virtualising the hardware
CITRIX
Intel x86 Desktop or Laptop Hardware
Processor (CPU)
Memory (RAM)
Disk Storage
Network Interface (NIC)
Single Physical Desktop or Laptop Hardware

VMware Horizon Mobile

VMware has created a Hypervisor for ARM-based devices. This is an exciting concept. Initially called the VMware Mobile Virtualization Platform, it was positioned as potentially running multiple different operating systems on a single device. Now it is called VMware Horizon Mobile, and is being positioned as allowing two instances of Android to run on a device: one a personal instance; the other a business instance that can be managed.

> *"enables enterprises to securely provision and manage a corporate mobile workspace on employees' Android smartphones in isolation from their personal environment. This dual persona solution enables enterprises to embrace employees' preferred mobile devices while maintaining the security, compliance and manageability enterprises require. Horizon Mobile provides a wide range of features to enhance productivity by creating a purpose-built and preconfigured native mobile workspace based on employee responsibilities that is tied to the user, not the device."*



Embrace and enable employees' transition to mobile devices by providing full access to enterprise applications and services while on the go.

Provide a consistent and easy-to-use native mobile experience to employees across a variety of devices.

Enable employees to use their preferred mobile device by providing two isolated and complete personas on a single device; employees can use one for personal life and the other for work life.

This opens up exciting possibilities for the future of mobility. Samsung, LG and Google's Motorola Mobility have been working with VMware on this. Separate phone numbers can be supported to allow separate billing for personal and business use.

Other BYOD Examples, Surveys and Quotes

State of Delaware BYOD Program July 2012:

> *"In an effort to keep up with the pace of mobile technology, the State of Delaware initiated an effort to not only embrace the concept of BYOD but to realize significant savings by having state employees turn in their state owned device in favor of a personally owned device. In order to encourage the behavior, the State agreed to reimburse a flat amount for an employee using their personal device or cell phone for state business. It was expected that by taking this action the State could stand to save $2.5 million or approximately half of the current wireless expenditure……*
>
> *The State of Delaware experience to date has been positive with specific savings and device reductions. The State anticipates continuing to grow the program by limiting the number of state owned devices while encouraging the use of personal devices into the future."*

Citrix is an organisation that provides technology to support BYOD and practices what it preaches. From 2008 it has allowed users to connect their own devices to its network and run its business applications in a Virtual Desktop environment.

> *"In keeping with our open workplace philosophy, Citrix allows anyone to bring in any type of device for work with no restrictions," says Paul Martine, chief information officer at Citrix Systems." (Citrix Bring Your Own Device White Paper 2012).*
>
> *"Participants should be required to buy their personal devices through normal consumer channels rather than an organization's purchasing department. This helps maintain clear lines of ownership as well as ensures that participants have a direct relationship with their hardware vendor." Citrix.*

Citrix also offers a secure "ShareFile" capability that acts like a corporate DropBox (Cloud-based storage with sychronisation).

Satisfying user demands for flexibility and choice is not the only reason. There are productivity benefits as well:

> *"According to recent research from enterprise WiFi provider iPass, many employees are working up to 20 additional hours per week unpaid as a result of bring your own device (BYOD) policies adopted by their firms." (ComputerWorld. Antony Savvas, London, Sunday, 14 October, 2012)*

A Cisco study in May 2012 involving 600 IT leaders (organisations with 1000+ employees) with responsibility for mobile solutions, across 18 industries, discovered that:

> *41% of enterprises said **most** Smartphones connected to the company network were employee-owned*

62% of enterprises pay for employee devices, voice and data plans

75% expect the share of employee-owned devices connecting to the business network to increase significantly over the next 2 years

69% of CIOs see BYOD as positive for their organisation, offering productivity and satisfaction benefits

In India over 50% of business mobile devices are employee owned and most organisations support BYOD

BYOD is seen as a potential source of innovation and competitive advantage

Cisco BYOD staff pay on average US$600 for their preferred devices to enhance their work experience

Some interesting quotes from Good Technology BYOD Report:

According to Forrester Research, more than half of US information workers now pay for their smartphones and monthly plans to do work for their employers, and three-quarters pick the smartphone they want, rather than accepting IT's choice.

If it becomes a simple affair in the eyes of an employee to start a project at work, put it on a mobile device for the train ride home—perhaps pausing to check the news or play Angry Birds—and make final tweaks to the project after the kids are in bed, that employee will be more productive.

"Based on overall survey responses, Good estimates the broad industry average cost for a company-owned device to be about US$80/month." - substantial savings opportunities await organizations that switch to BYOD programs.

Another customer, Union Bank, saved approximately US$1 million by switching to BYOD.

"Highly Regulated Industries Embrace BYOD: Large companies from the Finance/Insurance and Healthcare industries dominate the overall BYOD picture"

"Employees Are Willing to Pay for Personal Choice: 50 % of companies with BYOD models are requiring employees to cover all costs – and they are happy to do so; 45 % provide their employees with a stipend or "expense back" option to help subsidize the cost of their mobile device or service plan."

"Among the respondents, 72 % were already formally supporting BYOD programs. This was significantly higher than the 60 % level of support indicated in Good's January 2011 survey."

"Good's unique "containerization" approach allows a clean separation between personal and business data, apps and enhanced data loss prevention"

"Half of those surveyed with BYOD devices in place said that employees cover all costs associated with their devices including device and data plans."

> *“20 % allow eligible employees to expense back mobile services costs, but with nearly all of those customers requiring prior management approval and setting a fixed cap on expenses to control costs.”*
>
> *“Good has multiple customers who offer a variable stipend based on the user’s role. This approach allows the company to match spending exactly to the productivity benefit they associate with each role.”*

The US federal government Digital Services Advisory Group embraces BYOD:

> *“The US federal government, good at both regulating and embracing things, urges that a balance be struck between the two. Don't fight the trend, advises the government's Digital Services Advisory Group, formed and directed by federal CIO Steven VanRoekel. Rather, go with the flow, and recognize that BYOD can be an asset to organizations, if properly managed.*
>
> *That's the gist of the advisory group's latest government-wide bring-your-own-device (BYOD) guidelines. The directives, considered voluntary, are based on lessons learned from successful BYOD programs launched at forward-leaning agencies.*
>
> *While the report is targeted at helping federal agencies set up BYOD policies, the guidelines are instructive for commercial enterprises as well. Interestingly, there is a case study of one agency in which BYOD was smoothly integrated into a virtual desktop strategy.”* By Joe Mc Kendrick for Service Oriented | August 30, 2012

“In addition to offering an overview of considerations for BYOD adoption, the document highlights successful federal BYOD pilots or programs, including: “

- The Treasury Department’s Alcohol and Tobacco Tax and Trade Bureau implemented a virtual desktop that allows a BYOD solution with minimal policy or legal implications.
- The Equal Employment Opportunity Commission is one of the first federal agencies to launch a BYOD pilot in which employees can choose to opt out of the government-provided mobile device program and install third-party software on their own smartphones, so they can be used for work purposes.
- The State of Delaware officially embraced BYOD, which could save it an estimated $2.5 million -- about half of its current wireless costs.

Digital government push fuels BYOD adoption By Camille Tuutti Aug, 2012

Forrester report finds:

> *“More than half of US information workers pay for their smartphones and monthly plans, and threequarters pick the smartphone they want rather than accept IT’s choice.” “Consumerization Drives Smartphone Proliferation”, Forrester Research, Inc.Dec 2011.*
>
> *“The just-released BYOD guidance stresses that BYOD is not mandatory and the toolkit isn't meant to be comprehensive "but rather provides key areas for consideration and*

examples of existing policies and best practices." The document was produced by the Digital Services Advisory Group and the Federal CIO Council."

"The Consumer Outlook on Tablets, Q4 2012 Edition, shows that tablet ownership rates among online U.S. consumers reached 31 % as of September 2012, more than doubling the ownership rate from October 2011." Ce.org.

"Like it or not, the "bring your own device" (BYOD) trend is in full swing. According to Juniper Research, the number of employee-owned smartphones and tablets used in businesses will more than double by 2014, reaching 350 million compared with almost 150 million this year"

Mary Brandel, Network World, October 01, 2012

5.3. Mobility Device Policy Considerations

It is important to have input from user representatives, HR, Legal, Finance, Business Managers, IT and the Executive team, in formulating draft mobile device policies, agreeing the content of the initial release, and vetting on-going changes.

For examples of written policies, see appendices.

See next page for Mobile Device Policy Considerations.

Mobile Device Policy - Scope of Considerations in Policy Document

			Policy Components
1	**Mobile Device Policy for Organisation Supplied Devices.**		Mobile Device and Acceptable Use Policies are usually well established for laptops, internet access and email usage. These may need to be revised for Tablets, Smartphones, Mobile Data, Wi-Fi, Unified Messaging, storage options and business network VPN access.
		1.1	Purpose of Mobile Device Policy
		1.2	Range of mobile devices covered by the policy plus any exceptions and how to apply to use a new device not covered in the policy. The security solutions implemented may only work with specific features supported on the device and its operating system.
		1.3	Roles, Responsibilities and ownership of policy and enforcement. Include Legal, HR, Finance, IT and Management.
		1.4	Approvals processes
		1.5	Purchasing devices - options, process.
		1.6	Rules and process for set-up and security configuration (including encryption key set-up). Mobile Device Management (MDM) installation and configuration. Include auto-lock rules and timing, password enforcement/rotation/restrictions/number of failed attempts before wiping device, GPS tracking/finding requirements (e.g. "Find my iPad"). Rules on software updates: OS, patches, app updates. Corp app-store usage if deployed. Any limitations on Apple AppStore user-installed apps. Limitations of access to specific applications or data using that device or specific network connection. Jailbreaking/rooting, re-ROMing - some MDM tools can block such devices. Any possible exceptions for some users. (All usually forced by MDM solution). For small organisations an MDM solution may not be deployed. Some MDM tools can wipe business data and leave personal data intact.
		1.7	Rules on different types of network and systems access. Wi-Fi, Mobile Data, wired access, access from home network, via VPN. Use and restrictions around back-end services and systems when remote.
		1.8	Rules for Voice/Data/SMS Charges. Handling over-runs. Process to apply for a limit increase. International-roaming charges needs specific attention as costs can be high. Monitoring of usage. Caps for data volumes and user pays after that one of many options. Rules when using a Bulk data arrangement with service provider.
		1.9	Reporting of Lost, Stolen or malfunctioning device. Rules regarding timing, replacement and responsibilities. Also, when negligence a factor.
		1.10	Privacy and Data Protection: expectations regarding personal data, GPS tracking logs etc. and visibility to support staff. Password disclosure for some aspects of support. Legal department needs to ensure compliance with the law.
		1.11	Outline of IT Support Policy limitations depending on Laptop, Tablet, SmartPhone. Fully supported devices. Best efforts supported devices. Unsupported devices allowed access. Support calls processing. Exceptions. Some initial user training may be offered by IT to minimise downstream support issues.
		1.12	Storage Rules: on device, removeable (USB, MicroSD etc), Wi-Fi Based storage (Seagate Satelite), Cloud/Personal Cloud (e.g. DropBox). Data stored on properly configured iOS devices is much more secure than on most laptops (strong encryption). (Android also has strong encryption options.).
		1.13	Accessories used with device - ownership, exceptions if agreed by Manager (car kits, covers, headsets etc.)
		1.14	Mobile device use in vehicles (typically to be within the law).
		1.15	Limitations on exposing the mobile phone number outside Council requirements
		1.16	Limitations on personal usage of device
		1.17	Users agreements to policy document(s) - Process or policy online agreement system or Code of Conduct/Acceptable Use form signed, or could respond to email with acceptance of an attached policy. May need to itemise devices, services, exceptions, specific to user.
		1.18	Failure to comply statements and details depending on violation.
2	**Additional Policy Components for User-Owned Devices (BYOD).**	2.1	Eligibility for BYOD. May state restrictions based on roles.
		2.2	BYOD Request and Approval Process.
		2.3	Device restrictions, support limitations. Backup responsibilities. (If different from above).
		2.4	Agreement to accept Management and Security rules, tools and configuration by IT Department including other apps to be installed, enabling some features, disabling others. Agreement not to change the business settings and to provide passwords if required for business access to the device for specified reasons. This may mean some relaxation of MDM rules above for allowing users to install apps without requiring approval.
		2.5	Device Purchase process: Subsidy allowance or partial reimbursement. Frequency and timing for upgrades and replacements if lost or stolen.
		2.6	Voice/Data/SMS Charges for BYOD - Reimbursement options, if any.
		2.7	Responsibilities & Liabilities, Violation actions, failure to comply statements and details
		2.8	Contract changes and cancellations - fees/penalities - responsibilities
		2.9	Decommissioning device procedure on changing device, leaving organisation, termination, pro-rata charges calculations. Ownership of purchased apps. Reimbersed by business.
		2.10	Limitations on personal usage of device approved for business
		2.11	Conditions of business access to device, monitoring, wiping etc. Agreement on disclaimer for loss of personal data and purchased apps when organisation wipes device.
		2.12	Rules on other users access to owned device

5.4. Health, Safety and Mobile Devices

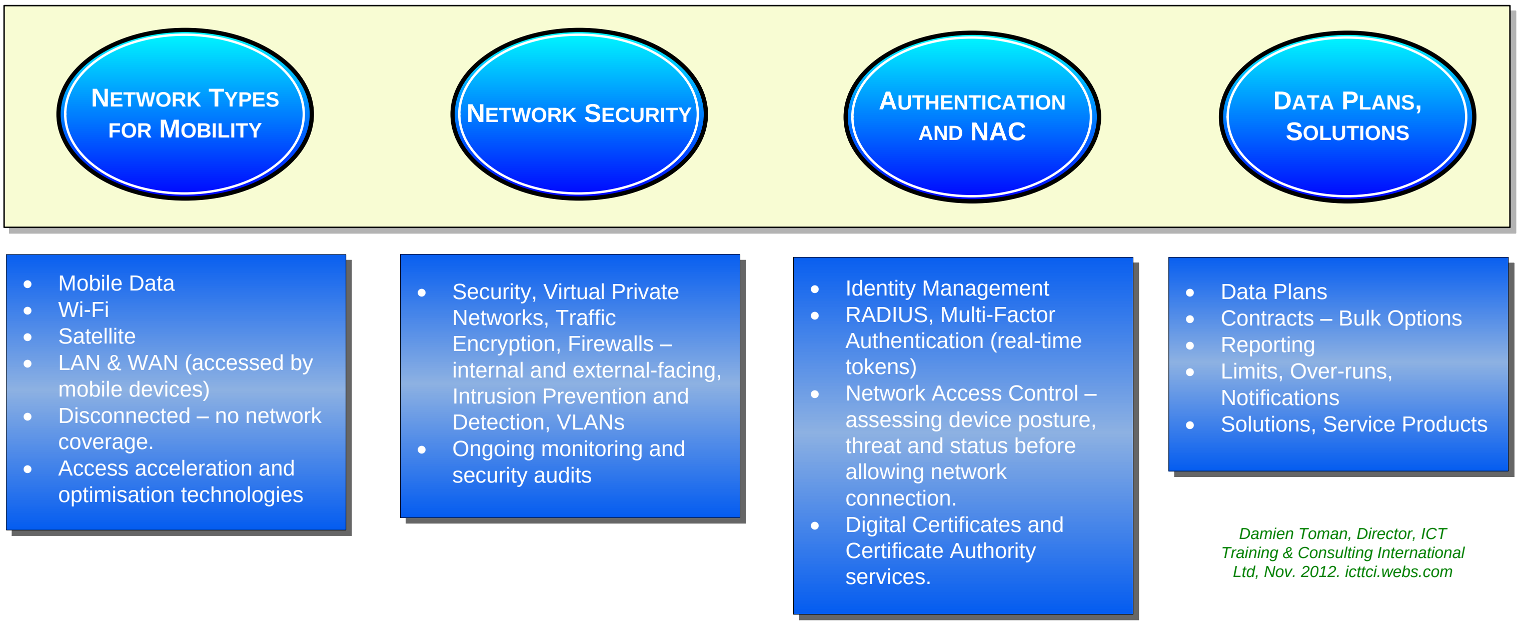
Last month (Oct 2012) The Supreme Court of Italy granted compensation to a worker after he developed a tumour which he claimed was caused by radiation from intensive use of a mobile phone for 12 years. Many radiation authorities and many long-term studies do not support the view that the radiation impacting the head can cause cancer.

If you use your mobile phone for long periods it may be worth considering a Bluetooth wireless ear device as a precautionary measure (see Wikipedia).

Mobile device use in vehicles needs to be within the law and the Mobile Device Policy should clearly state this.

6. Networks, Access Management & Security for Mobility

In this section we will look at connectivity using mobile devices, the options available, how we can provide secure access and some considerations on usage.



Network Types for Mobility

- Mobile Data
- Wi-Fi
- Satellite
- LAN & WAN (accessed by mobile devices)
- Disconnected – no network coverage.
- Access acceleration and optimisation technologies

Network Security

- Security, Virtual Private Networks, Traffic Encryption, Firewalls – internal and external-facing, Intrusion Prevention and Detection, VLANs
- Ongoing monitoring and security audits

Authentication and NAC

- Identity Management
- RADIUS, Multi-Factor Authentication (real-time tokens)
- Network Access Control – assessing device posture, threat and status before allowing network connection.
- Digital Certificates and Certificate Authority services.

Data Plans, Solutions

- Data Plans
- Contracts – Bulk Options
- Reporting
- Limits, Over-runs, Notifications
- Solutions, Service Products

Damien Toman, Director, ICT Training & Consulting International Ltd, Nov. 2012. icttci.webs.com

A major challenge is that the scale of many Local Government organisations can hardly justify the investment in sophisticated security solutions that require significant expertise to implement and ongoing expertise to maintain. At the same time, they are obliged to be aware of and abide by the government guidelines:

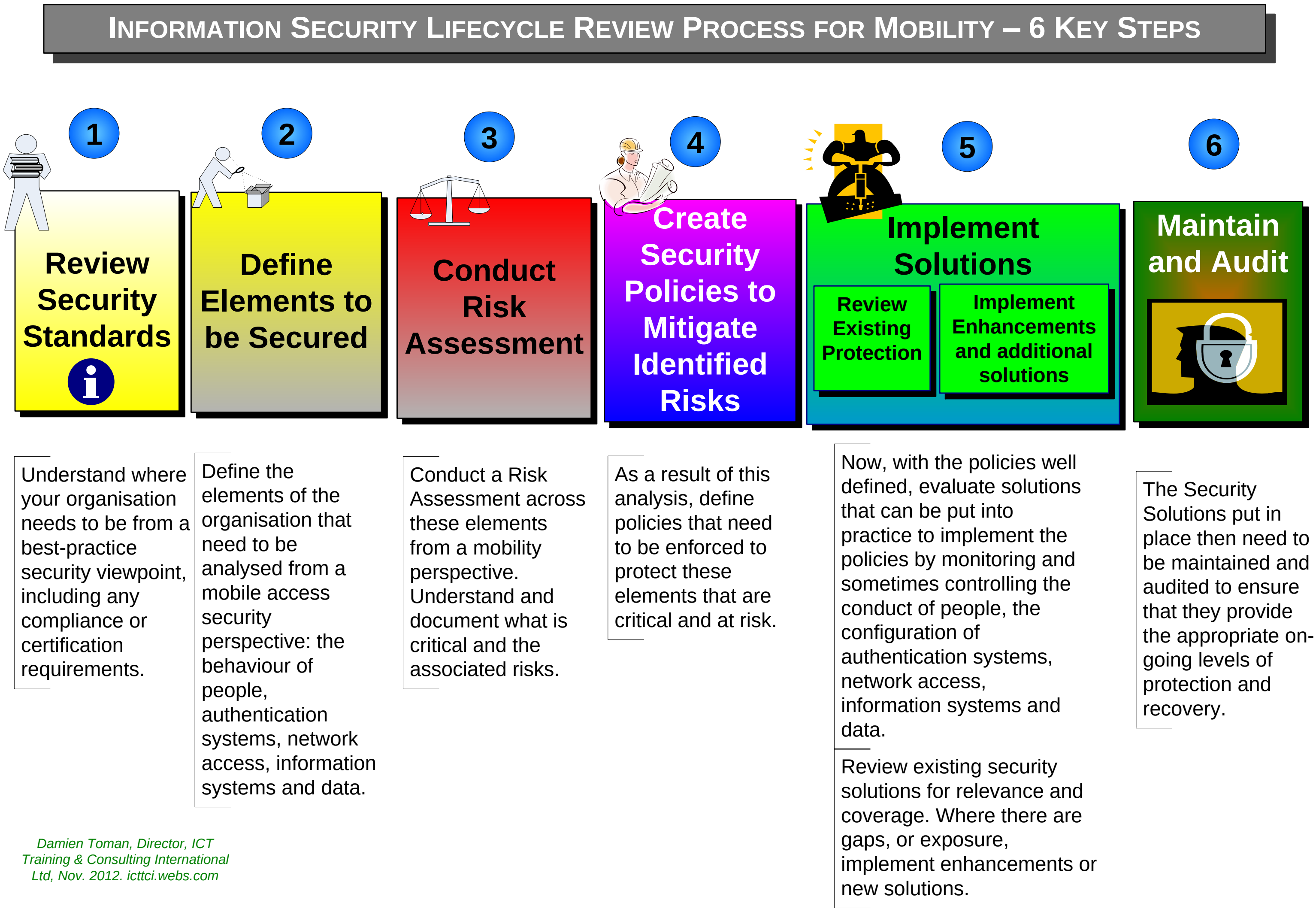
> *"The New Zealand Information Security Manual (NZISM) is the national baseline technical security policy, describing baseline and minimum mandatory technical security standards for government departments and agencies." Government Communications Security Bureau June 2011."* (a very large document).

The good news is that these new Smartphones and Tablet devices are typically much more secure than the laptops that we have all been using for years. That is especially true if the hard disk drives on the laptops are not encrypted (many, if not most, are not encrypted). Also, while more Shared Services options are being implemented, there is the possibility of implementing Cloud-based Security Services for Local Government.

We will start with an overview of a security lifecycle review process, with particular reference to mobility. This is a good place to start before rushing into specific solutions.

6.1. Information Security Lifecycle Review Process

It is important to review the latest requirements for security in The New Zealand Information Security Manual, particularly relating to network access for mobile devices. Some approaches will be considered "best practice" but it is important to at least satisfy the minimum requirements if you are a small Council.



INFORMATION SECURITY LIFECYCLE REVIEW PROCESS FOR MOBILITY – 6 KEY STEPS
1
Review Security Standards
2
Define Elements to be Secured
3
Conduct Risk Assessment
4
Create Security Policies to Mitigate Identified Risks
5
Implement Solutions
Review Existing Protection
Implement Enhancements and additional solutions
6
Maintain and Audit

Understand where your organisation needs to be from a best-practice security viewpoint, including any compliance or certification requirements.

Define the elements of the organisation that need to be analysed from a mobile access security perspective: the behaviour of people, authentication systems, network access, information systems and data.

Conduct a Risk Assessment across these elements from a mobility perspective. Understand and document what is critical and the associated risks.

As a result of this analysis, define policies that need to be enforced to protect these elements that are critical and at risk.

Now, with the policies well defined, evaluate solutions that can be put into practice to implement the policies by monitoring and sometimes controlling the conduct of people, the configuration of authentication systems, network access, information systems and data.

Review existing security solutions for relevance and coverage. Where there are gaps, or exposure, implement enhancements or new solutions.

The Security Solutions put in place then need to be maintained and audited to ensure that they provide the appropriate on-going levels of protection and recovery.

Damien Toman, Director, ICT Training & Consulting International Ltd, Nov. 2012. icttci.webs.com

Next we can then tackle the elements of the organisation that need to be considered from a mobility and network perspective. This includes not just the data files and data access systems but also the behaviour of users (the Policy Components listed earlier can indicate many of those elements).

Once all the key elements have been defined, then a risk assessment can be conducted across those elements, with particular emphasis on those elements rated as being most critical, and most sensitive, to the organisation.

Now, after the risk assessment, is the time to tackle policy. Policy should not be the starting point, as policies should be specifically designed to mitigate the identified and documented risks, with emphasis on those most critical elements.

Once the desired policies have been identified, then your existing security solutions should be analysed, particularly in terms of mobility, and the security relating to new devices that will be connected. The solutions-set should help mitigate the identified risks. There will likely be a gap between what worked before as a set of security solutions and what will work downstream as you deliver your Mobility Strategy. This defined gap should be used as a basis for evaluating solutions available to provide the required level of protection, to meet the government guidelines and to minimise the investment required to deliver a solution.

Perfect security does not exist. You could try to implement every conceivable security option, invest more than the Council can afford, and still have problems. The mitigation of identified risks should be your guide. Spend as little as possible to achieve what is required. Having completed the earlier analysis, you will have weighed-up where the critical elements lie.

Once the new or enhanced security solutions have been implemented, then they can be audited and tested to understand how well they do help enforce the policies, the behaviours, and the management of who has access to what information.

Finally, when all is implemented and tested, and looks good, the work is not done! This is an on-going battle. The bad guys around the world, and possibly within your own organisation, keep coming up with new ways to work around security systems (the recent kiosk issue in NZ may be a good example). A well-defined on-going documented maintenance procedure to ensure that systems are kept updated and patched from the latest vulnerabilities is required. All changes should be tested. Recovery procedures should also be documented. This includes recovery from breached or failed systems.

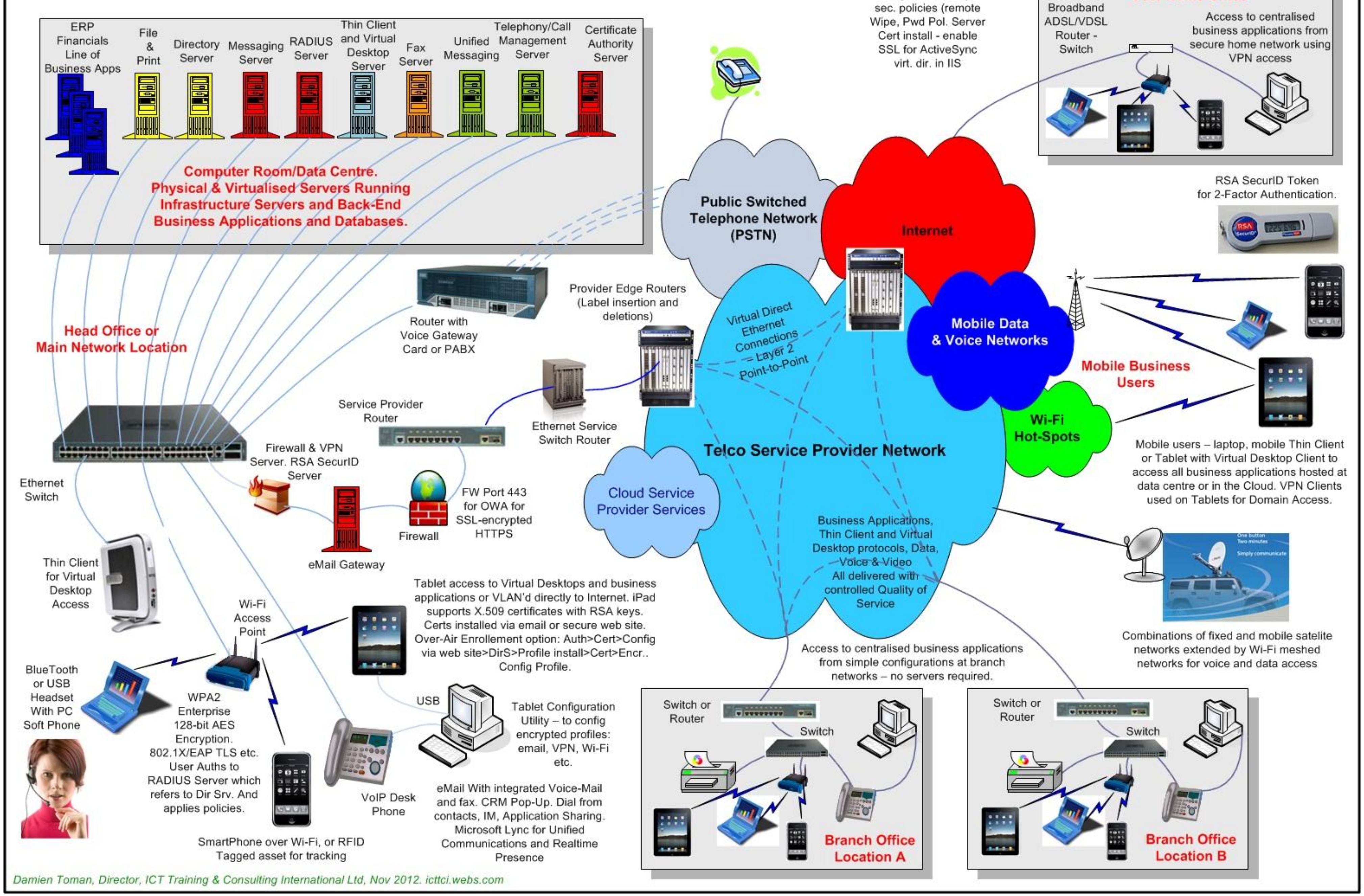
6.2. Overview of a Multi-Site Network with Security for Mobility

The following network diagram illustrates the key components of a multi-site network implementation. It shows the main business office with computer room (or Data Centre) housing the application and infrastructure servers. It also shows connectivity to remote sites via a service-provider network. In this particular instance, as many do today, the remote sites utilise the data centre servers to minimise equipment required at each site. Depending on the applications architecture, and the network bandwidth available, a Virtualisation approach like this, (using Citrix technology, for instance, as some Councils do already) rather than a Client-Server approach, keeps remote sites simple to manage and lowers the Total Cost of Ownership.

Office workers who are sometimes home office teleworkers can also be integrated to all the back-end applications over secure VPN links via their (typically) wired broadband connection (ADSL/VDSL).

The next category, the mobile users, is a key focus here. With more users having access to mobile devices, the Mobile Data Networks and Wi-Fi networks becoming more accessible, faster and cheaper, this is the inevitable strategic growth area for business and a path to more engaged users and better productivity. The security solutions required are also a key consideration to pave the way for this new world to unfold without causing havoc in the business.

Network Access Management & Security for Mobility



ERP Financials Line of Business Apps
File & Print
Directory Server
Messaging Server
RADIUS Server
Thin Client and Virtual Desktop Server
Fax Server
Unified Messaging
Telephony/Call Management Server
Certificate Authority Server
Computer Room/Data Centre. Physical & Virtualised Servers Running Infrastructure Servers and Back-End Business Applications and Databases.
Head Office or Main Network Location
Ethernet Switch
Thin Client for Virtual Desktop Access
BlueTooth or USB Headset With PC Soft Phone
Wi-Fi Access Point
Router with Voice Gateway Card or PABX
Service Provider Router
Firewall & VPN Server. RSA SecurID Server
eMail Gateway
Firewall
FW Port 443 for OWA for SSL-encrypted HTTPS
Ethernet Service Switch Router
Provider Edge Routers (Label insertion and deletions)
Public Switched Telephone Network (PSTN)
Internet
Mobile Data & Voice Networks
Wi-Fi Hot-Spots
Mobile Business Users
Telco Service Provider Network
Virtual Direct Ethernet Connections – Layer 2 Point-to-Point
Cloud Service Provider Services
USB
VoIP Desk Phone
User Home Office
Broadband ADSL/VDSL Router - Switch
Switch or Router
Switch
Branch Office Location A
Branch Office Location B

WPA2 Enterprise 128-bit AES Encryption. 802.1X/EAP TLS etc. User Auths to RADIUS Server which refers to Dir Srv. And applies policies.

SmartPhone over Wi-Fi, or RFID Tagged asset for tracking

Tablet access to Virtual Desktops and business applications or VLAN'd directly to Internet. iPad supports X.509 certificates with RSA keys. Certs installed via email or secure web site. Over-Air Enrollement option: Auth>Cert>Config via web site>DirS>Profile install>Cert>Encr.. Config Profile.

Tablet Configuration Utility – to config encrypted profiles: email, VPN, Wi-Fi etc.

eMail With integrated Voice-Mail and fax. CRM Pop-Up. Dial from contacts, IM, Application Sharing. Microsoft Lync for Unified Communications and Realtime Presence

For MS Exchange: Configure ActiveSync sec. policies (remote Wipe, Pwd Pol. Server Cert install - enable SSL for ActiveSync virt. dir. in IIS

Access to centralised business applications from secure home network using VPN access

RSA SecurID Token for 2-Factor Authentication.

Mobile users – laptop, mobile Thin Client or Tablet with Virtual Desktop Client to access all business applications hosted at data centre or in the Cloud. VPN Clients used on Tablets for Domain Access.

Business Applications, Thin Client and Virtual Desktop protocols, Data, Voice & Video All delivered with controlled Quality of Service

Combinations of fixed and mobile satelite networks extended by Wi-Fi meshed networks for voice and data access

Access to centralised business applications from simple configurations at branch networks – no servers required.

Damien Toman, Director, ICT Training & Consulting International Ltd, Nov 2012. icttci.webs.com

This example diagrammatic network accomodates mobile users in the office over Wi-Fi, providing flexibility to move around the office, discuss what is on the device screen with colleagues, be connected in meetings without tripping over wires or having to wire meeting rooms with many Ethernet sockets, access from lunch or rest areas, and may even extend to the closest café. Combining multiple antennae and multiple radios in access points allows high density usage (MIMO – Multi-In, Multi Out).

When beyond the reach of that Wi-Fi, users can access service provider Mobile Data Networks for voice and data access, providing connectivity in most populated areas.

When in remote areas, or when other networks are not available, (as a result of damage from storms, floods, earthquakes, fires and even volcanos) satelite network services can be very useful. Napier today has a trailer fully equiped with a satelite dish to allow wired and wireless networks to be set up at short notice and use satelite services for voice and data. It makes sense to have such services available in a few suitable areas around New Zealand, to deal with emergencies. A few trailers in each island could cover a very wide area.

Most Councils have at least access to a satelite phone. Not many have mobile voice and data access via satelite. A few have a “Satelite in a Suitcase” solution which could work very well from a truck or 4WD and provide Wi-Fi around the vehicle for voice and data for multiple emergency services staff.

Another important development, mentioned earlier, is free metro Wi-Fi deployment. Even these free, open, Wi-Fi Internet services, can provide very secure access to business systems through the use of Virtual Private Networks and strong authentication, providing full encrypted traffic between the device user and the back end systems. We will now explore some examples of how that security can be implemented.

6.3. Identity Management, Authentication and Network Access Control

Identity Management and Single Sign-On

Identity is a challenge in any ICT systems environment, regardless of mobility requirements. Mobility just adds to the challenge. Users typically have many different passwords for access to different systems. Directory services and single-sign-on solutions can help manage these complex environments with an aim to reduce support costs, provide better security and easier access to information, in multiple systems, for authenticated users. It can ease the burden of setting up new recruits and quickly removing access for employees who leave, without duplication of effort caused by setting the user up on every system they need access to.

The issue is that it is often difficult and expensive to implement. Often many applications and databases cannot easily be made to synchronise with the master “meta” directory and therefore the SSO concept falls down – it is often just not feasible. Smaller Councils would also not be able to justify investments in such elaborate solutions.

So, the solution is usually to challenge a user to authenticate with just username and password. This may be made much more secure by implementing a two-factor authentication solution where the user is also challenged to provide a pin-number or code from a token device (often a key-ring with small display of a code that changes every few minutes in line with back-end servers that will have the same code at that moment – see network diagram).

Network Access Control

A further important security measure can be implemented to check the "posture" of devices attempting to connect to the network. If the device operating system is not up-to-date with security patches, or the anti-malware software is not up-to-date with the latest signatures (all this information is available from reading the registry database, or equivalent, on the user device), the device may be pointed directly to a remediation server, or the Internet, for the updates to be made before access is granted. If the device looks like it is infected (identification of suspicious code, services or software), it can be quarantined (VLAN'd to a web server that explains the process to follow) and not allowed to connect (the user may have been accessing web sites from home that have installed malware on the laptop, for instance). All these activities are logged, monitored and alerts generated to administrators depending on the severity of the issue.

If the posture of the device is not checked, then there are major risks of malware outbreaks on the network as the user will be authenticated, from inside the network (if in the office) and will have avoided the scrutiny of the perimeter protection servers (which will often include Intrusion Prevention & Detection services as well as Firewalling).

Once authentication has taken place, the policies for that user (in the user Profile stored on the directory server) will grant access to the services and applications that the user has been set up to access - sometimes provided through a user group access policy.

Many solutions require a software agent to be installed on the device (supporting the 802.1x protocol standard). For some BYOD implementations, where it would be too much of a burden to provision each user individually, or implement a Mobile Device Management solution, an agentless solution can be deployed by having the user agree to a web-based interrogation of their device to check for malware. Only user devices that passed the check would be granted access.

Cisco solutions are very mature at "Network Admission Control" (their terminology for Network Access Control) in this area but will be most suitable for larger organisations. Some specific solutions, for instance, can be provided by niche approaches from vendors like AeroHive (see later) that suit small implementations but can also grow with only incremental investments.

RADIUS (Remote Authentication Dial-In User Service)

RADIUS is a client/server protocol for security management. A RADIUS server provides Authentication of users, Authorisation to access specific network services and records the user usage of those services (Accounting). This is often referred to as triple-A services (AAA). A Windows Server can provide RADIUS services. The RADIUS Server will typically (these days) access the Windows Active Directory Server to authenticate the user-provided username and password.

The RADIUS server authenticates Wi-Fi Access Points and creates the cryptographic keying material as part of the Wi-Fi Protected Access v2 process (Enterprise WPA2, 802.11i standard). This is important for allowing only approved Access Points to operate on the LAN.

Digital Certificates

A Digital Certificate is a standards-based (typically X.509) electronic signing arrangement that uses public and private keys, derived from multiple information sources (like username, password, organisation etc.) and used like an ID card. A Digital Certificate is provided by a Certificate Authority server (Microsoft Windows Servers can provide Certificate Authority services). Data that is encrypted using one key can only be decrypted using the other key. The key pair is time-stamped so that it expires and is replaced periodically to enhance security.

> *"The sender obtains the recipient's public key from a directory service* [such as Active Directory – DT] *and uses it to encrypt the message before sending it. When the message is received, the recipient uses his or her private key to decrypt the message. As long as the private key is kept secure, no other user can decrypt the message and the recipient is assured that the transmission hasn't been tampered with."* Microsoft.

Digital Certificates are used to allow secure authentication of users to email, Wi-Fi networks, VPNs, and other services, without having to log in each time (to synchronise and receive email updates etc.). They are also used to encrypt network traffic (often over the Internet) between the user and the back end server. Users can be emailed a Certificate, click on it, it asks the user to accept the Certificate, when accepted it then installs the certificate on the user device. Certificates can also be provided from a secured web site. They can also be distributed by Mobile Device Management software.

Mobile Data Networks, Data Plans, Coverage

Use of Mobile Data Networks needs careful consideration of the bandwidth utilisation of various applications, the roaming charges when travelling abroad and the issues around business applications that require connectivity when you are outside the coverage area (no network).

These challenges also raise important questions around choice of delivery architectures for business applications. Keeping all you application installations and data in the Data Centre provides the maximum security, best support model, and the most flexible solution to cope with the growing choice of devices that need access. Tablets and laptops can be effective Thin Clients to back-end Virtual Desktops or Published Applications on the web. This architecture depends on connectivity.

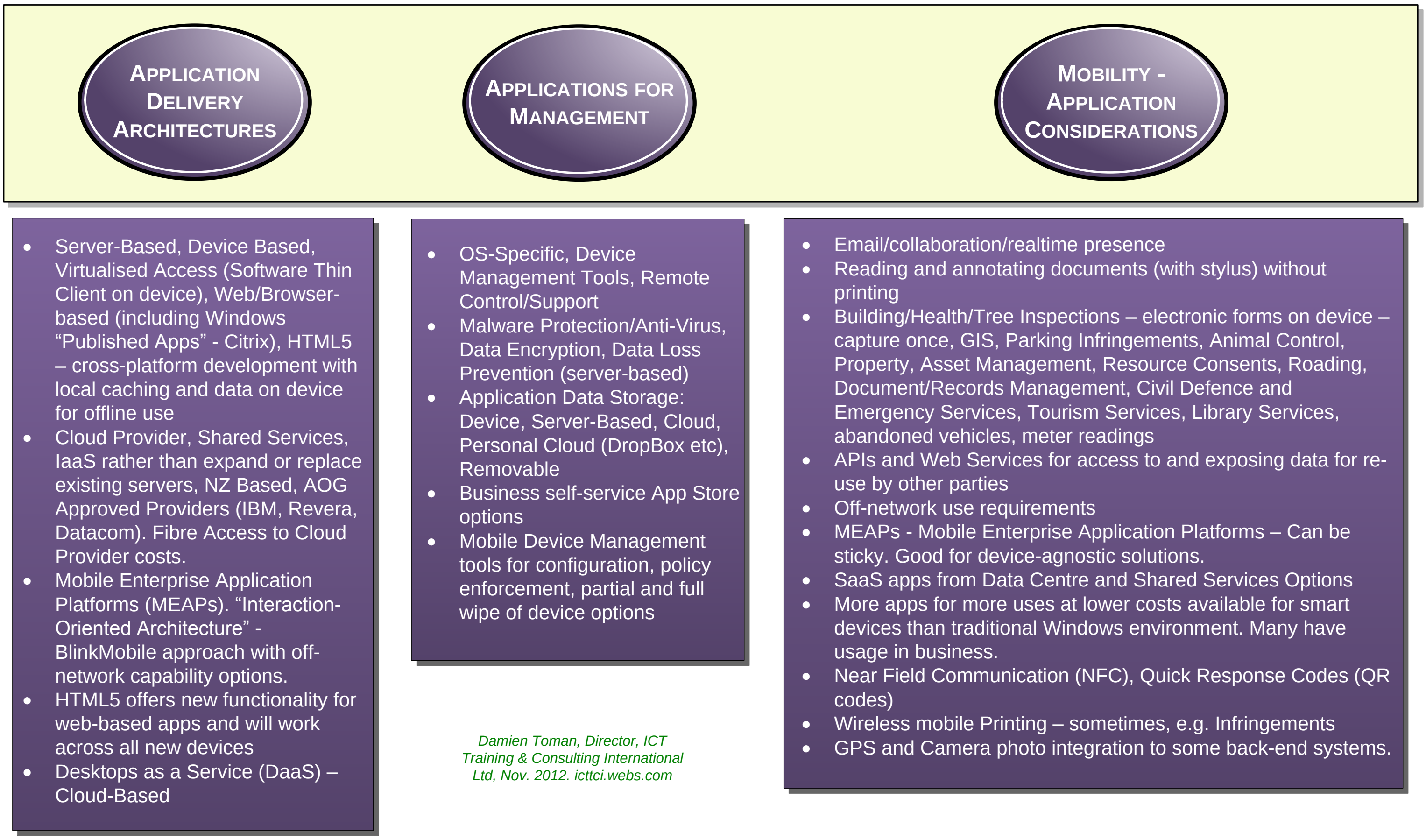
Using some applications, like Skype or video conferencing, over international mobile networks can clock up serious data charges.

Some service providers offer a Bulk mobile data deal for an organisation. That is a very useful and flexible option but how will that work for a BYOD user?

The architecture, data and applications delivery choices, for connected and disconnected use, will be discussed in the next section.

7. Applications, Delivery Architectures, Management and Data

With any form of network connectivity, there are many options for delivering information systems to mobile users. We will look at those options in this section. We will also look at the challenge of providing mobile applications, and data access, when outside network coverage. This is a requirement for many field workers in some locations.



APPLICATION DELIVERY ARCHITECTURES

- Server-Based, Device Based, Virtualised Access (Software Thin Client on device), Web/Browser-based (including Windows "Published Apps" - Citrix), HTML5 – cross-platform development with local caching and data on device for offline use
- Cloud Provider, Shared Services, IaaS rather than expand or replace existing servers, NZ Based, AOG Approved Providers (IBM, Revera, Datacom). Fibre Access to Cloud Provider costs.
- Mobile Enterprise Application Platforms (MEAPs). "Interaction-Oriented Architecture" - BlinkMobile approach with off-network capability options.
- HTML5 offers new functionality for web-based apps and will work across all new devices
- Desktops as a Service (DaaS) – Cloud-Based

APPLICATIONS FOR MANAGEMENT

- OS-Specific, Device Management Tools, Remote Control/Support
- Malware Protection/Anti-Virus, Data Encryption, Data Loss Prevention (server-based)
- Application Data Storage: Device, Server-Based, Cloud, Personal Cloud (DropBox etc), Removable
- Business self-service App Store options
- Mobile Device Management tools for configuration, policy enforcement, partial and full wipe of device options

MOBILITY - APPLICATION CONSIDERATIONS

- Email/collaboration/realtime presence
- Reading and annotating documents (with stylus) without printing
- Building/Health/Tree Inspections – electronic forms on device – capture once, GIS, Parking Infringements, Animal Control, Property, Asset Management, Resource Consents, Roading, Document/Records Management, Civil Defence and Emergency Services, Tourism Services, Library Services, abandoned vehicles, meter readings
- APIs and Web Services for access to and exposing data for re-use by other parties
- Off-network use requirements
- MEAPs - Mobile Enterprise Application Platforms – Can be sticky. Good for device-agnostic solutions.
- SaaS apps from Data Centre and Shared Services Options
- More apps for more uses at lower costs available for smart devices than traditional Windows environment. Many have usage in business.
- Near Field Communication (NFC), Quick Response Codes (QR codes)
- Wireless mobile Printing – sometimes, e.g. Infringements
- GPS and Camera photo integration to some back-end systems.

Damien Toman, Director, ICT Training & Consulting International Ltd, Nov. 2012. icttci.webs.com

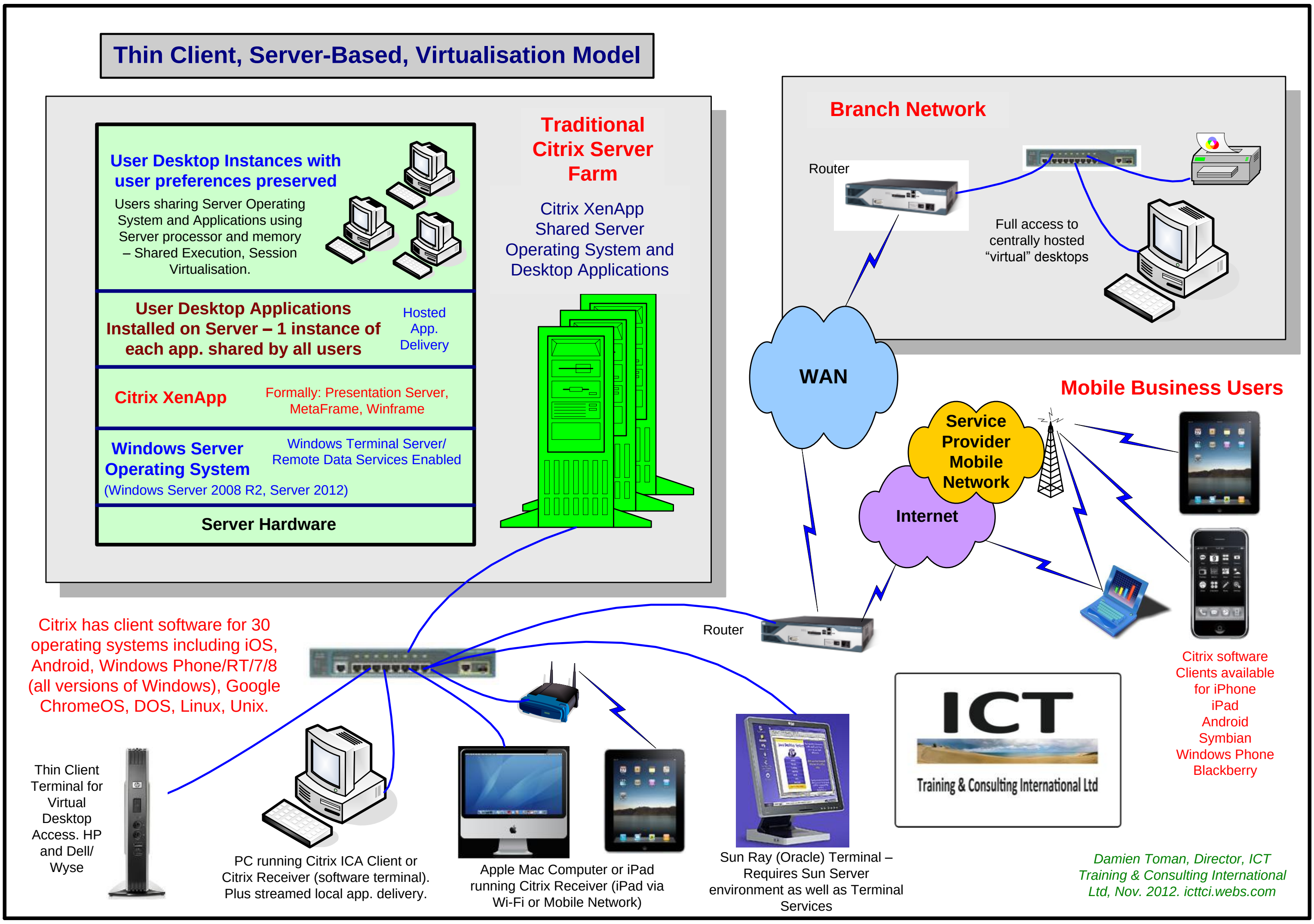
Fortunately many of the application providers, and mobile specialist developers, have developed solutions to allow disconnected mobile use (see Section 9 for updates). This is a particularly exciting area, especially with Smartphones and Tablets for applications delivery. Also new strategic web technologies, like HTML5, can potentially minimise the need for Operating-System-Specific solutions. Most organisations, and most providers, do not want to have three versions of every app (iOS, Android and Windows) if they want to satisfy BYOD and the variety of devices that users will have.

When it comes to enabling applications in the field, few Councils are starting this journey right now. Most have already implemented some mobile solutions. The reason to re-think Mobile Strategy is that there any many more options available now. It is also not just about the application, but also the user, their device preferences, and the business long term options for shared and Cloud-based services.

7.1. Server-Based Computing/Thin Client/Virtual Desktop Infrastructure for Mobility; Benefits and Limitations

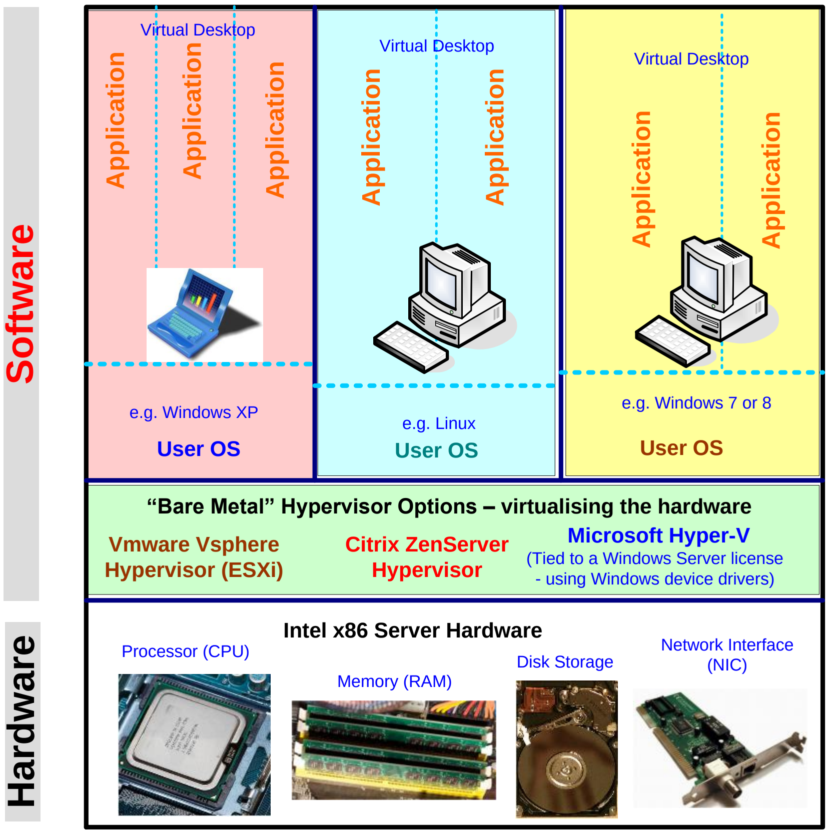
Many Councils' made decisions, years ago, to enable existing applications to be used in the field, without any application software changes, by implementing Server-Based Computing. This is a form of Desktop Virtualisation where each user, say from a laptop with a Citrix Client installed (Thin Client software), can access an instance of a server-based Virtual Desktop. The application runs on the server but the user sees and interacts with it just like when on the wired network in the office. This approach still has many advantages today, as all the application installation and data stays securely in the Data Centre. Nowadays the Thin Client software can run on a Tablet, even a Smartphone (needs a large screen), and have access to the same full Windows 32-bit or 64-bit desktop.

The desktop is not running Windows XP, Vista, Windows 7 or Windows 8. It is running a user-specific instance of a desktop on the Windows Server operating system. This was called Winframe, Metaframe or Presentation Server (name changes over the years). It is now called XenApp and uses the Windows Terminal Services feature of Windows Servers to make the operating system multi-user. (See diagram below).


Thin Client, Server-Based, Virtualisation Model
User Desktop Instances with user preferences preserved
Users sharing Server Operating System and Applications using Server processor and memory – Shared Execution, Session Virtualisation.
User Desktop Applications Installed on Server – 1 instance of each app. shared by all users
Hosted App. Delivery
Citrix XenApp
Formally: Presentation Server, MetaFrame, Winframe
Windows Server Operating System
Windows Terminal Server/ Remote Data Services Enabled
(Windows Server 2008 R2, Server 2012)
Server Hardware
Traditional Citrix Server Farm
Citrix XenApp Shared Server Operating System and Desktop Applications
Branch Network
Router
Full access to centrally hosted "virtual" desktops
WAN
Mobile Business Users
Service Provider Mobile Network
Internet
Router
Citrix has client software for 30 operating systems including iOS, Android, Windows Phone/RT/7/8 (all versions of Windows), Google ChromeOS, DOS, Linux, Unix.
Citrix software Clients available for iPhone iPad Android Symbian Windows Phone Blackberry
Thin Client Terminal for Virtual Desktop Access. HP and Dell/ Wyse
PC running Citrix ICA Client or Citrix Receiver (software terminal). Plus streamed local app. delivery.
Apple Mac Computer or iPad running Citrix Receiver (iPad via Wi-Fi or Mobile Network)
Sun Ray (Oracle) Terminal – Requires Sun Server environment as well as Terminal Services
ICT
Training & Consulting International Ltd
Damien Toman, Director, ICT Training & Consulting International Ltd, Nov. 2012. icttci.webs.com

More recently, with Virtual Desktop Infrastructure (VDI), multiple Windows 7 desktops (including XP, Vista or 8) can run as Virtual Machines on a server, using VMware, Citrix or Microsoft Hypervisor technology. This enables many discreet user desktop Virtual Machines based in the Data Centre or Cloud. A user can have an iPad, Android or Windows RT Tablet, or a Google Chromebook, or even a large phone (Samsung Galaxy Note II) and have access to a full Windows 7 desktop with all the business applications that can run in the office.

Virtual Desktop Infrastructure – VDI



Running Multiple Virtual Desktops accessed via New Protocols that handle multimedia and HD Graphics - Enabling Richer Virtual Desktops

- **Citrix HDX or ICA**
- **Vmware PCoIP**
- **Microsoft's RDP or Remote FX**

Single Physical Server Hardware

Damien Toman, Director, ICT Training & Consulting International Ltd, Nov. 2012. icttci.webs.com

There are two main **challenges** with these Virtualisation approaches:

1. You need connectivity

2. Tablets and Smartphones, without mice, behave differently and not all users will be comfortable with that. Tablets do work pretty well, but the user may need to learn a few new swipe gestures and keyboard short-cuts. Some users find a Bluetooth keyboard very useful if doing much data input.

There are however, significant benefits to using Virtual Desktops:

1. Once you have the server infrastructure in place, any user can easily be given mobile access to all or some business applications. Even office-based users don't need a PC. They can have an inexpensive Windows Terminal (hardware Thin Client made by HP and Wyse/Dell).

2. All data is secure in the Data Centre. No data is stored on the device.

3. No Mobile Device Management server and Client software really needs to be purchased or implemented.

4. Set up an application once on the server and make it available to all users or specific groups – easiest form of management.

5. All application and desktop OS patches are done by the ICT engineers/Admins without touching the device.

6. ICT Support staff can take control of a user's desktop environment (if they agree) and help walk them through problem resolution, minimising support costs.

7. You have full compatibility with all your existing applications and no new apps for mobility are necessary.

8. This is a low-risk way to migrate to Windows 7 or 8 desktops, without wiping out the user's current operating system configuration. A Virtual desktop cam be created from a current physical machine.

9. Susan Souren, Taupo District Council, says they have enabled mobile access to all their applications using Citrix XenApp over a Virtual Private Network. Peter Darlington, Tasman District Council, says they also use Citrix XenApp for remote access to all applications and use Citrix Netscaler for optimised secure remote access (a Citrix-tuned SSL-VPN that also provides load balancing and application acceleration).

US federal government Digital Services Advisory Group, Aug 2012:

> *"The Alcohol and Tobacco Tax and Trade Bureau (TTB) decided to reduce the costs, time and effort required to refresh desktop and laptop computers used for client computing needs. TTB has a widely dispersed workforce with many personnel working from home full time and over 80 percent of the workforce regularly teleworking. Replacing desktop and laptop computers every 3 to 4 years cost TTB about $2 million and disrupted the IT program and business users for several months. TTB determined that the best solution was to centralize all client computing power and applications, user data, and user settings and allow access to TTB resources by thin client computing devices. A thin client is a computing device or program that relies on another device for computational power. Currently about 70 percent of TTB personnel use thin client devices to access all TTB applications and data.*
>
> *TTB desktop and laptop computers were due for refresh this year. However, the virtual desktop solution allowed TTB to avoid the expense of replacing hardware. The savings*

achieved paid for TTB's virtual desktop implementation—which cost approximately $800,000—and saved TTB $1.2 million.

The rapid pace of change in the mobile device market makes the virtual desktop solution particularly attractive. Because no data touches the user device, there is no need for a mobile device management (MDM) solution on a non-TTB device.

The final result, which is likely the greatest benefit of the TTB Virtual Desktop solution relative to BYOD, is the ***minimization or elimination of complex legal and policy issues****. Because* ***no data touches the BYOD device*** *and no work is physically accomplished on the BYOD equipment, all requests for discovery of information from a user's computer can be satisfied without having to recover anything from the user's personal device."*

Solution:

VMware for server virtualization

Citrix XenDesktop, XenApp, XenClient (pilot), Receiver, Citrix Provisioning Services

Citrix Netscalers for remote access

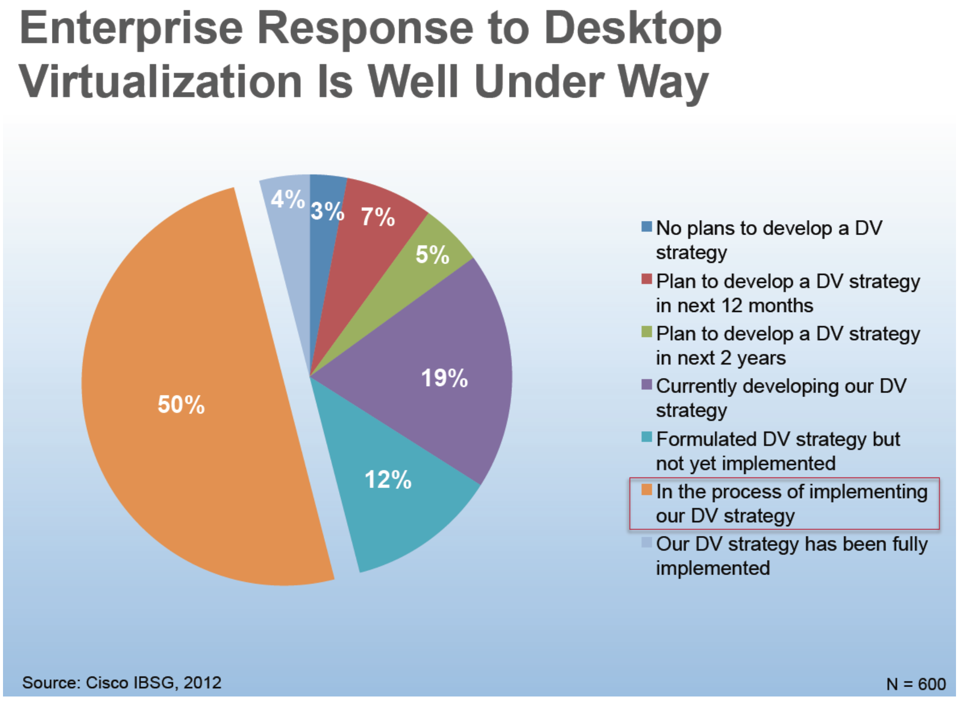
Desktops as a Service (DaaS):

"global legal services leader Foley & Lardner LLP has adopted virtual desktops and bring-your-own-device (BYOD) to enhance end-user productivity"

"The real underlying benefit is being able to securely deliver the desktop as a service (DaaS). We are no longer tied to a physical desktop"

By Dana Gardner for BriefingsDirect August 2012

Cisco 2012:



Enterprise Response to Desktop Virtualization Is Well Under Way

Source: Cisco IBSG, 2012

N = 600

After considering Virtual Desktop options, the next options to consider are web-based and native development environments for applications delivery.

7.2. Mobility Application Development Choices

Web-Based Applications and HTML5

For applications that already provide a web-based interface, browsers on the devices provide easy access. Not all browsers are compatible with all web-based applications, so testing is required before any roll-out. iOS, for instance, does not support Adobe Flash which is used by many web sites. Some web sites require specific plug-ins or downloaded code to be in the browser – this can make some applications only function correctly with not only a specific browser, but even a specific version of a browser (Internet Explorer is a good example). Many business applications developed for IE6 will not work with later versions (application Virtualisation can be a good way around this problem – using Citrix XenApp, VMware ThinApp or App-V from Microsoft).

The issue of requiring connectivity for web-based applications remains. This can mean that in some locations it is just not possible to run the business application on a mobile device.

HTML5 promises to help address some of the limitations of web-based applications requiring network connectivity. It is supported by all the latest device platforms and therefore will allow an application to be developed once and run on all. It also supports disconnect mode and local storage access, via a local cache, when no network is available. Even Adobe (Flash provider) now realises that HTML5 is the future and many of the Council applications vendors are moving along the HTML5 path (see later for provider updates).

Another benefit of using HTML5 is that an app does not have to be installed on the device (from an app store).

Some challenges remain for HTML5 apps. Performance will not be as good as a native app. (Facebook struggled to make an HTML5 app with acceptable performance – they abandoned that approach and developed native apps). Also, HTML5 is new and many older devices and browsers may not support it. Some device features will not be available to HTML5 apps – for instance GPS and camera functionality. With these limitations, native apps will still be required for some business applications, though more Web Services and APIs are being developed to work around these issues over time. The wide choice of browsers with different feature-sets is also an on-going battle for mobile devices and HTML5 apps.

Some development tools encourage a structured development approach where a common code base can be created and adapted to each native environment.

Native Apps for Mobile Devices

Native apps developed for each device platform and form-factor will provide the best user experience. The issue is cost and expertise. If organisations decide to tread the native path, they should consider standardising on a particular device or platform. This will be at odds with some users and their preferences. One approach would be to have a general broad BYOD strategy for the organisation but with limited choices for specific roles where apps need to be deployed.

MEAPs

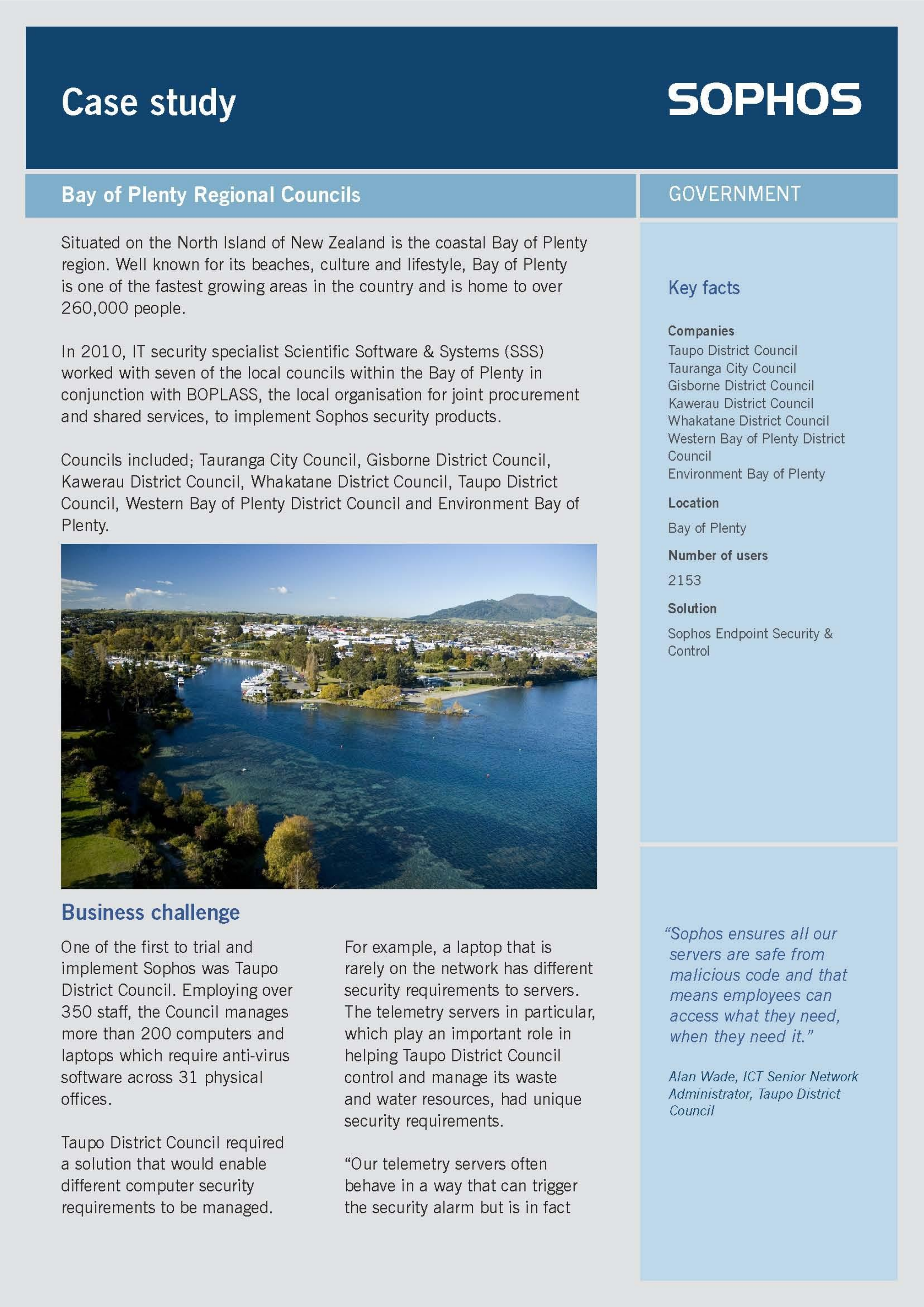
Mobile enterprise application platforms are another approach to dealing with many platforms, front and back-end systems. The approach uses middleware services to make it easier to access back-end business applications securely and from multiple devices. SAP (with Sybase Unwired Platform) and BlinkMobile offer this approach (see case studies later in this paper). It speeds up the development of the client-side applications and minimises the expertise required to build apps (4GL development tools are typically used rather than native coding for specific devices). They support both native and HTML5 approaches and can utilise local device storage for disconnected use. A MEAP solution should be considered if the organisation has strategic plans to create many mobile apps.

> *"The Gartner Group predicts that by 2015 mobile app development projects will outnumber native PC projects by a ratio of 4-to-1." Cimarron Buser, Apperian*

Next we will look at some Case Studies for various deployments of mobile solutions.

8. Local Government Mobility Case Studies

8.1. Bay of Plenty Regional Councils – Sophos



Case study

SOPHOS

Bay of Plenty Regional Councils

GOVERNMENT

Situated on the North Island of New Zealand is the coastal Bay of Plenty region. Well known for its beaches, culture and lifestyle, Bay of Plenty is one of the fastest growing areas in the country and is home to over 260,000 people.

In 2010, IT security specialist Scientific Software & Systems (SSS) worked with seven of the local councils within the Bay of Plenty in conjunction with BOPLASS, the local organisation for joint procurement and shared services, to implement Sophos security products.

Councils included; Tauranga City Council, Gisborne District Council, Kawerau District Council, Whakatane District Council, Taupo District Council, Western Bay of Plenty District Council and Environment Bay of Plenty.

Business challenge

One of the first to trial and implement Sophos was Taupo District Council. Employing over 350 staff, the Council manages more than 200 computers and laptops which require anti-virus software across 31 physical offices.

Taupo District Council required a solution that would enable different computer security requirements to be managed.

For example, a laptop that is rarely on the network has different security requirements to servers. The telemetry servers in particular, which play an important role in helping Taupo District Council control and manage its waste and water resources, had unique security requirements.

"Our telemetry servers often behave in a way that can trigger the security alarm but is in fact

Key facts

Companies

Taupo District Council
Tauranga City Council
Gisborne District Council
Kawerau District Council
Whakatane District Council
Western Bay of Plenty District Council
Environment Bay of Plenty

Location

Bay of Plenty

Number of users

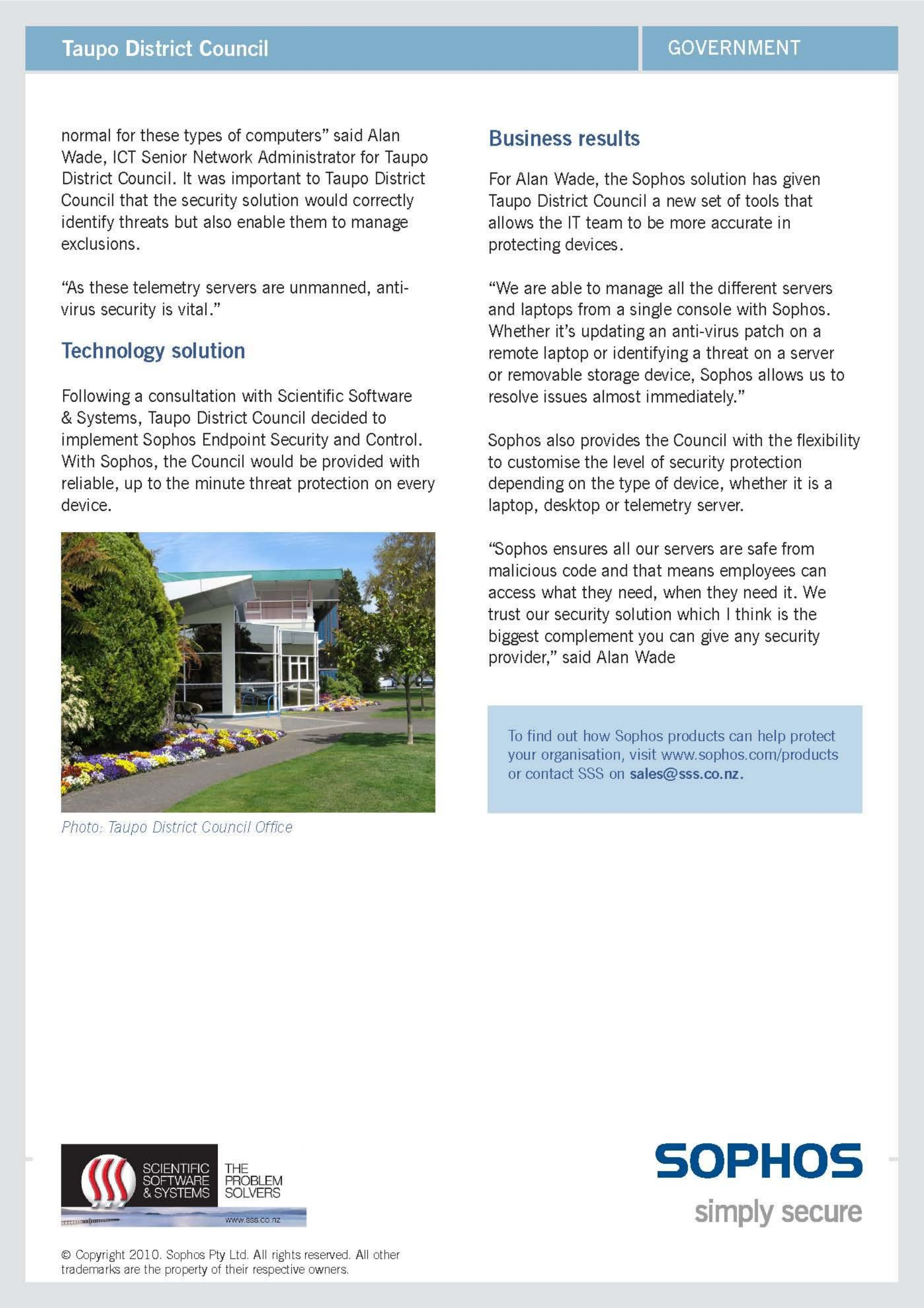
2153

Solution

Sophos Endpoint Security & Control

"Sophos ensures all our servers are safe from malicious code and that means employees can access what they need, when they need it."

Alan Wade, ICT Senior Network Administrator, Taupo District Council



Taupo District Council | GOVERNMENT

normal for these types of computers" said Alan Wade, ICT Senior Network Administrator for Taupo District Council. It was important to Taupo District Council that the security solution would correctly identify threats but also enable them to manage exclusions.

"As these telemetry servers are unmanned, anti-virus security is vital."

Technology solution

Following a consultation with Scientific Software & Systems, Taupo District Council decided to implement Sophos Endpoint Security and Control. With Sophos, the Council would be provided with reliable, up to the minute threat protection on every device.

Photo: Taupo District Council Office

Business results

For Alan Wade, the Sophos solution has given Taupo District Council a new set of tools that allows the IT team to be more accurate in protecting devices.

"We are able to manage all the different servers and laptops from a single console with Sophos. Whether it's updating an anti-virus patch on a remote laptop or identifying a threat on a server or removable storage device, Sophos allows us to resolve issues almost immediately."

Sophos also provides the Council with the flexibility to customise the level of security protection depending on the type of device, whether it is a laptop, desktop or telemetry server.

"Sophos ensures all our servers are safe from malicious code and that means employees can access what they need, when they need it. We trust our security solution which I think is the biggest complement you can give any security provider," said Alan Wade

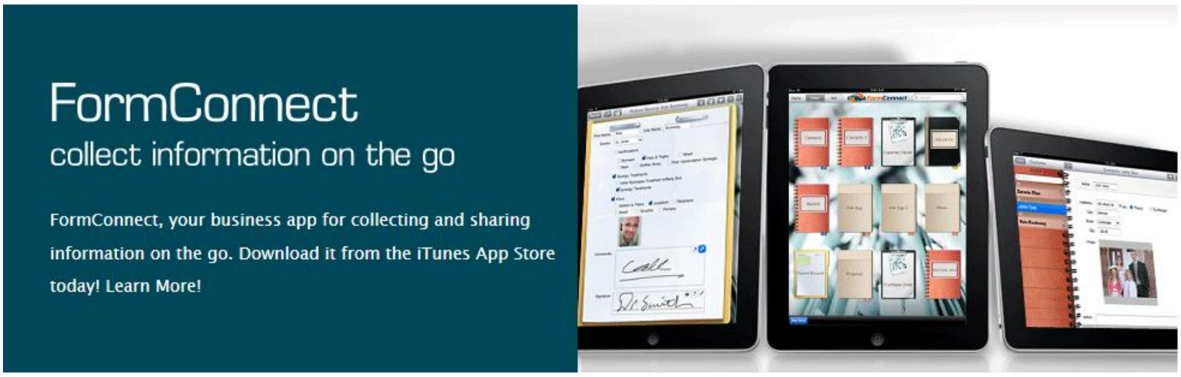
To find out how Sophos products can help protect your organisation, visit www.sophos.com/products or contact SSS on **sales@sss.co.nz**.

SCIENTIFIC SOFTWARE & SYSTEMS THE PROBLEM SOLVERS
www.sss.co.nz

SOPHOS
simply secure

8.2. Hastings District Council - FormConnect App

FormConnect (http://www.formconnections.com/) is an iPad app which allows you to easily design a form. Note, so easy my 16 year old daughter, after giving her a 5 minute lesson, created forms for the Health inspection solution, I will be demonstrating.



FormConnect

collect information on the go

FormConnect, your business app for collecting and sharing information on the go. Download it from the iTunes App Store today! Learn More!

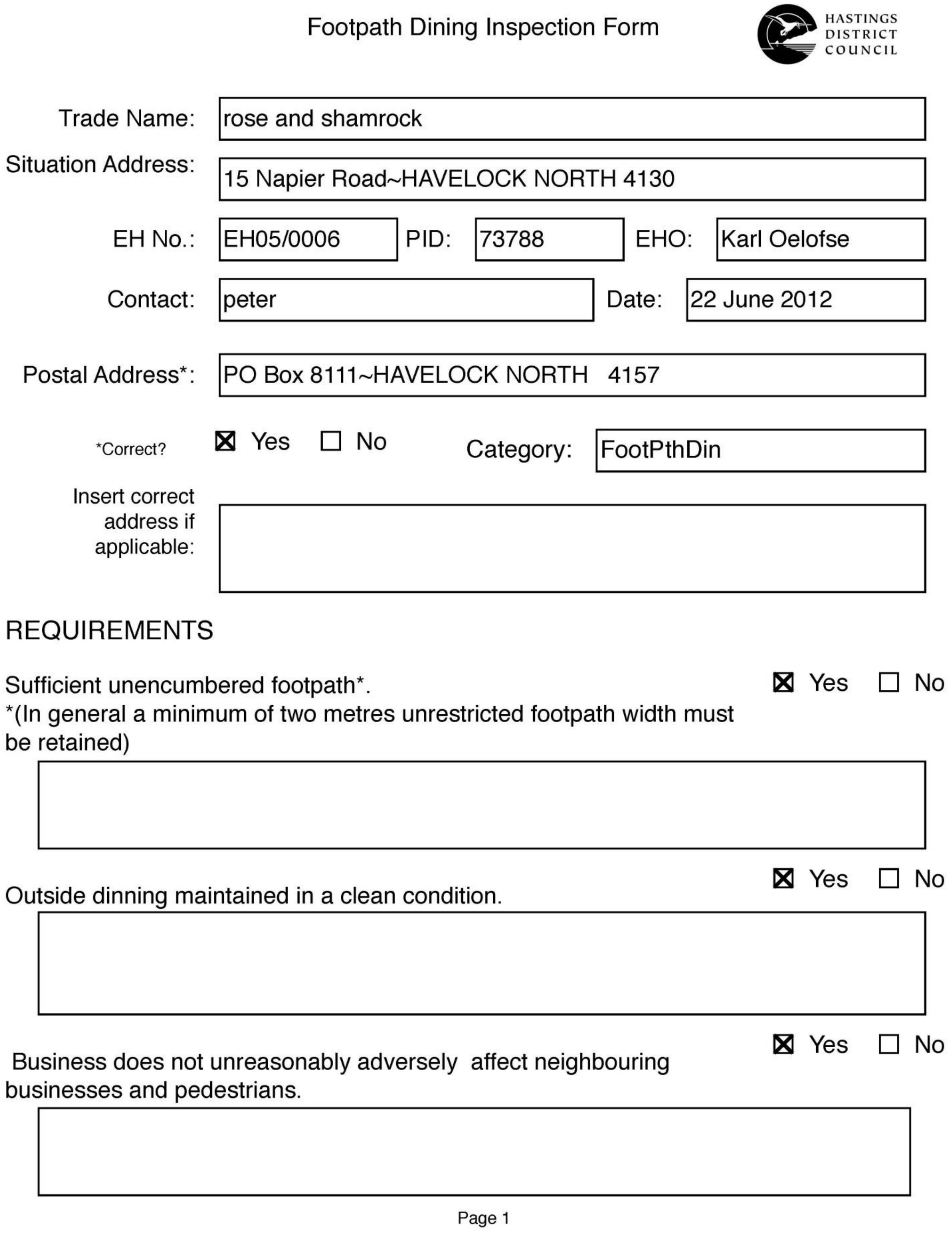
The form and its data is all stored on the iPad and does not require one to be connected; thus it is an offline data capture program. The form developer provides for most field types i.e. Alpha, numeric, drop down list, radio button, photo (both from the Library and from the camera live), date and time etc. More importantly, it is easy to alter the forms or copy parts from another form. There is the ability to 'lock' the form so as to stop your end user tampering with it!.

Data is easily imported from any system that can output a csv file. In my example, we will use Excel and then output as a csv. Likewise, data that has been inputted can be singularly emailed as a pdf (see example) or exported as csv/xml etc If you want to move the whole database & form there is a function to do this i.e. useful to copy data onto another iPad.

It is a very useful app for $13.99.

See sample form over page.

Sample Form:



Footpath Dining Inspection Form

HASTINGS DISTRICT COUNCIL

Trade Name: rose and shamrock

Situation Address: 15 Napier Road~HAVELOCK NORTH 4130

EH No.: EH05/0006 PID: 73788 EHO: Karl Oelofse

Contact: peter Date: 22 June 2012

Postal Address*: PO Box 8111~HAVELOCK NORTH 4157

*Correct? ☒ Yes □ No Category: FootPthDin

Insert correct address if applicable:

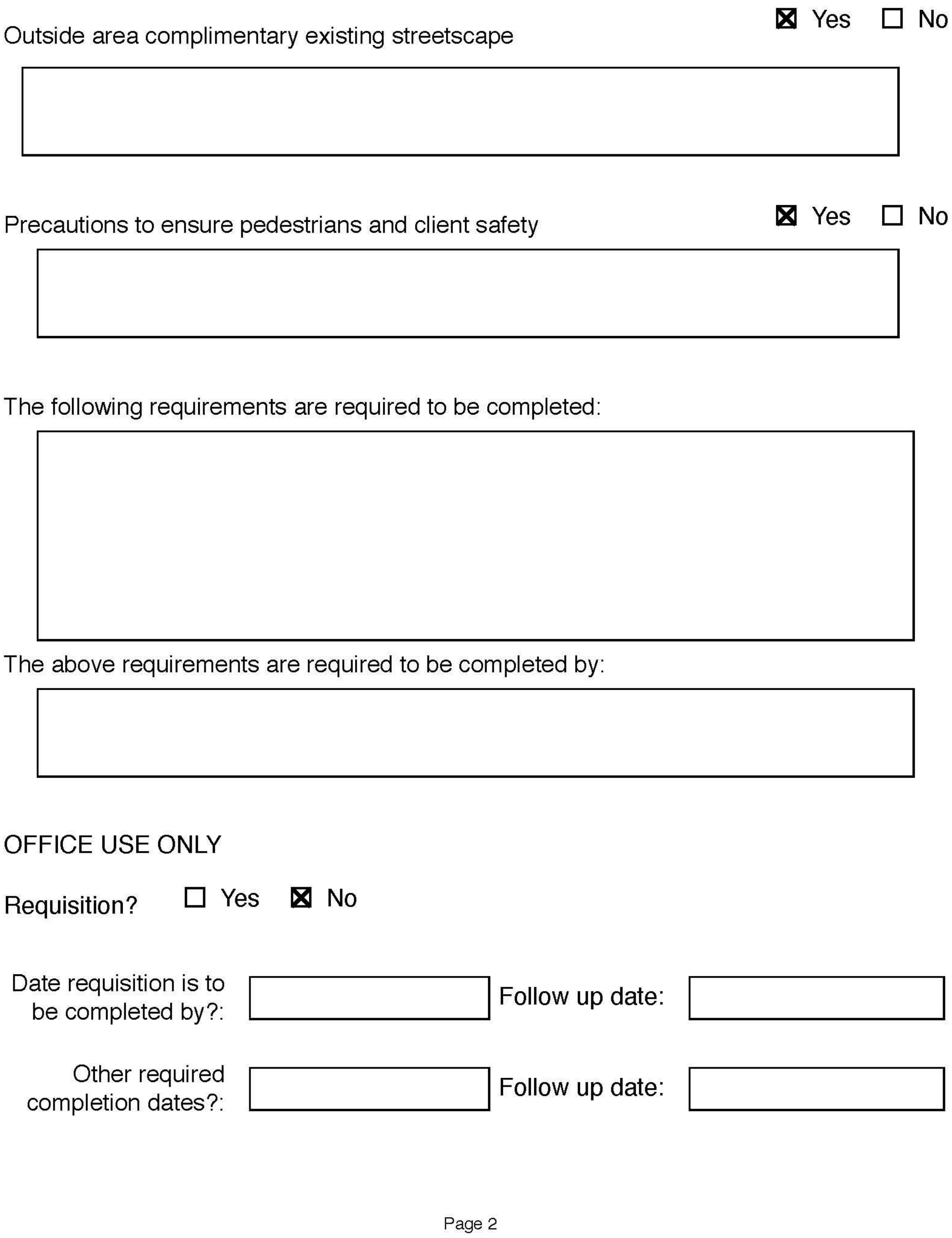
REQUIREMENTS

Sufficient unencumbered footpath*. ☒ Yes □ No
*(In general a minimum of two metres unrestricted footpath width must be retained)

Outside dinning maintained in a clean condition. ☒ Yes □ No

Business does not unreasonably adversely affect neighbouring businesses and pedestrians. ☒ Yes □ No

Page 1



Outside area complimentary existing streetscape ☒ Yes ☐ No

Precautions to ensure pedestrians and client safety ☒ Yes ☐ No

The following requirements are required to be completed:

The above requirements are required to be completed by:

OFFICE USE ONLY

Requisition? ☐ Yes ☒ No

Date requisition is to be completed by?: Follow up date:

Other required completion dates?: Follow up date:

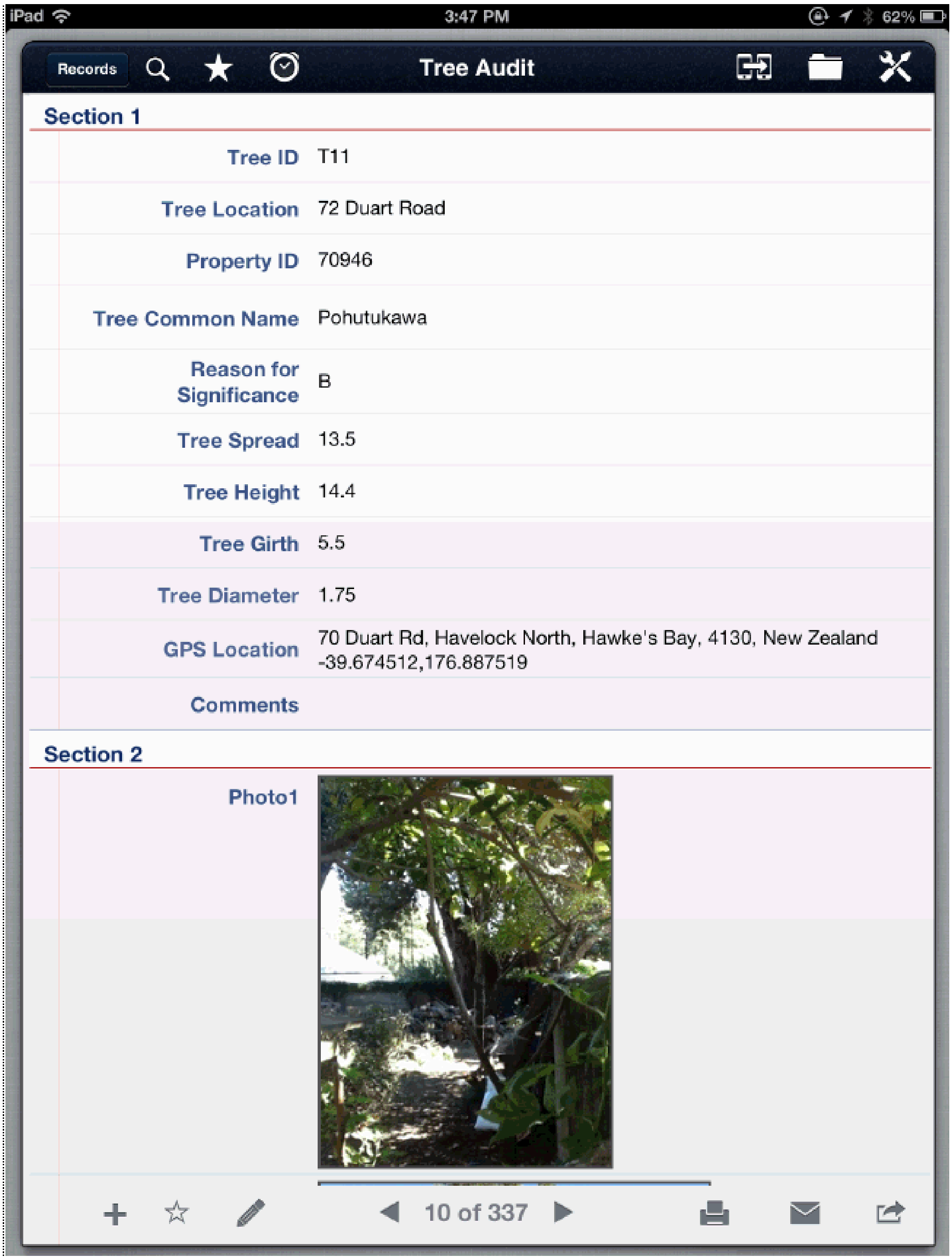
Page 2

Photograph of footpath dining set up

Photograph of footpath dining set up

COMMENTS

I used another app called Tap Forms ($6.99, http://www.tapforms.com/) to do capture of our Protected Trees. This is a much simpler one field on one line type form, but did have two features which currently is not available in FormConnect – it had a direct link to google maps, plus also could do calculations.   Here is a screen shot:

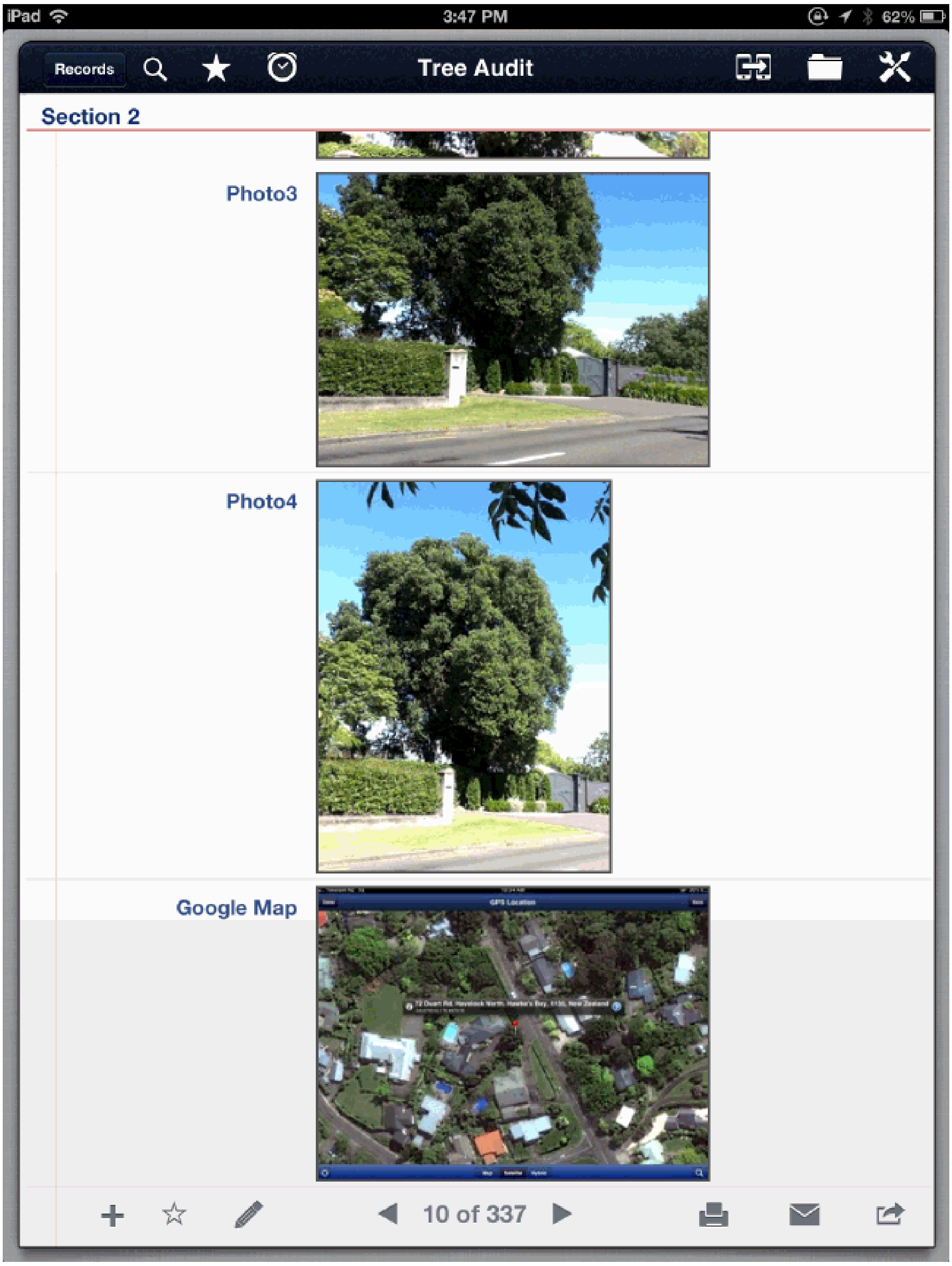


Section 1

Tree ID	T11
Tree Location	72 Duart Road
Property ID	70946
Tree Common Name	Pohutukawa
Reason for Significance	B
Tree Spread	13.5
Tree Height	14.4
Tree Girth	5.5
Tree Diameter	1.75
GPS Location	70 Duart Rd, Havelock North, Hawke's Bay, 4130, New Zealand -39.674512,176.887519
Comments	

Section 2

Photo1



By Ian Wright, IS Manager, Hastings District Council.

8.3. Hutt City Council Goes Mobile with TechnologyOne

With the need to increase the amount of productive time in the field for its Trade Waste Inspectors, New Zealand's Hutt City Council (HCC) turned to TechnologyOne's new mobile offer.

The Council hoped to reduce paperwork, improve service quality and provide a significant increase in productive time through avoiding the need for double handling of data.

The Council, which services a community of more than 100,000 people, deployed a trial version of the TechnologyOne Mobile solution in under four weeks as part of a phased implementation strategy, with plans to extend mobile capabilities to other divisions.

The Council initially focused on ways to streamline the annual premises inspection process for the trade waste team, which is responsible for inspecting, monitoring and issuing licenses to more than 600 sites each year.

The Trade waste team also responds to pollution incidents, investigates overland flow stormwater issues and carries out storm-water inflow audits.

HCC Manager of IS Projects, Tony Skerrett, said the mobile technology will streamline the team's outputs and speed up the renewals inspection process.

> *"The TechnologyOne Mobile solution will greatly improve the way the trade waste team operates. Officers will no longer need to be in the Council building to input data on specific sites, log information or flag areas for action," he said.*
>
> *"The high level of integration between the office and mobile workers will save considerable administration time, meaning Council officers can spend more time doing their jobs and less time sitting behind a desk.*
>
> *"We envisage that the ability to start and end work in the field, rather than at the office, will lead to ongoing cost savings."*

The new mobile offering allows inspection officers to access a full database of sites from a handheld mobile device enabling information and images to be updated quickly and easily. These records are then integrated with the TechnologyOne solutions back in the office, removing the need for paperwork and onerous data entry.

In this instance, the mobile inspections solution interacts directly with the back end Property & Rating solution, which covers all aspects of councils' interaction with the community such as building consents, animal inspections, trade waste management and water billing, rates and a raft of other regulatory functions.

The TechnologyOne Property & Rating Mobile solution allows workflow items and inspections to be completed in real time and onsite, reducing the administrative double handling and ensuring data accuracy, security and relevance.

Mr Skerrett said the other benefit Hutt City Council had gained from using TechnologyOne Mobile solutions was the improvement in the quality and accuracy of the data.

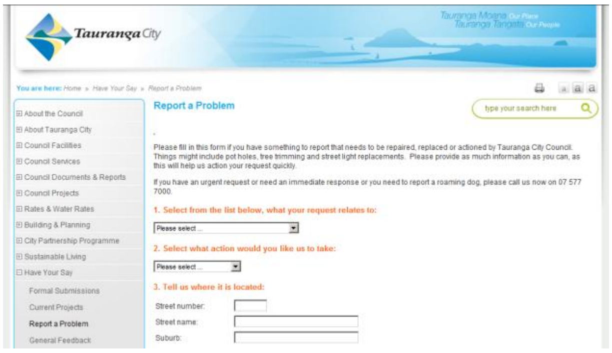
> *"We have found there are huge benefits to be gained by taking an approach that considers the end to end solution from software to hardware and are delighted with the results so far," he said.*
>
> *"The Council has already received interest from other internal departments who are keen to become involved in our mobile technology journey."*

TechnologyOne Executive Chairman, Adrian Di Marco, said the highly integrated TechnologyOne Mobile solution was ideal for supporting offsite workers and had been developed to help organisations work smarter.

> *"The value of a sophisticated mobile solution is measured through its ability to quickly improve processes and productivity, deliver a superior user experience and enable offsite workers to work more efficiently," Mr Di Marco said.*
>
> *"It is about lightening the load so workers can do what they need to do while also ensuring the data is replicated in the back office system to avoid unnecessary duplications.*
>
> *"Mobile devices bypass the delays by having the data displayed or collected at the point at which it is needed so the information can be relayed rapidly back to the enterprise systems for fast processing.*
>
> *"The TechnologyOne Mobile solutions are used by a diverse range of occupations within our customer organisations including all levels of government and utility companies."*

8.4. Origen Ozone: Tauranga City Council, Western Bay District Council, Rotorua District Council

When residents at **Tauranga City Council** contact the council to raise a service request the information is captured in the Ozone Contact Centre module. Information can start it's journey through the Contact Centre module using the Ozone desktop client, Ozone mobile web interface, web services, or via online services providing a vast range of flexible options to gather information efficiently and appropriately.



Report a Problem

Please fill in this form if you have something to report that needs to be repaired, replaced or actioned by Tauranga City Council. Things might include pot holes, tree trimming and street light replacements. Please provide as much information as you can, as this will help us action your request quickly.

If you have an urgent request or need an immediate response or you need to report a roaming dog, please call us now on 07 577 7000.

1. Select from the list below, what your request relates to:

Please select ...

2. Select what action would you like us to take:

Please select ...

3. Tell us where it is located:

Street number:

Street name:

Suburb:

The service request information once captured is managed by the customizable workflow engine to distribute the request out to the necessary people either internally in the organization or externally to the organization. Information can be distributed by a range of channels including web, mobile SMS, email, fax or workflow tasks.

At Tauranga City Council the service request is instantly available to the contractor via the Ozone mobile web interface, an email notification is sent to the contractor to alert them to the request and an integration also raises the service request information automatically via web services into their internal systems.

Tauranga City Council has embraced the technology that the Ozone architecture offers and use the mobile web interface to provide access to service request information, this interface provides more timely and accurate information to the customer when they enquire on their service request in the future.

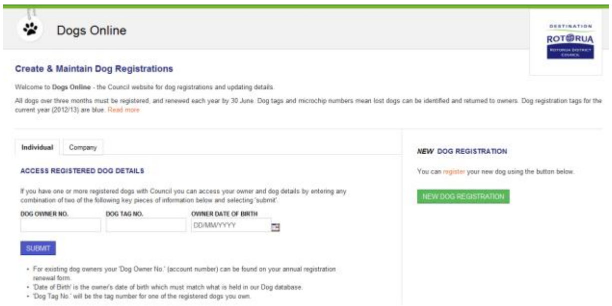
Western Bay District Council has implemented a third party mobile inspections solution 'Go-Get' for building inspections in the Ozone Building Consents module. Below is a quote from Steve Hill (Group Manager Customer Services- WBOPDC 04/10/2011)

"Integration between Go Gets and Ozone for the building consent inspection and approval processes has significantly increased our productivity and cost effectiveness whilst meeting the more stringent requirements of being a BCA (Building Consent Authority)"

Western Bay's use of the Ozone mobility technologies such as web services have made information available to inspectors in the field, improving efficiency of data capture and collection when performing inspections. The information collected while mobile is also synchronised back into the system using Ozone's web services.

Rotorua District Council (recent winners at the 2012 ALGIM customer service awards) provide an online services interface to their residents around a number of their Ozone modules. Recently the Animal Control modules has a resident online services web interface added to their Ozone Contact Centre and Animal Control modules.

Now residents in the Rotorua district register their dogs from any mobile device with WIFI access.



Create & Maintain Dog Registrations

Welcome to **Dogs Online** - the Council website for dog registrations and updating details.

All dogs over three months must be registered, and renewed each year by 30 June. Dog tags and microchip numbers mean lost dogs can be identified and returned to owners. Dog registration tags for the current year (2012/13) are blue. Read more

ACCESS REGISTERED DOG DETAILS

If you have one or more registered dogs with Council you can access your owner and dog details by entering any combination of two of the following key pieces of information below and selecting 'submit'.

DOG OWNER NO.

DOG TAG NO.

OWNER DATE OF BIRTH DD/MM/YYYY

- For existing dog owners your 'Dog Owner No.' (account number) can be found on your annual registration renewal form.
- 'Date of Birth' is the owner's date of birth which must match what is held in our Dog database.
- 'Dog Tag No.' will be the tag number for one of the registered dogs you own.

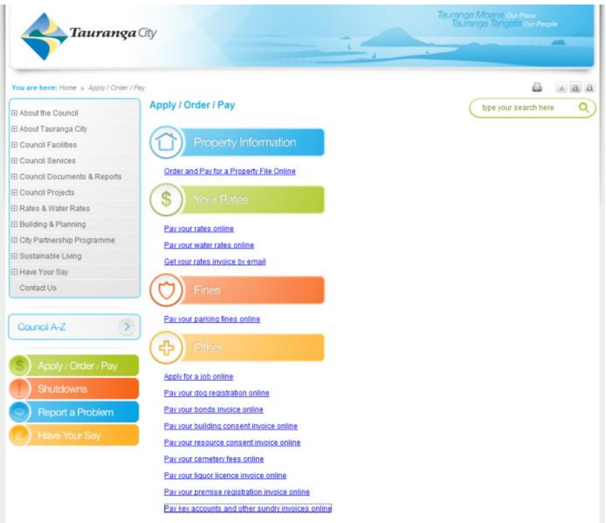
NEW DOG REGISTRATION

You can register your new dog using the button below.

This solution uses Ozone mobile web services and an integration to the Ozone modules to provide mobile web access to the Ozone systems.

Tauranga City Council have provided an extensive range of online services to their residents make payments to the council via the web. This provides users with the ability to pay their rates, water, parking fines, dog registrations and all other sundry debtor invoices.

Email notifications are sent from the system providing alerts to residents when key information is required and driving traffic to payments online.



Apply / Order / Pay

Property Information

- Order and Pay for a Property File Online

Your Rates

- Pay your rates online
- Pay your water rates online
- Get your rates invoice by email

Fines

- Pay your parking fines online

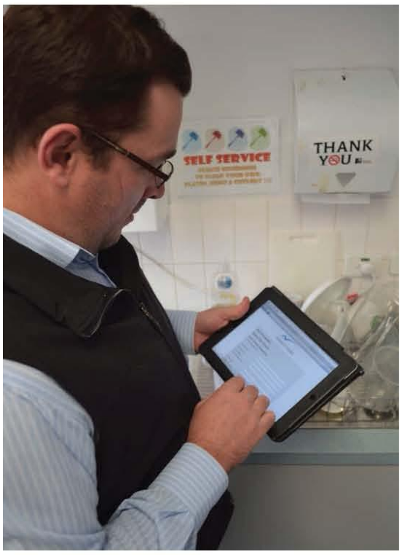
Other

- Apply for a job online
- Pay your dog registration online
- Pay your bonds invoice online
- Pay your building consent invoice online
- Pay your resource consent invoice online
- Pay your cemetery fees online
- Pay your liquor licence invoice online
- Pay your premise registration invoice online
- Pay key accounts and other sundry invoices online

8.5. Auburn City Council - BlinkMobile Forms into Pathway

Auburn City Council CaseStudy

Auburn City Council Delivers on IT Any Time, Anywhere, with BlinkMobile Solution



Auburn City Council is the authority responsible for a thriving 31 square kilometre local government area right at the heart of Sydney. Located just 17 kilometres from the Sydney central business district and six kilometres from the city of Parramatta, the area is home to a number of major attractions including the world-class sporting facilities of Sydney Olympic Park, Bicentennial Park, the Auburn Botanic Gardens and the Gallipoli Mosque. The city boasts a high degree of cultural diversity with residents drawn from 124 countries.

A very mobile workforce

In 2010, when Sarju Sahu arrived as the newly-appointed Manager of Information Technology at Auburn City Council, he was struck by the mobile nature of the Council's workforce. He found 38 per cent of staff operated in-field basis. These included tree, food and fire inspectors, rangers, parking inspectors, building surveyors and maintenance staff responsible for working on roads, footpaths, buildings and parks, and more.

It was quickly apparent to Sahu that if his team was to provide effective and efficient productivity tools and solutions to support the Council, mobility had to be included within the IT strategy. His first priority was to develop an IT vision statement: 'IT everywhere, stay productive and connected anywhere, anytime, on any network and with any device'.

Over the next few months, Sahu spent time observing the business, learning its policies, procedures, practices and processes. Once he had a good understanding of the scale and scope of work, he approached the Council Executive Team with a proposal for automating processes for mobile and in-field staff, equipping them so that they could capture data and initiate workflows while out in the field. The likely productivity and efficiency gains were attractive and the executive agreed to the initiative.

Online and Off-line considerations

Sahu consulted with a group of representatives from a variety of Council departments and prepared a short list of work processes that would be suited for a pilot program. Top of their recommendations were the private tree preservation permit process managed by Council's Tree Coordinator, followed by food inspections.

Sahu's team set about investigating mobile enabling technologies which included BlinkMobile, an Australian headquartered Mobile Enterprise Application Platform (MEAP) provider. Blink's Sydney-based partner EcoView Mobile, a technology and consulting services company worked with Council to tailor a solution which would enable staff to capture, send and receive data remotely using mobile forms.

"BlinkForms became our preferred solution," Sahu says, "because it is quite flexible and scalable. It can be used for any device. Its biggest strength, which was very appealing to the Executive Team, is that it has off-line capabilities. For a project that is all about efficiency, productivity and effectiveness, this was important because if the system can't be used in off-line mode staff won't be productive. With BlinkMobile, even if there is no network connection, people can still carry on with their work and the data can be uploaded later."

The Executive Team were very supportive and gave the go-ahead to Sahu's process automation and technology recommendations and the pilot project commenced in mid-2011.

www.blinkmobile.com.au

AUBURN CITY COUNCIL
MANY CULTURES ONE COMMUNITY

BlinkMobile interactive

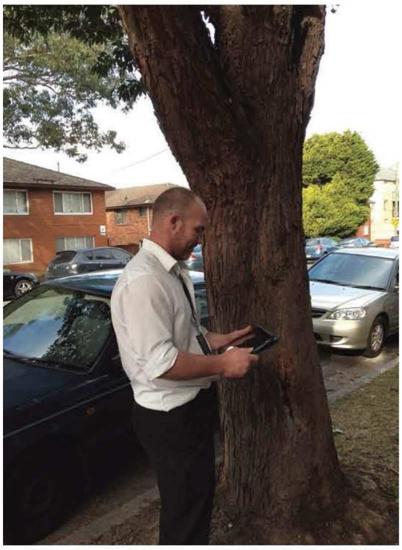
A team effort

Sahu established a project team involving BlinkMobile, EcoView, Infor, the developer of Pathway, one of the Council's key mission critical information systems, and two internal stakeholders. "We needed two-way integration with the Council's Pathway application. This was going to be hard to achieve unless we had all the parties involved working together," he notes.

EcoView worked with Council to develop mobile forms that would allow the Tree Coordinator to enter data and photographs using the Blink mobility platform. They also developed a custom adaptor to sit between Blink and Pathway, enabling integration between the applications. Integration was also established with the Council's records management, email and GPS systems. The forms were tested both on and off-line, and new security measures were put in place to manage the introduction of mobile devices.

Securing the data

"When we first started this project, one of the concerns raised was security," said Sahu. "Because of this we have ensured end-to-end security in a number of ways. We are using mobile device management software to control passwords, provide remote locking and application control. We use SSL encryption, a firewall, and both Pathway's security and Blink's security. We've also introduced remote wiping so content can be erased if a device is lost or stolen."



Sahu believes establishing the high level of security has been a rewarding exercise for the organisation as it has only served to strengthen the Council's existing privacy and information security measures.

Improvements all around

Since the tree inspection and food inspection applications have gone live, the inspectors can use iPads to capture data on the BlinkMobile form which then automatically uploads the data to Pathways. The process has increased the efficiency of the Council and the productivity of in-field staff. It has also improved business workflows and improved the capture of data to the Council's document management system.

Customers are sharing in the benefits. Staff are finding they can respond faster to customer requests and better documentation of inspections is resulting in improved communication with rate payers. The online forms have reduced paperwork and replaced paper forms. There's also been a reduction in duplication of processes, with data only being entered once.

The automation of the tree inspection process has altogether eliminated entering information into the hard copy inspection form, entering the information manually from the form to the Council's Pathway application, scanning the form and emailing/sending the completed form to the Tree Coordinator and then manually saving the form into the Council's record management system. The extent of this automation enabled the Tree coordinator to complete 10-20 inspections in a day depending on the proximity of the trees as compared to 5-6 inspections a day with the manual process.

"The interest and enthusiasm of the Tree Coordinator and Manager Parks & Recreation in implementing the new processes was very important to the pilot's success along with the commitment and support from the Executive Team," said Sahu.

The cost and production efficiencies that have been gained from the pilot led to the immediate go-ahead by the Executive Team for Sahu and his team to automate as many field processes as possible.

Future developments

Today Auburn City Council uses BlinkForms for its tree inspections, licensed food site inspections, and ad hoc food inspections. Many more inspection applications are planned for the immediate future including public tree inspection; fire inspection, personal health related hairdressing/barber/beauty/skin/penetration inspection, regulated premises inspection, swimming pool inspection and building surveyor inspection; and many more to follow. 'One key benefit which is a by-product of the automation is that we are leveraging our learning from the initial BlinkMobile and EcoView solution investment. The design has been flexible enough to develop and automate new processes with marginal effort," Sahu observes.

The new mobility tools and forms are helping the IT team to achieve its vision of keeping Council staff connected and engaged anywhere, at any time. More importantly, red tape has been reduced; staff productivity is increasing along with community satisfaction with Council services.

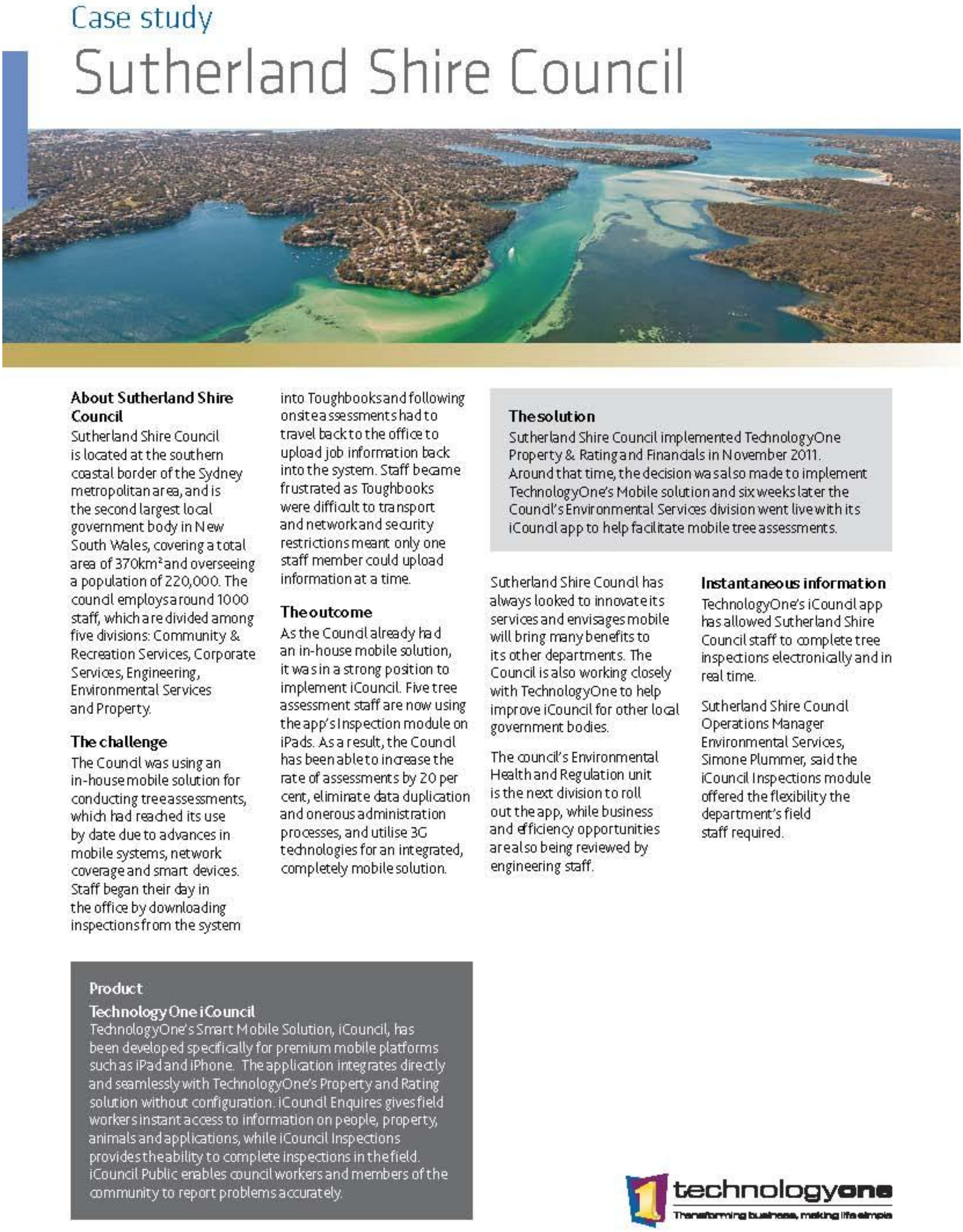
"This pilot project was an excellent demonstration of teamwork and commitment from all the partners – including the General Manager, the Executive and Management Teams and operational staff; and was critical to the success of this program," said Sahu.

www.blinkmobile.com.au

AUBURN CITY COUNCIL
MANY CULTURES ONE COMMUNITY

BlinkMobile interactive

8.6. Sutherland Shire Council – TechnologyOne iCouncil



Case study

Sutherland Shire Council

About Sutherland Shire Council

Sutherland Shire Council is located at the southern coastal border of the Sydney metropolitan area, and is the second largest local government body in New South Wales, covering a total area of 370km² and overseeing a population of 220,000. The council employs around 1000 staff, which are divided among five divisions: Community & Recreation Services, Corporate Services, Engineering, Environmental Services and Property.

The challenge

The Council was using an in-house mobile solution for conducting tree assessments, which had reached its use by date due to advances in mobile systems, network coverage and smart devices. Staff began their day in the office by downloading inspections from the system into Toughbooks and following onsite assessments had to travel back to the office to upload job information back into the system. Staff became frustrated as Toughbooks were difficult to transport and network and security restrictions meant only one staff member could upload information at a time.

The outcome

As the Council already had an in-house mobile solution, it was in a strong position to implement iCouncil. Five tree assessment staff are now using the app's Inspection module on iPads. As a result, the Council has been able to increase the rate of assessments by 20 per cent, eliminate data duplication and onerous administration processes, and utilise 3G technologies for an integrated, completely mobile solution.

The solution

Sutherland Shire Council implemented TechnologyOne Property & Rating and Financials in November 2011. Around that time, the decision was also made to implement TechnologyOne's Mobile solution and six weeks later the Council's Environmental Services division went live with its iCouncil app to help facilitate mobile tree assessments.

Sutherland Shire Council has always looked to innovate its services and envisages mobile will bring many benefits to its other departments. The Council is also working closely with TechnologyOne to help improve iCouncil for other local government bodies.

The council's Environmental Health and Regulation unit is the next division to roll out the app, while business and efficiency opportunities are also being reviewed by engineering staff.

Instantaneous information

TechnologyOne's iCouncil app has allowed Sutherland Shire Council staff to complete tree inspections electronically and in real time.

Sutherland Shire Council Operations Manager Environmental Services, Simone Plummer, said the iCouncil Inspections module offered the flexibility the department's field staff required.

Product

Technology One iCouncil

TechnologyOne's Smart Mobile Solution, iCouncil, has been developed specifically for premium mobile platforms such as iPad and iPhone. The application integrates directly and seamlessly with TechnologyOne's Property and Rating solution without configuration. iCouncil Enquires gives field workers instant access to information on people, property, animals and applications, while iCouncil Inspections provides the ability to complete inspections in the field. iCouncil Public enables council workers and members of the community to report problems accurately.

technologyone
Transforming business, making life simple

Instantaneous information continued

"No one likes going out with a form and clipboard, then coming back to the office to re-enter all the information into a computer – our department loves working outdoors and iCouncil allows staff to complete their work in the field," said Ms Plummer.

Implementation of the app is straightforward as all iCouncil modules integrate with maps, phone, internet and email to optimise the quality of information and enable maximum efficiency.

The app is available to any local government body using TechnologyOne Property & Rating.

"We have never flown through an implementation like we have with TechnologyOne. It took less than six weeks for us to go live," Ms Plummer said

"Most of the time, organisations are tied up with colossal technology concerns such as server set up, but TechnologyOne systems and their high level of integration allowed for a completely streamlined process.

"Now that technical staff understand the iCouncil product, further roll out of the tool can be completed within a few hours or days at the most."

Key benefits

Configured using fast and simple application features such as event checklists, application conditions and events workflow, iCouncil functions make inspections easier by granting staff the ability to start and end work in the field rather than the office.

With tree inspectors able to receive work directly and report assessment results immediately, Sutherland Shire Council has already realised several benefits.

Significant time savings have been made, along with greater accuracy as a result of automatic updates and data security with iOS data protection features.

Under the old mobile system, tree inspectors were getting through an average of 75 applications a week, but with iCouncil they are now able to complete around 90 applications a week.

"Our staff are able to respond to jobs quicker with access to real time information and we are subsequently providing customers with more efficient service," said Ms Plummer.

"By using a completely mobile solution, our small tree inspections team is no longer tied up in travel and administration."

Furthermore, the Council has eliminated significant Occupational Health & Safety concerns by getting rid of Toughbooks, which were very heavy and extremely difficult to haul around on the job.

Working together to deliver results

Since going live with iCouncil, Sutherland Shire Council has provided TechnologyOne with valuable feedback to ensure the app is optimised for other local government bodies.

"TechnologyOne has been very receptive to our feedback and we are still working with its staff to guarantee the most effective results with iCouncil," said Ms Plummer.

"For example, risk is a big factor in the tree assessment business and we have a thorough checklist that consists of about 160 items, which need to be uploaded, reviewed and processed quickly.

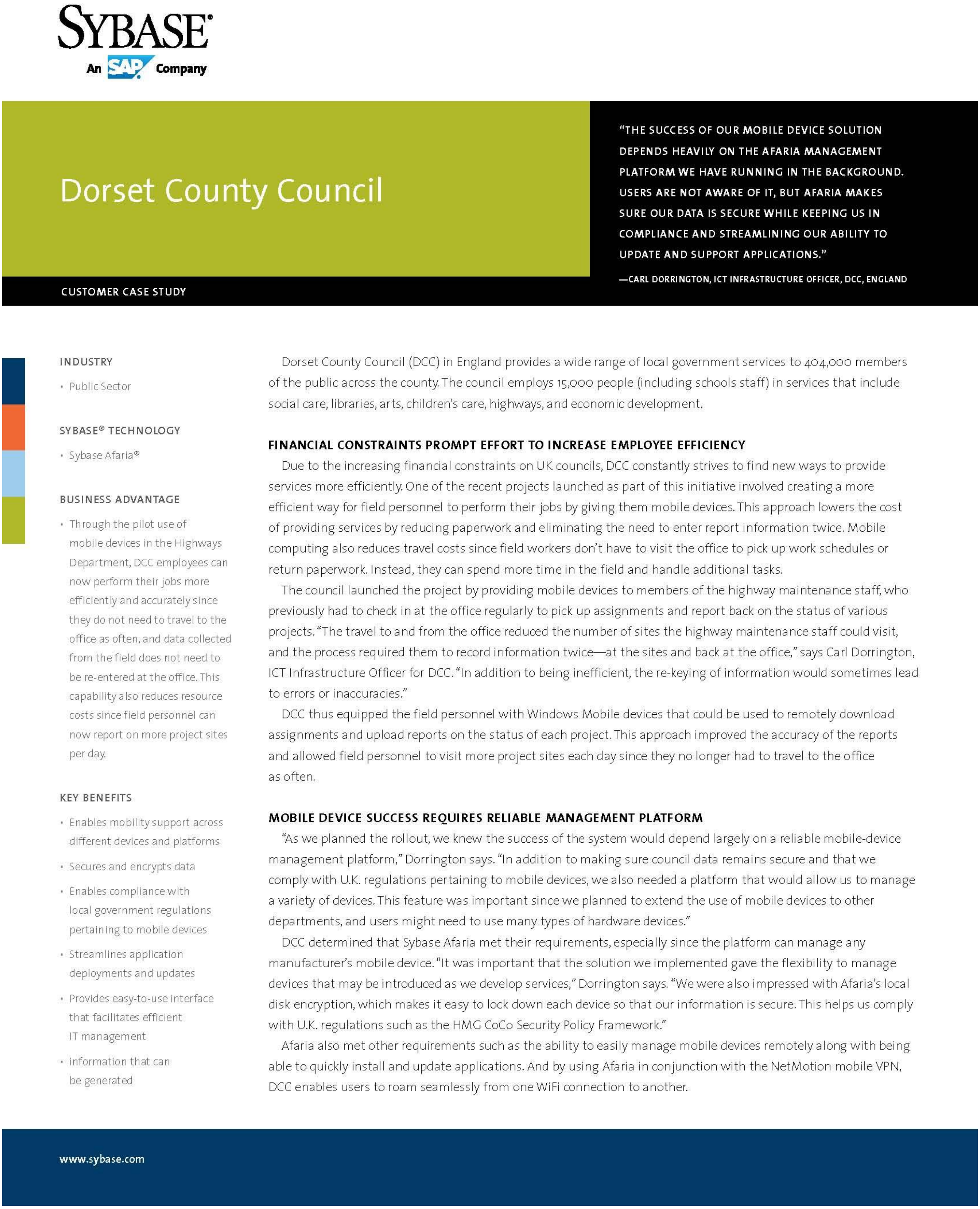
"No one likes going out with a form and clipboard, then coming back to the office to re-enter all the information into a computer – our department loves working outdoors and iCouncil allows staff to complete their work in the field,

"By using a completely mobile solution, our small tree inspections team is no longer tied up in travel and administration.

"iCouncil is a significant investment for a free service, but it has certainly proved worthwhile."

Simone Plummer
Operations Manager
Environmental Services,
Sutherlands Shire Council

8.7. Dorset County Council Deploys SAP Afaria



SYBASE
An SAP Company

Dorset County Council

CUSTOMER CASE STUDY

"THE SUCCESS OF OUR MOBILE DEVICE SOLUTION DEPENDS HEAVILY ON THE AFARIA MANAGEMENT PLATFORM WE HAVE RUNNING IN THE BACKGROUND. USERS ARE NOT AWARE OF IT, BUT AFARIA MAKES SURE OUR DATA IS SECURE WHILE KEEPING US IN COMPLIANCE AND STREAMLINING OUR ABILITY TO UPDATE AND SUPPORT APPLICATIONS."

—CARL DORRINGTON, ICT INFRASTRUCTURE OFFICER, DCC, ENGLAND

INDUSTRY

- Public Sector

SYBASE® TECHNOLOGY

- Sybase Afaria®

BUSINESS ADVANTAGE

- Through the pilot use of mobile devices in the Highways Department, DCC employees can now perform their jobs more efficiently and accurately since they do not need to travel to the office as often, and data collected from the field does not need to be re-entered at the office. This capability also reduces resource costs since field personnel can now report on more project sites per day.

KEY BENEFITS

- Enables mobility support across different devices and platforms
- Secures and encrypts data
- Enables compliance with local government regulations pertaining to mobile devices
- Streamlines application deployments and updates
- Provides easy-to-use interface that facilitates efficient IT management
- information that can be generated

Dorset County Council (DCC) in England provides a wide range of local government services to 404,000 members of the public across the county. The council employs 15,000 people (including schools staff) in services that include social care, libraries, arts, children's care, highways, and economic development.

FINANCIAL CONSTRAINTS PROMPT EFFORT TO INCREASE EMPLOYEE EFFICIENCY

Due to the increasing financial constraints on UK councils, DCC constantly strives to find new ways to provide services more efficiently. One of the recent projects launched as part of this initiative involved creating a more efficient way for field personnel to perform their jobs by giving them mobile devices. This approach lowers the cost of providing services by reducing paperwork and eliminating the need to enter report information twice. Mobile computing also reduces travel costs since field workers don't have to visit the office to pick up work schedules or return paperwork. Instead, they can spend more time in the field and handle additional tasks.

The council launched the project by providing mobile devices to members of the highway maintenance staff, who previously had to check in at the office regularly to pick up assignments and report back on the status of various projects. "The travel to and from the office reduced the number of sites the highway maintenance staff could visit, and the process required them to record information twice—at the sites and back at the office," says Carl Dorrington, ICT Infrastructure Officer for DCC. "In addition to being inefficient, the re-keying of information would sometimes lead to errors or inaccuracies."

DCC thus equipped the field personnel with Windows Mobile devices that could be used to remotely download assignments and upload reports on the status of each project. This approach improved the accuracy of the reports and allowed field personnel to visit more project sites each day since they no longer had to travel to the office as often.

MOBILE DEVICE SUCCESS REQUIRES RELIABLE MANAGEMENT PLATFORM

"As we planned the rollout, we knew the success of the system would depend largely on a reliable mobile-device management platform," Dorrington says. "In addition to making sure council data remains secure and that we comply with U.K. regulations pertaining to mobile devices, we also needed a platform that would allow us to manage a variety of devices. This feature was important since we planned to extend the use of mobile devices to other departments, and users might need to use many types of hardware devices."

DCC determined that Sybase Afaria met their requirements, especially since the platform can manage any manufacturer's mobile device. "It was important that the solution we implemented gave the flexibility to manage devices that may be introduced as we develop services," Dorrington says. "We were also impressed with Afaria's local disk encryption, which makes it easy to lock down each device so that our information is secure. This helps us comply with U.K. regulations such as the HMG CoCo Security Policy Framework."

Afaria also met other requirements such as the ability to easily manage mobile devices remotely along with being able to quickly install and update applications. And by using Afaria in conjunction with the NetMotion mobile VPN, DCC enables users to roam seamlessly from one WiFi connection to another.

www.sybase.com

AFARIA STREAMLINES DEVICE CONFIGURATION AND APPLICATION UPDATES

To help DCC deploy Afaria, Sybase provided training on how to configure mobile devices for each user. The IT staff can now set up user groups on their own ahead of time with specific policies that apply to groups and then add users to each group as necessary. NetMotion launches a program that runs Afaria, and after a user is verified, Afaria automatically configures the device and picks up the policy based on the group the user belongs to. "Each department has a policy template—we just add users to the appropriate Active Directory group, and Afaria automatically applies the correct policy configuration," Dorrington says.

The Afaria Session Manager feature helps DCC install and update applications with scripts created by the IT staff. "Session Manager makes our job a lot easier when it comes to writing scripts," Dorrington says. "Once Sybase gave us a demo on using Session Manager and the other Afaria features, we were able to manage the solution on our own. The deployment went very smoothly without any problems."

When devices are in use, DCC can monitor that they are used for the right purpose since users can connect only through the council's mobile VPN. Dorrington also emphasizes the ease-of-use as a major benefit: "Because Afaria streamlines application deployment and updates via Session Manager, we can identify devices that need updates and then monitor to confirm that updates have gone through."

Since information is encrypted by Afaria, DCC can give devices to users and know that information is safe even if a device is lost or stolen. "If necessary, we can easily remote-wipe the devices," Dorrington says. "The level of security that Afaria provides will also help us respond to any compliance audits we might be subject to by letting us run configuration reports."

INCREASED EMPLOYEE EFFICIENCY WITH REDUCED COUNCIL RESOURCE COSTS

Now that end-users in the highway maintenance department realize the benefits of accessing applications to help them perform their jobs using Windows Mobile devices, the council plans to roll out the solution to other departments over time. "Social services would also benefit greatly from the ability to submit reports from the field," Dorrington says.

DCC end users who have tried the mobile solution have given positive feedback on how much of a difference mobile devices make in helping them perform their jobs more efficiently. In the long run, DCC views the mobile-device approach as a way to reduce costs since the staff can get more work done in less time. "Everyone in the field across every department could receive assignments and submit reports without having to travel back to the office," Dorrington says. "And with information submitted just once, fewer input mistakes will occur, which will reduce staff time further. The accurate data collection over time will also lead to improved business intelligence that management can analyze for ways to enhance our services."

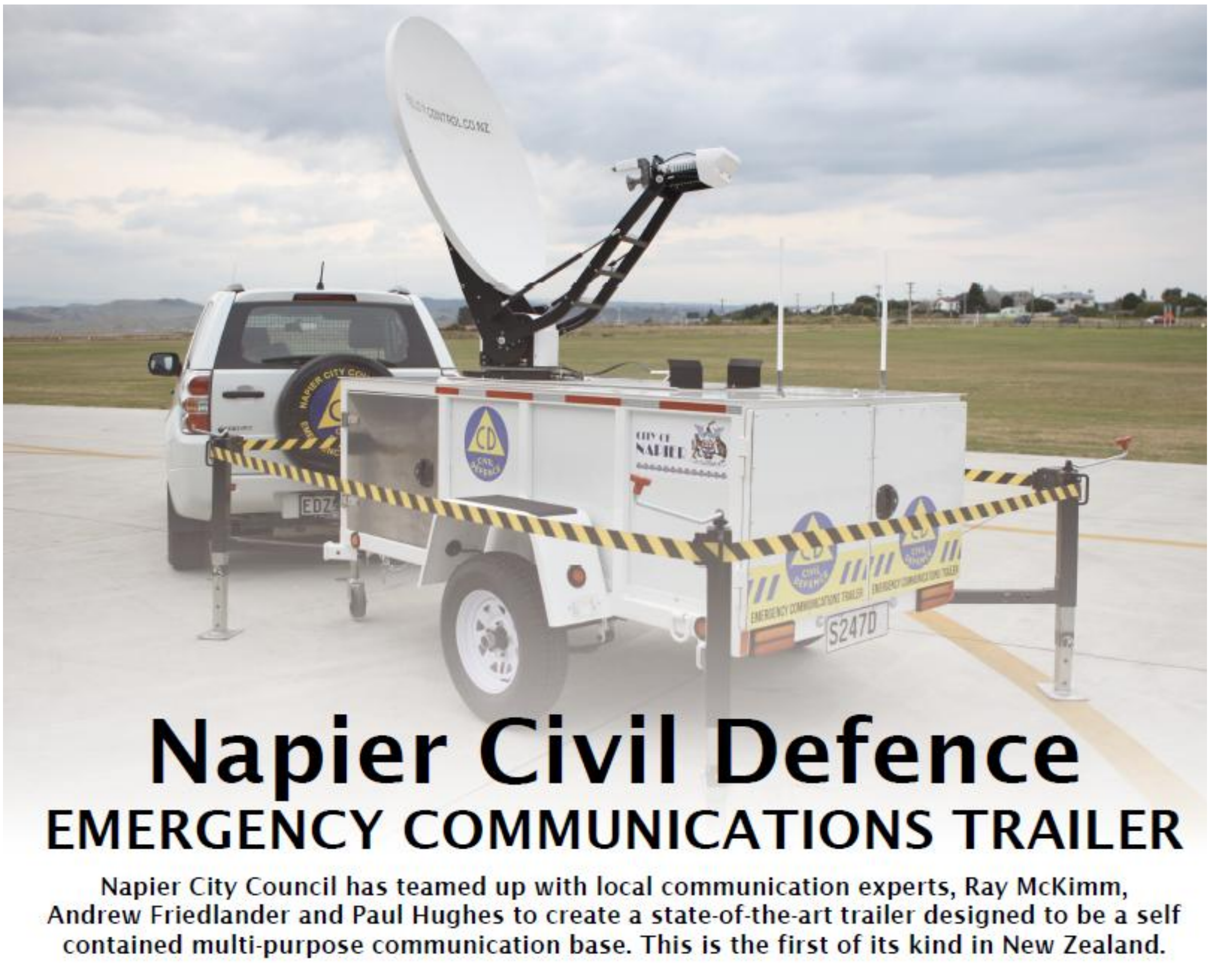
For information on our comprehensive Consulting and Education Services to support your Sybase technology initiatives, visit us at www.sybase.com/consulting.

Sybase, Inc.
Worldwide Headquarters
One Sybase Drive
Dublin, CA 94568-7902
U.S.A
1 800 8 sybase

www.sybase.com

8.8. Mobile Networking for Emergency Response Support

The Napier Communication Trailer is a first for New Zealand:



Napier Civil Defence

EMERGENCY COMMUNICATIONS TRAILER

Napier City Council has teamed up with local communication experts, Ray McKimm, Andrew Friedlander and Paul Hughes to create a state-of-the-art trailer designed to be a self contained multi-purpose communication base. This is the first of its kind in New Zealand.

This trailer has high-tech devices enabling it to serve as an emergency command post within five minutes of set-up. And Napier City Council has acquired the first of its kind in New Zealand.

The Council recognised the importance of efficient communication with emergency services after the recent tragedies in Canterbury and Japan. Their Civil Defence team subsequently teamed up with local communication experts, Ray McKimm, Andrew Friedlander and Paul Hughes to create a state-of-the-art trailer designed to be a self contained multi-purpose communication base. Made in the USA, the trailer can be quickly deployed via road or air to provide communication via satellite, 3G Mobile, wireless and UHF anywhere in the country.

Many local authorities have existing mobile communication systems that connect to one service, such as satellite, but this system has taken it a step further by providing connections to multiple services, i.e. copper, cellular, fibre and satellite.

Napier Civil Defence Manager, Angela Reade says during the initial stages of an event the trailer can provide telephone and internet access for four people via satellite immediately.

"The trailer's capabilities expand from there depending on the scale of the event," Angela says. "The services can be escalated by connecting to the cellular network, enabling communication for response teams as they arrive.

"It allows emergency management to continue with its response while allowing Council to continue business as usual. It basically becomes a central hub to deliver council services."

As well as recognising the importance of efficient communication in an emergency, the trailer ensures that Napier Civil Defence can use EMIS (Emergency Management Information System) even if all the networks are down, which is recommended by the Ministry of Civil Defence.

"We see the trailer being used for local and regional one-off events as well as a national resource when required."

Different pods (portable operation devices) equipped with specialist equipment are stored in the trailer, and swapped depending on what is required for the event. Currently there are four pods: a First Aid pod, with first aid equipment, extra oxygen, bandages, masks etc; a communication pod, with extra handheld radios, portable repeaters, battery chargers and long-range radios; a server backup pod containing Council systems; and a fuel pod and stand-alone generator, enabling the trailer to operate for longer periods.

Angela says she is thrilled to have the communication trailer as it enables her team to respond immediately after an event even if the emergency operation centre is inaccessible.

"It gives us more confidence knowing that our business continuity plan has that additional option if we need it. We are grateful to Ray, Andrew and Paul for their excellent service and expertise in creating this valuable resource as well as local businesses for their enthusiasm and support. It's a great example of how public and private sectors can work really well together."

For more information about the communication trailer see www.fieldcontrol.co.nz

The trailer provides the following:

Wireless internet connectivity using the cellphone mobile network

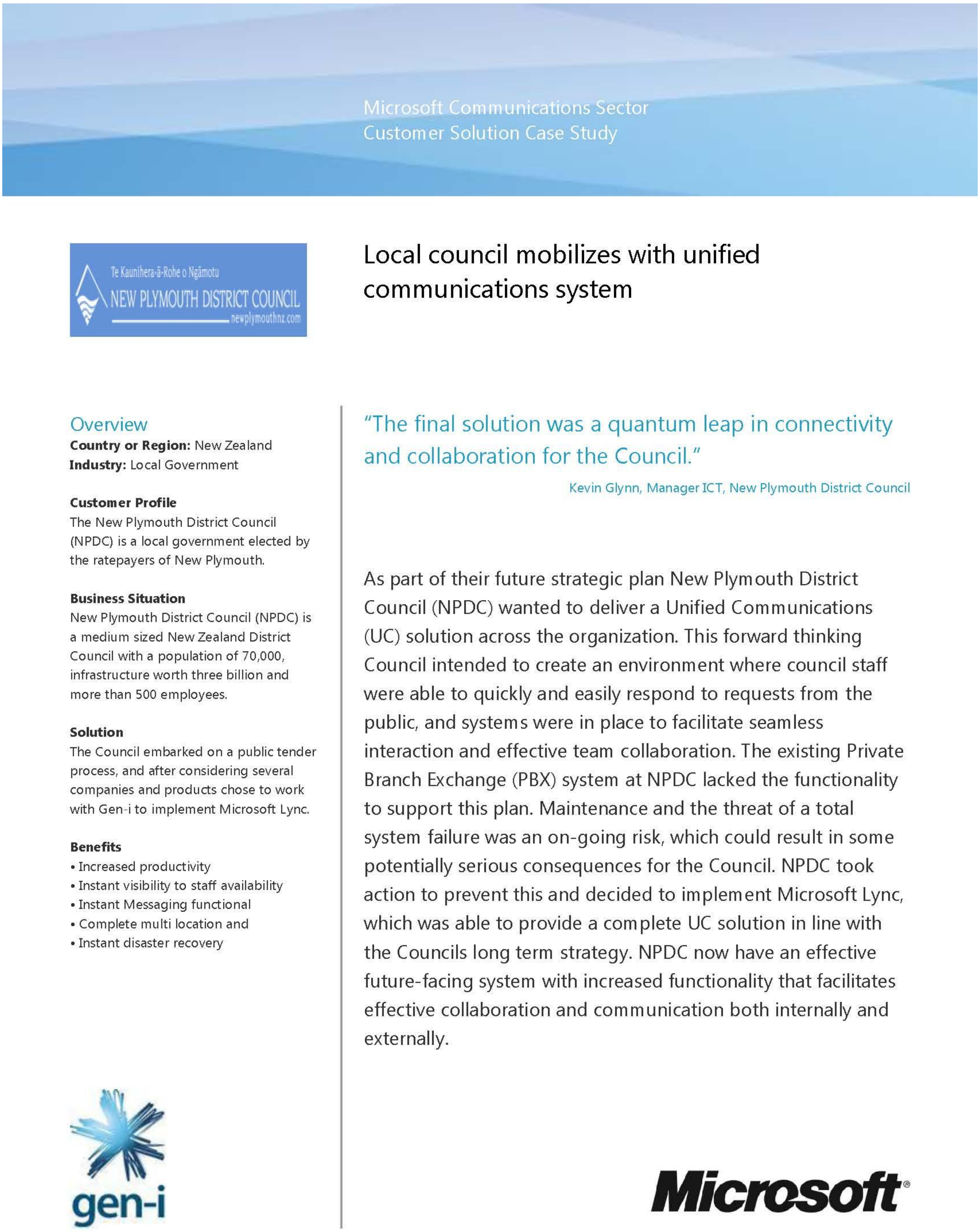
Establishes a wireless/LAN hub for multi uses to connect

Provides a communication link between satellite and internet

Additional power outlets for charging and operating extra devices

The ability to have additional Portable Operation Devices (PODs) which can carry an array of equipment

8.9. Microsoft Lync – New Plymouth District Council



Microsoft Communications Sector
Customer Solution Case Study

Te Kaunihera-ā-Rohe o Ngāmotu
NEW PLYMOUTH DISTRICT COUNCIL
newplymouthnz.com

Local council mobilizes with unified communications system

Overview

Country or Region: New Zealand
Industry: Local Government

Customer Profile
The New Plymouth District Council (NPDC) is a local government elected by the ratepayers of New Plymouth.

Business Situation
New Plymouth District Council (NPDC) is a medium sized New Zealand District Council with a population of 70,000, infrastructure worth three billion and more than 500 employees.

Solution
The Council embarked on a public tender process, and after considering several companies and products chose to work with Gen-i to implement Microsoft Lync.

Benefits

- Increased productivity
- Instant visibility to staff availability
- Instant Messaging functional
- Complete multi location and
- Instant disaster recovery

> "The final solution was a quantum leap in connectivity and collaboration for the Council."
>
> Kevin Glynn, Manager ICT, New Plymouth District Council

As part of their future strategic plan New Plymouth District Council (NPDC) wanted to deliver a Unified Communications (UC) solution across the organization. This forward thinking Council intended to create an environment where council staff were able to quickly and easily respond to requests from the public, and systems were in place to facilitate seamless interaction and effective team collaboration. The existing Private Branch Exchange (PBX) system at NPDC lacked the functionality to support this plan. Maintenance and the threat of a total system failure was an on-going risk, which could result in some potentially serious consequences for the Council. NPDC took action to prevent this and decided to implement Microsoft Lync, which was able to provide a complete UC solution in line with the Councils long term strategy. NPDC now have an effective future-facing system with increased functionality that facilitates effective collaboration and communication both internally and externally.

Situation

New Plymouth District Council (NPDC) is a medium sized New Zealand District Council with a population of 70,000, infrastructure worth three billion and more than 500 employees. The council is responsible for the management of the environmental, social, economic and cultural well-being of the New Plymouth District.

NPDC was looking to the future and had a vision of providing a robust Unified Communications (UC) solution throughout the organization. With a philosophy of content sharing, the Council aimed to provide the public with easy access to information and staff, but was increasingly restricted by the existing infrastructure.

As part of the Microsoft infrastructure Optimization (IO) model, NPDC worked through an overall strategic plan called the Data Centre Renewal and Optimisation Programme (DROP) which is made up of three phases. The second phase involved replacing the legacy PBX and contact center systems.

The existing Private Branch Exchange (PBX) had limited functionality and concerns about reliability were an ongoing source of stress for the Council. The system was impacting the Council's ability to service external customers.

NPDC required a system that was easy to use, while providing the required levels of functionality and robust collaboration needed to service the entire organization. The legacy phone system previously in place, provided some of the required functionality, but it was too complex and cumbersome for council staff to use effectively.

"Some people knew how to use certain features on the existing system, but because it was so complicated it was difficult to teach others and most people just didn't bother with them. We needed a system that was easy to use," says Kevin Glynn, Manager ICT at NPDC.

With the upcoming Rugby World Cup 2011 games planned for New Plymouth, it was the ideal time to assess the current infrastructure situation, review the needs of the organization, and select the appropriate replacement.

Solution

The Council embarked on a public tender process, and after considering several companies and products chose to work with Gen-i to implement Microsoft Lync.

Gen-i was chosen as the selected partner due to the breadth and depth of their technology capability. The system decision was based on multiple criteria – best fit, value for money, and the ability of the system to grow and change with the needs of the Council in the future.

Prior to the Microsoft Lync rollout NPDC installed the Microsoft Lync Client throughout the organization. This gave staff the opportunity to familiarize themselves with the look and feel of the system, and to utilize some of the features such as 'Presence' and 'Contacts'.

"Installing the Client allowed users to test out some of the system features before they actually had to use it and this worked really well for us," says Kevin.

A phased approach was selected for the implementation which began in May 2011 and continued through to August 2011. Part of the implementation strategy involved selecting a group of enthusiastic product advocates from a cross section of departments. This meant that there were people with varying degrees of familiarity in each department, who could then support their co-workers.

An initial pilot group of 50 users was selected for the first phase. Once this group was running successfully, the number was then expanded to 100 to test the system with higher call volumes. The next step was to roll out the Wide Area Network (WAN) based sites in August 2011, with the remote access sites completed in September 2011. The implementation ran in parallel with the existing PBX which is in the process of being phased out.

The implementation ran very smoothly, with any new system it takes time for everyone to get used to using it, but Lync is very intuitive and Council staff picked it up very quickly.

"There were no real issues, it was remarkably straightforward and people were very positive about the new system in general," says Kevin.

Benefits

Some of the benefits of implementing Microsoft Lync were realized immediately by the NPDC team. Staff learned to use the system very quickly and with minimal training. Some of the benefits include:

- Increased productivity
- Instant visibility to staff locations and availability
- Instant Messaging functionality
- Complete multi location and offsite access for staff
- Instant disaster recovery
- Future proofed solution

The ability to collaborate easily amongst groups of people has been a real time saver for the Council. Using Microsoft Lync has reduced the amount of meetings required and helped to expedite decision making. For example, when people are on a call discussing an issue and input is required from another person, it is easy to see if that person is available and invite them in to your discussion to solve the problem there and then.

Council staff can use Presence to see, at a glance, the status of colleagues – if they are busy or available, and where they are currently located in the building. They can even view a photo of the person whom they are communicating with, particularly useful in large organizations such as NPDC where staff often deal with teams in different locations that they may not have met in person before.

"The final solution was a quantum leap in connectivity and collaboration for the Council," says Kevin.

Instant Messaging (IM) is a very useful communications tool when colleagues need quick responses to questions. It allows staff members to collaborate effectively and efficiently on topics. As a topic requires further input, other users can be invited to participate in the discussion.

Microsoft Lync provides a mobile solution for NPDC staff. Users logging in to the network have the same access to Contacts, Presence and IM regardless of their location. This means that people can work from home or different locations without issue or technical changes.

One of the major advantages of a mobile solution, is that in the event of a disaster, staff can be moved to a new location and begin working almost immediately. This will reduce recovery time, costs and prevent a delay in providing council services.

For More Information

For more information about Microsoft products and services go to: www.microsoft.com

For more information about Gen-i products and services, call 09 306 4600 or visit the website at: www.gen-i.co.nz

For more information about New Plymouth District Council products and services, call 06 759 6060 or visit the website at: www.newplymouthnz.com

This case study is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Document published November 2011

Microsoft Lync has provided NPDC with a sophisticated, future proof communications tool that facilitates effective collaboration. The new system has delivered a group wide UC solution for the Council.

Microsoft Communications Sector

Microsoft Communications Sector delivers integrated, adaptable, comprehensive solutions built on innovative software. These solutions help communications service providers develop, deploy, and evolve customized and differentiated offerings that enhance the user experience.

For more information about Microsoft solutions for the Communications Sector, go to: www.microsoft.com/serviceproviders

9. Service Provider and Vendor Solutions Update

9.1. Eagle ARC GIS: Mobile Solution for Local Government

Esri offers a variety of mapping applications to help Local Government improve field operations and make more informed business decisions. These include:

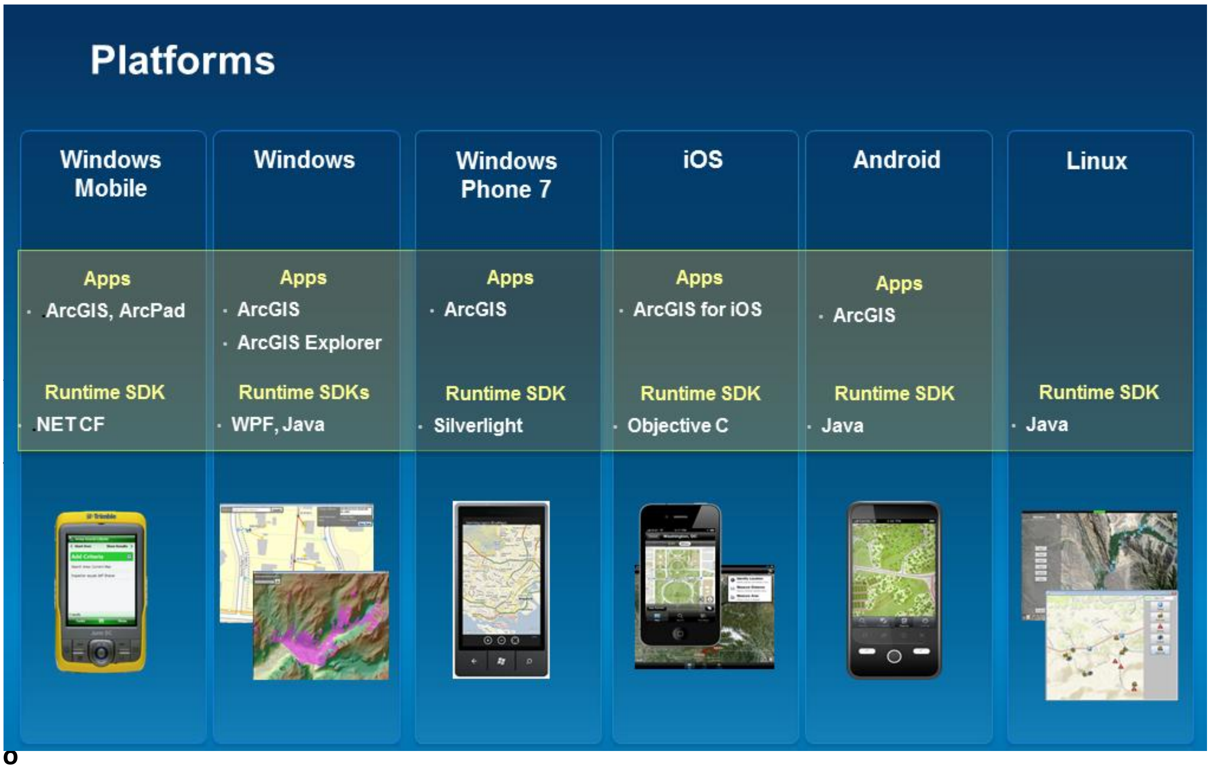
1. ArcGIS for Smartphones and Tablets – includes applications for Windows, Android and iOS devices.

2. ArcGIS for Windows Mobile - task-driven mobile GIS application for Windows Mobile and Windows tablet devices

3. ArcPad - map-centric and Windows-based field mapping and data collection application for GIS professionals.

The options can then be further divided into ready-to-deploy field applications, or ArcGIS Runtime SDK's which allow developers to leverage native software development kits for each mobile platform and either extend the configurable applications, or to build highly focused apps that target specific devices and workflow needs.

This is best summarised in the illustration below:



Platforms

Windows Mobile	Windows	Windows Phone 7	iOS	Android	Linux
Apps · ArcGIS, ArcPad	Apps · ArcGIS · ArcGIS Explorer	Apps · ArcGIS	Apps · ArcGIS for iOS	Apps · ArcGIS	
Runtime SDK .NET CF	Runtime SDKs · WPF, Java	Runtime SDK · Silverlight	Runtime SDK · Objective C	Runtime SDK · Java	Runtime SDK · Java

o

Ready-to-deploy applications

ArcGIS includes ready-to-deploy field applications that span the smartphone, tablet and rugged device platforms:

Mobile applications—ArcGIS is available on smartphones and tablets as a configurable application that can:

- Explore a collection of maps published and shared using ArcGIS Online
- Query map layers
- Collect new spatial information in the field

It is available on iPhone, iPad and iPod touch devices, Android phones and tablets and Windows Phone devices.

ArcGIS for Windows Mobile—Includes a task-driven mobile application optimised for Windows Mobile and Windows Tablet devices. The application can use either a web services architecture to synchronize information between the field and office or a desktop check-out and check-in workflow. Field maps and field workflows are configurable using a desktop application called Mobile Project Center. The application includes tasks for field map viewing, field inspection, and field data collection; it targets non-GIS professionals who are managing/collecting assets, are responding to incidents, and/or are in need of high accuracy GPS in harsh conditions that require fully disconnected use. ArcGIS for Windows Mobile includes an SDK (described below).

ArcPad—Includes a map-centric application that focuses on field tasks that require relatively simple geographic tools. These tasks are typically performed on handheld and tablet computers. Providing a set of tools, ArcPad targets the GIS professional that demands flexibility and sophistication from the tools that they use. ArcPad is not recommended for use by non-GIS processionals; the level of training required is quite high.

ArcGIS Runtime SDKs

ArcGIS is available as native software development toolkits for both smartphone and tablet platforms as well as the Windows desktop and Windows Mobile platforms:

1. Smartphones and tablets

    - ArcGIS Runtime SDK for Android—A Java developer toolkit used to develop Android applications that can be deployed within an organisation or to Google Play.
    - ArcGIS Runtime SDK for iOS—A native Objective C developer toolkit used to develop iPhone/iPad and iPod touch applications that can be deployed within an organisation or to the iTunes App Store.
    - ArcGIS Runtime SDK for Windows Phone—A Silverlight developer toolkit used to develop Windows Phone applications that can be deployed to the Zune Marketplace.

2. Tablets, notebooks, and rugged mobile devices

    - ArcGIS Runtime SDK for WPF—A developer toolkit used to develop Windows applications that can be deployed within an organization.
    - ArcGIS Runtime SDK for Java—Java developer toolkit used to develop Java applications that can be deployed within an organization.

- ArcGIS Runtime SDK for Windows Mobile—A developer toolkit used to:
  - Develop standalone applications and embed GIS functionality into existing applications for Windows Mobile and Windows running on notebooks, tablets, and desktops
  - Develop custom tasks/extensions for the ArcGIS for Windows Mobile field applications

The ArcGIS Web APIs for JavaScript and Flex can also be used to build cross platform mobile applications, either as browser-based applications or native applications through the use of third-party tools. Developers can quickly provide connected mobile applications to multiple operating systems with minimal effort. If you need to target a mobile workforce that uses a wide range of devices (Apple, Android, Blackberry) and do not have the time or resources to build native applications, then building a cross-platform mobile web solution may be the right solution.

To learn more read about the following APIs:

- ArcGIS API for Javascript—Leverage the compact version of the Javascript API to target mobile devices. View mobile samples in the Mobile folder in the JavaScript samples area.
- ArcGIS API for Flex—Use the Flex Mobile framework with the Flex API to target mobile devices.

Building mobile solutions

Building a great mobile solution starts with a good understanding of the needs and habits of your mobile workforce (are they in the office or out, connected to the web when working or not, working in harsh field conditions or the comfort of a vehicle, experience with mobile devices or used to working with paper). Understanding their needs and habits will guide you to either build your own focused application using the SDKs or to configuring and possibly extending the ready-to-deploy mobile apps.

Critical to the success of the solution is to define and create the map resources used inside of your mobile applications. Workflows start with the building of a strong information model. For example, when replacing a paper-based workflow the information type definition will drive the look and feel of the form that replaces paper.

Additional Comments

Nearly 65% of all NZ Local Government have access to ArcGIS software, many of which have an Enterprise Licence Agreement (ELA) with Esri which entitles them to use unlimited deployments of ArcGIS products, including the Mobile products listed above.

Esri also provide a number of JavaScript/HTML 5 application templates for local government that that can be used by the public on a desktop, mobile phone, or tablet device. These include:

- “Citizen Service Request” - is typically used by public works agencies, water utilities, or other local government organisations to deliver a web-based service request application

- “Election Polling Places” - is a application that helps people locate their election polling place, comment on conditions at the polling place, and obtain information about currently elected officials

- “The Tax Parcel Viewer” - provides the general public and other interested parties local government property rating and assessment information

Summary of Esri’s stance on adopting HMTL5:

http://blogs.esri.com/esri/arcgis/2011/11/17/some-thoughts-on-the-direction-of-the-arcgis-web-mapping-apis-javascript-flex-and-silverlight/

9.2. Kaon

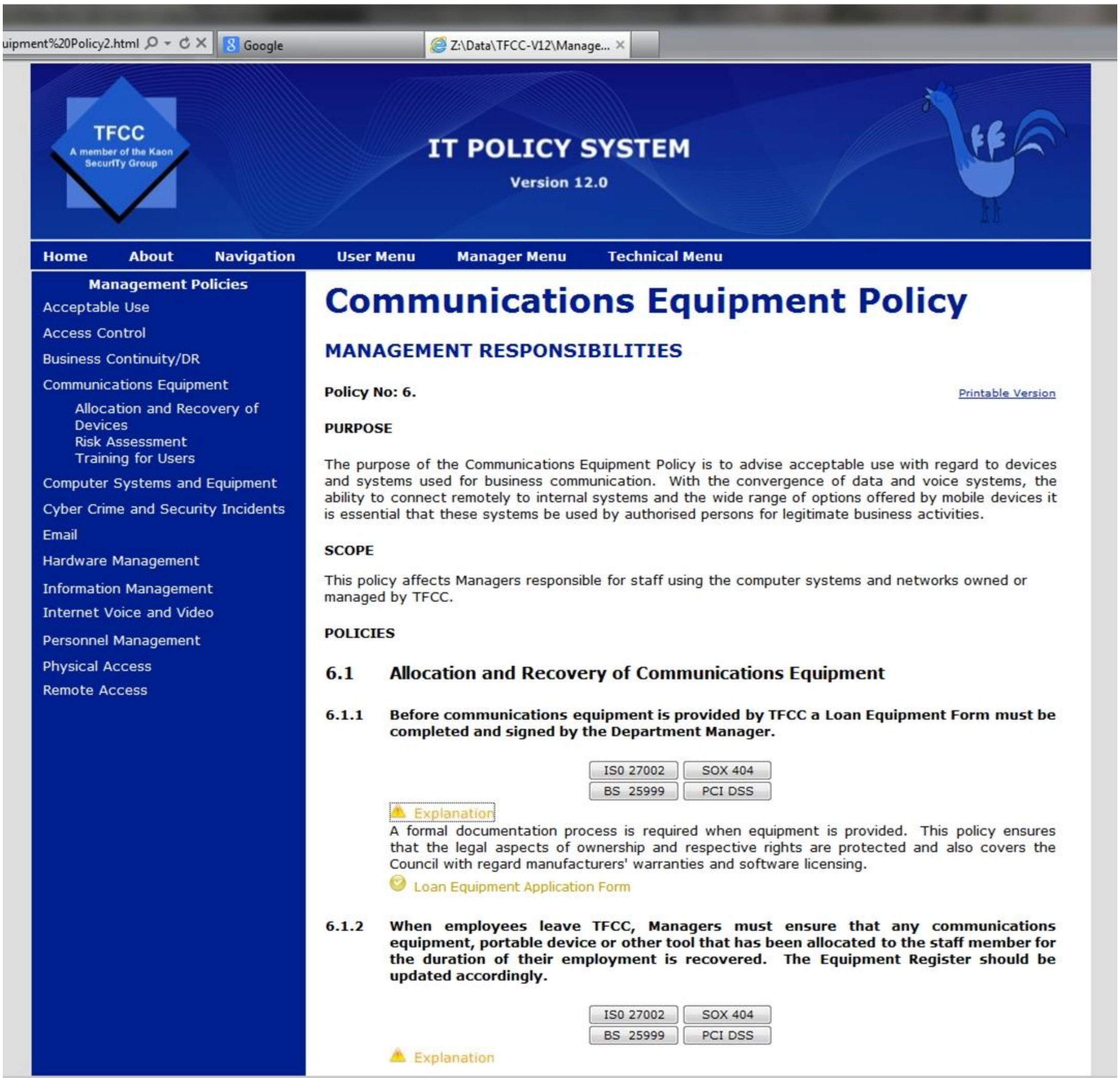
Kaon provides comprehensive web-based policy development tools and security services to around one third on the Local Government organisations in New Zealand.

The web-based template approach helps Councils fast-track policy creation, updates and deployment to all staff. It also covers standards compliance features and views for different levels of users and managers.

The system is kept up-to-date with the latest developments including the creation of policies to handle mobile BYOD policies.

See appendices for an abbreviated sample Mobile Device Policy provided by Kaon and a SecurITy services overview.

Here is how the well-designed web-based interface looks for the **Communications Equipment Policy:**



Communications Equipment Policy

MANAGEMENT RESPONSIBILITIES

Policy No: 6.

PURPOSE

The purpose of the Communications Equipment Policy is to advise acceptable use with regard to devices and systems used for business communication. With the convergence of data and voice systems, the ability to connect remotely to internal systems and the wide range of options offered by mobile devices it is essential that these systems be used by authorised persons for legitimate business activities.

SCOPE

This policy affects Managers responsible for staff using the computer systems and networks owned or managed by TFCC.

POLICIES

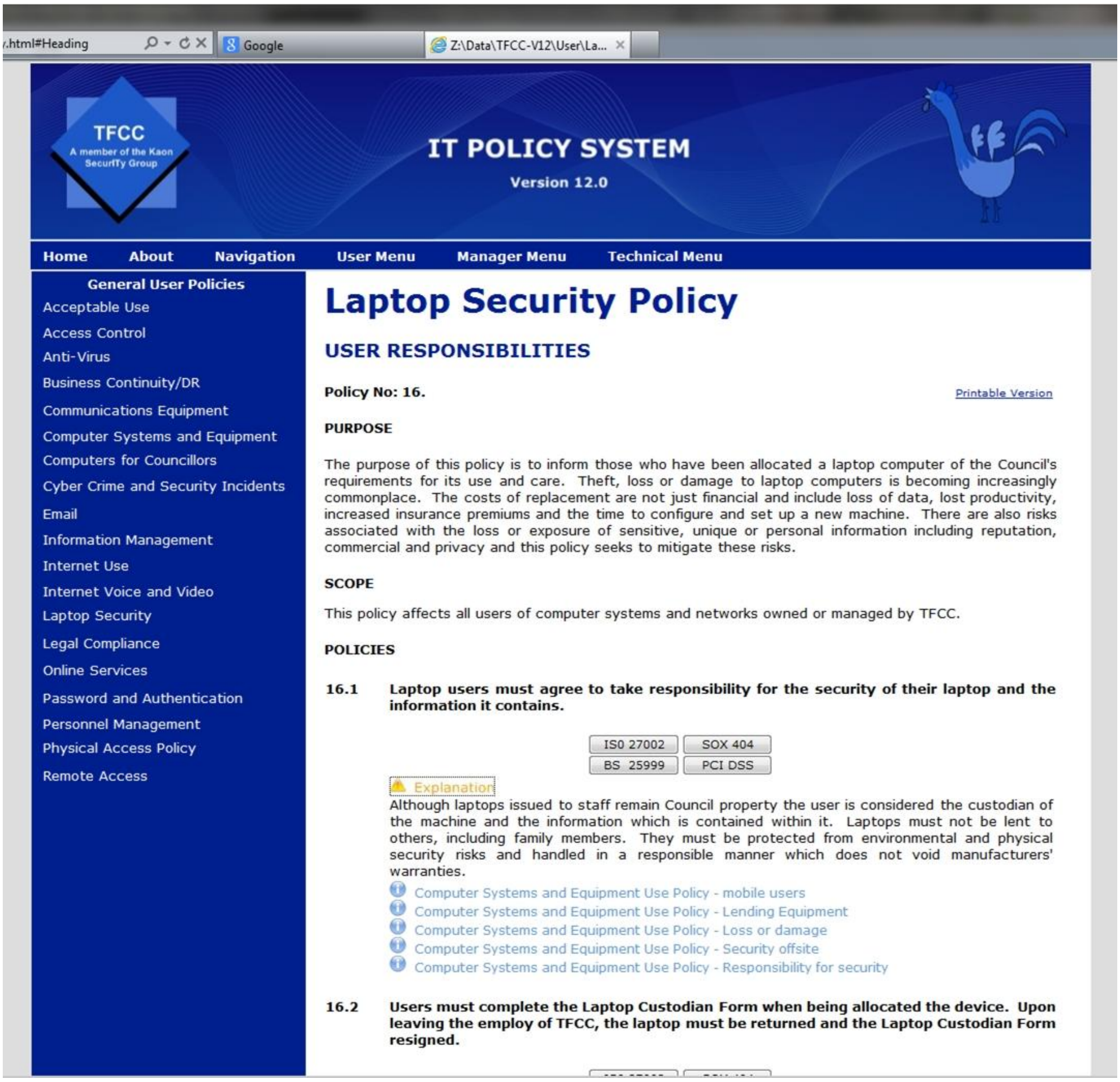
6.1 Allocation and Recovery of Communications Equipment

6.1.1 Before communications equipment is provided by TFCC a Loan Equipment Form must be completed and signed by the Department Manager.

A formal documentation process is required when equipment is provided. This policy ensures that the legal aspects of ownership and respective rights are protected and also covers the Council with regard manufacturers' warranties and software licensing.

6.1.2 When employees leave TFCC, Managers must ensure that any communications equipment, portable device or other tool that has been allocated to the staff member for the duration of their employment is recovered. The Equipment Register should be updated accordingly.

Laptop Security Policy Screen:



Laptop Security Policy

USER RESPONSIBILITIES

Policy No: 16.

PURPOSE

The purpose of this policy is to inform those who have been allocated a laptop computer of the Council's requirements for its use and care. Theft, loss or damage to laptop computers is becoming increasingly commonplace. The costs of replacement are not just financial and include loss of data, lost productivity, increased insurance premiums and the time to configure and set up a new machine. There are also risks associated with the loss or exposure of sensitive, unique or personal information including reputation, commercial and privacy and this policy seeks to mitigate these risks.

SCOPE

This policy affects all users of computer systems and networks owned or managed by TFCC.

POLICIES

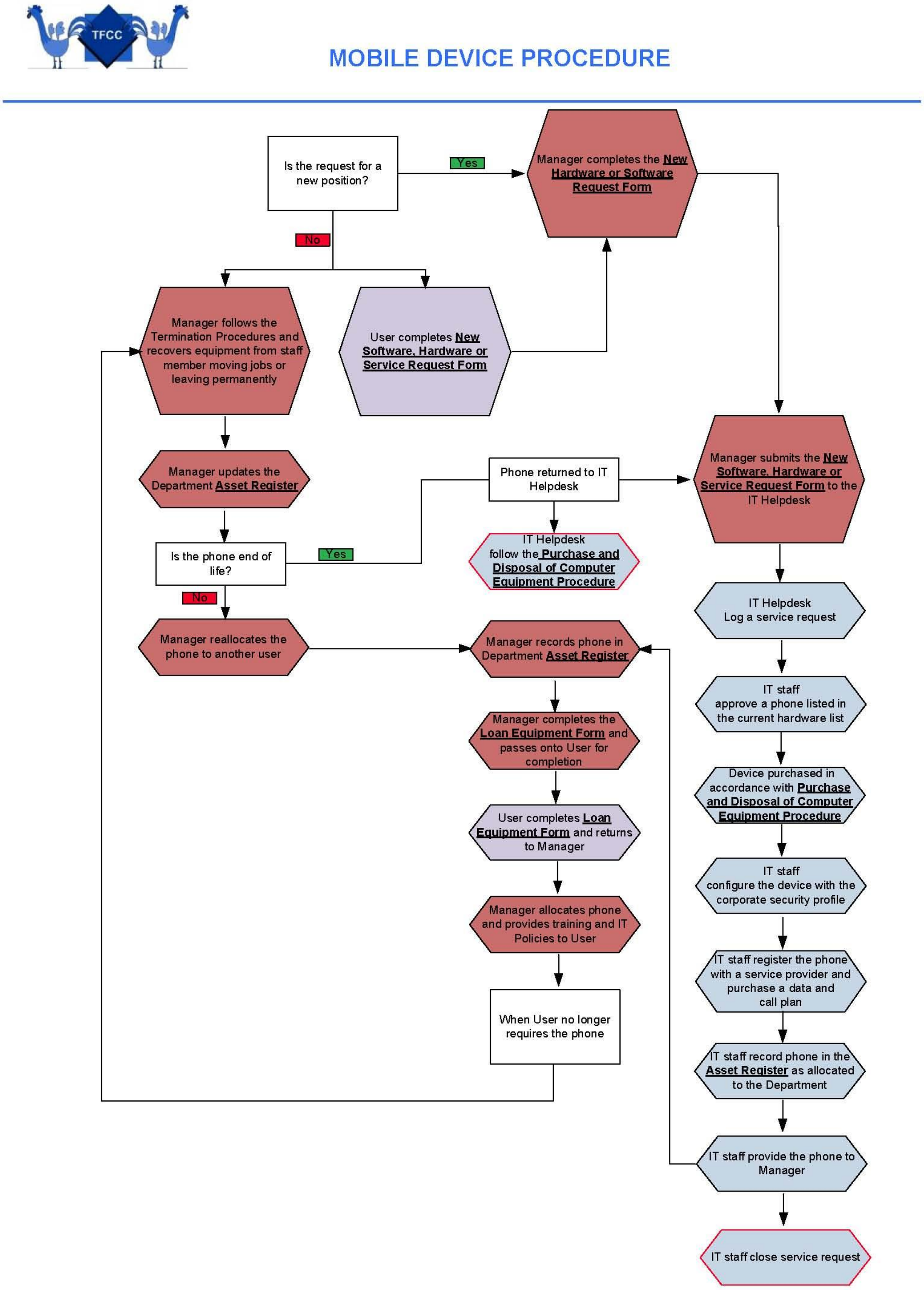
16.1 **Laptop users must agree to take responsibility for the security of their laptop and the information it contains.**

Although laptops issued to staff remain Council property the user is considered the custodian of the machine and the information which is contained within it. Laptops must not be lent to others, including family members. They must be protected from environmental and physical security risks and handled in a responsible manner which does not void manufacturers' warranties.

- Computer Systems and Equipment Use Policy - mobile users
- Computer Systems and Equipment Use Policy - Lending Equipment
- Computer Systems and Equipment Use Policy - Loss or damage
- Computer Systems and Equipment Use Policy - Security offsite
- Computer Systems and Equipment Use Policy - Responsibility for security

16.2 **Users must complete the Laptop Custodian Form when being allocated the device. Upon leaving the employ of TFCC, the laptop must be returned and the Laptop Custodian Form resigned.**

New Mobile Device Procedure Process Example:


TFCC
MOBILE DEVICE PROCEDURE
Is the request for a new position?
Yes
No
Manager completes the New Hardware or Software Request Form
Manager follows the Termination Procedures and recovers equipment from staff member moving jobs or leaving permanently
User completes New Software, Hardware or Service Request Form
Manager updates the Department Asset Register
Phone returned to IT Helpdesk
Manager submits the New Software, Hardware or Service Request Form to the IT Helpdesk
IT Helpdesk follow the Purchase and Disposal of Computer Equipment Procedure
Is the phone end of life?
Yes
No
IT Helpdesk Log a service request
Manager reallocates the phone to another user
Manager records phone in Department Asset Register
IT staff approve a phone listed in the current hardware list
Manager completes the Loan Equipment Form and passes onto User for completion
Device purchased in accordance with Purchase and Disposal of Computer Equipment Procedure
User completes Loan Equipment Form and returns to Manager
IT staff configure the device with the corporate security profile
Manager allocates phone and provides training and IT Policies to User
IT staff register the phone with a service provider and purchase a data and call plan
When User no longer requires the phone
IT staff record phone in the Asset Register as allocated to the Department
IT staff provide the phone to Manager
IT staff close service request

Note: Items highlighted in bold and underlined are associated with other forms, procedures or processes.

	RESPONSIBILITY FOR THIS PROCEDURE: MANAGERS
	ACCOUNTABILITY FOR THIS PROCEDURE: IT MANAGER
	VERSION:1.0 UPDATED: 31 JANUARY 2012
	ROLES AFFECTED BY THIS PROCEDURE
🟥	Managers
🟦	IT staff, IT Helpdesk staff
🟪	Computer User
	OTHER RELEVANT DOCUMENTS:
✓	New Hardware or Software Request Form
✓	Loan Equipment Form
ℹ	Purchase and Disposal of Computer Equipment Procedure
ℹ	New Hardware Procedure
ℹ	Communications Equipment Policy
ℹ	Asset Register

9.3. Origen Ozone

See section 8 for Origen case studies.

mobility by design

When there is the requirement within an organisation for mobility it is very important that the architecture and design of the current systems are able to support the solution. The Ozone product is designed from the ground up to support Cloud, SaaS and distributed processing architectures with 100% services based execution of all business logic.

Many of Ozone's modules have been extended into the mobile space with web, virtualization and remote desktop, increasing the reach and efficiency of the system. Modules such as Contact Centre, Purchase Orders, Accounts Payable, Time sheeting, Inspections, Environmental Monitoring, Animal Control all embrace the requirement for mobile information.

extensibility

The extensibility of the Ozone product encourages Ozone customers to adapt and evolve the capabilities by layering additional function on top of the Ozone solution.

In many cases Ozone web services have been successfully used by Ozone customers to develop their own integration to industry specific solutions.

ozone mobile

Although the Ozone architecture encourages mobility via existing technologies there are always a number of risks with 3rd party integration, and maintaining a number of different applications on the device is not ideal.

For this reason Origen’s direction with Ozone Mobile is for an application that is deployed and managed by the Ozone server. Ozone Mobile will take mobile data to the next level for Ozone customers, providing both the data and configuration of the mobile device from the Cloud (Ozone servers).

Ozone Mobile is a flexible platform that extends the current Ozone application framework, providing administration of mobile devices, UI forms, data selection and synchronisation, security and platform independence.

This solution will be developed to provide standard features expected of a mobile platform such as offline storage, offline data validation, native application support, and device hardware support (GPS, Photos, Maps).

Benefits of this approach include:

- Any smart device is supported
- Councils can configure mobile device for any function
- No complicated integration is required

- Offline operation is possible

Ozone mobile will be supported on 4” screens to 10.1” screen tablets, touch screen.

When data is synchronised to a device, if the device goes offline the data in the mobile business object will be stamped as offline also, so that users with the same data on multiple devices cannot overwrite and synchronise data overwriting each other’s data.

When the Ozone mobile device is online data will be synchronised with the mobile business object on the server automatically based on the selection criteria entered, data will be validated when synchronised to ensure validation rules are met. And event logic on the mobile business object will be executed to perform business rule and workflow checks.

When the Ozone mobile device is offline data will be stored in local storage on the device, data will be marked as un-synchronised and when the device is online again the data will be validated and synchronised with the mobile business object. Data that fails the validation will be highlighted to the device user.

9.4. Sophos

SSS have around 50 council customers with various security and mobile device management products. 40 of these have Sophos Endpoint Security Advanced. See case study on this product in section 8.

User-based licensing for all Local Government organisations is based on 15,000 users, which provides very attractive pricing.

Sophos has announced a free anti-virus app for Google Android devices which uses a Sophos Cloud service. It also has also announced Android and Apple iOS apps for securing files held in DropBox (Personal Cloud storage).

> *The Sophos anti-virus app for Android will be free in November and will be integrated into The Sophos mobile-device management software Sophos Mobile Control. "It acts as a scanner and looks for malicious apps and malware," says Payal Mehrotra, Sophos mobile product manage.*

Sophos Mobile Control

- Sophos Mobile Control product is designed to keep all your mobile phones and tablets safe, whether it is an IOS, Android, Windows or Blackberry device. Sophos does so by providing you with two cloud based management portals; The self service portal for your employees and the management interface for your IT team.
- Self Service Portal (SSP) : This portal is designed to deal with the BYOD scenario and allows your employee to log on and register their own device which can then be managed securely by the IT team. Using the SSP the employee can be given the right to lock, wipe, locate and backup their device in case of the device being lost or stolen. This is especially important on weekends as they have no or limited means to contact the IT admin or manager.
- Management Interface (MI): Once devices have been registered through the SSP or the MI the IT team can manage the mobile device fleet. The IM allows you to: Create policies, block applications, monitor bandwidth usage, send text messages, locate devices, create a corporate app portal, delete devices, wipe phones, decommission phones and profiles and much more.

Sophos Mobile Security Free Edition

This free version of Sophos Mobile Control is for Androids only and has no central management portal. It is designed to keep individual Android users safe as the Android platform is more prone to infections due to its open source design. It allows you to scan apps for malicious code, scan your apps and grey list them as well as performing a remote lock through a second mobile phone. Tracking of the device is also possible through in build location awareness of Android phones.

Sophos UTM (ex Astaro)

- Sophos new UTM devices have various features to help secure mobile workforce's, such as Wireless Protection, HTML5, VPN Clients and Network Protection.

- Wirless Proetction/Management: Your wireless networks need the same policies and protection as the wired network. This can be difficult without a way to centrally manage the network and extend your security. We give you these capabilities with Wireless Protection. Now the wireless network is easily managed and protected, ensuring consistency across your organization. Sophos UTM acts as a wireless controller, centrally managing Sophos Wireless Access Points. All configuration, logging and troubleshooting is done within the UTM appliance. ophos Wireless Access Points are similar to thin clients in relation to the Sophos UTM. Intelligence in the access points is minimized and centralized in the Sophos UTM instead. Our built-in reporting displays information about connected wireless clients without the need for a separate tool. Controlling your wireless networks has never been easier.

- HTML5 provides controlled network access to third parties and IT staff who are outside of the office. Our HTML5 VPN Portal allows access from anywhere.

- VPN Clients: With more and more people working outside the main office, you need an easy and secure means of connecting them to the corporate network. Sophos VPN Clients let you do that with options and how to allow users to connect..

- Network Protection: Sophos Network Protection includes many fully integrated features: an intrusion prevention system, denial-of-service protection, a VPN gateway, an HTML5 VPN portal, advanced routing and more. We help protect your network by keeping bad traffic out and enabling secure access to authorised users.

Web Protection Suite

- The Sophos Web Protection Suite allows you to easily manage iPads, mobile devices, shared workstations, guest access and more.

- Control access by device or network segment; Enable user logins from iPads or other devices; easily manage guest access; utilise single sign-on for macs; allow web applications to work seamlessly; create location-aware policies and suppress activity logging to protect privacy.

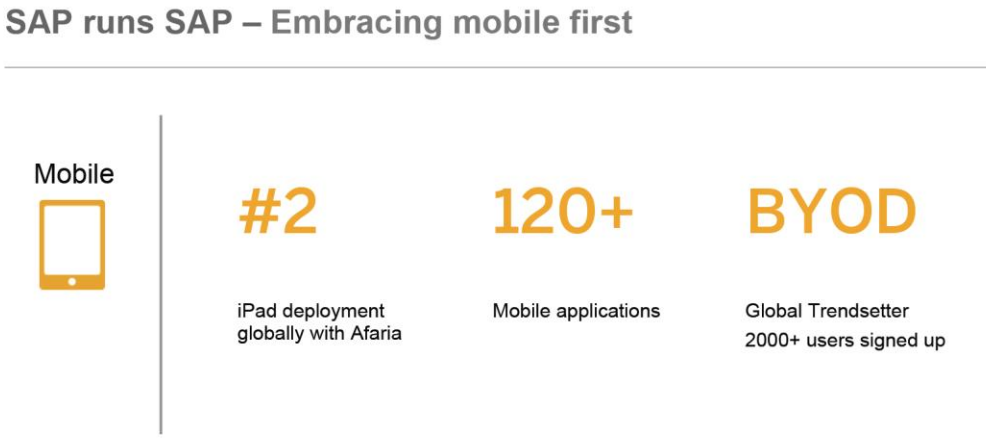
- This is important as you can have different policies for different devices and the way in which these devices connect into the network. For example you could define a policy for ipads connecting on the wifi vs laptops connecting on the LAN.

9.5. SAP

SAP not only provides applications for Local Government (e.g. as used by Auckland City Council), but also provides a world-leading Mobile Enterprise Application Platform (MEAP) for developing mobile applications that tap into your existing systems. SAP also provides a world-leading Mobile Device Management solution, called Afaria that they have used to deploy over 2000 BYOD users so far. It can be configured to allow users to enrol and manage their devices, even lock or wipe their device if lost. This is a very efficient approach for growing numbers of users in a medium to large organisation. Auckland City Council and Wellington Regional Councils are looking at Afaria.

SAP has serious scale:

- 60,000 employees worldwide
- Over 3800 staff in IT Globally
- Managing 77,000 PCs/Laptops, 29,000 Smartphones, 14,500 iPads
- Managing 46,000 Servers (Physical & Virtual)



SAP runs SAP – Embracing mobile first

Mobile

#2

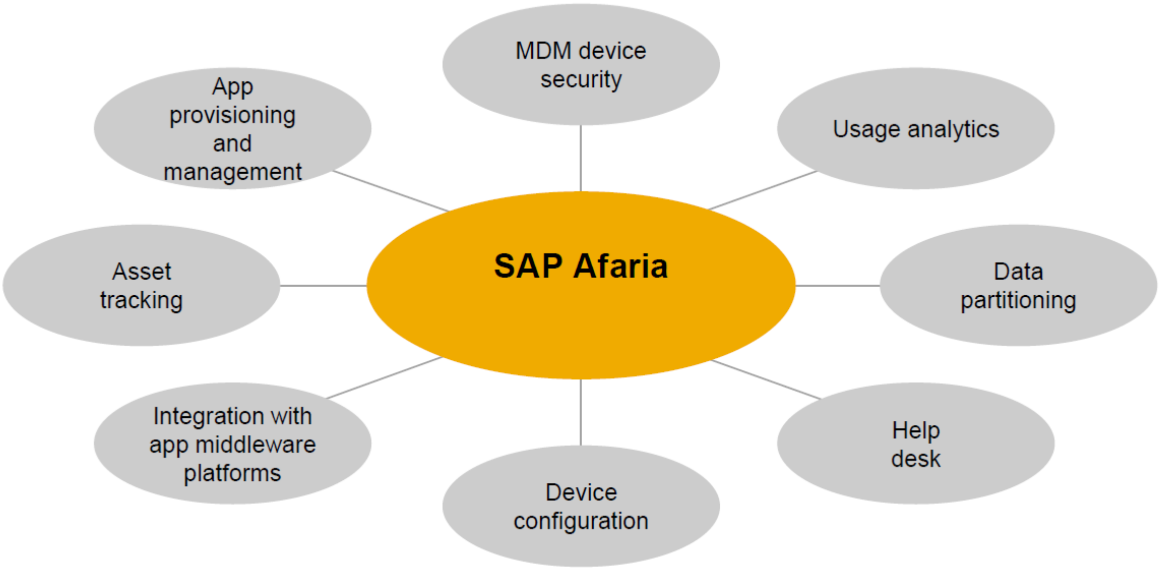
iPad deployment globally with Afaria

120+

Mobile applications

BYOD

Global Trendsetter
2000+ users signed up



SAP Afaria

MDM device security

Usage analytics

Data partitioning

Help desk

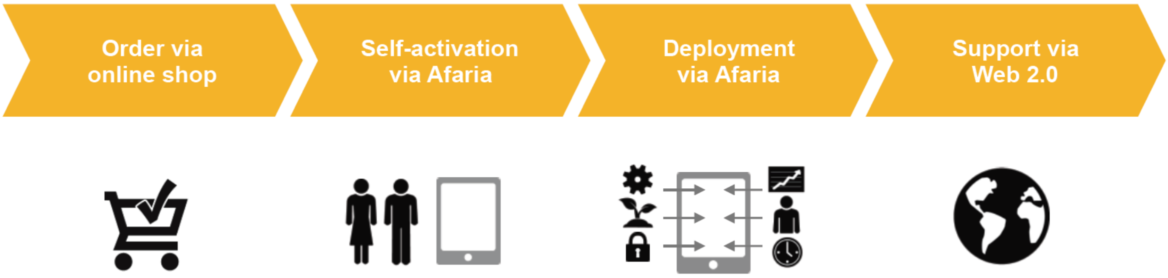
Device configuration

Integration with app middleware platforms

Asset tracking

App provisioning and management

Enterprise mobility process management with SAP Afaria



Security

- Enforcement of password settings
- Push Wi-Fi and VPN certificates
- Reporting to ensure compliance
- Access control
- Application-level control
- Remote lock and wipe

Introduction of iPhone/iPad – Offering “what’s included”

Mail / Exchange ActiveSync (EAS)

- MS Exchange 2007 backend, access via reverse proxy & CAS (loadbalanced)
- Secured with SSL, login with domain credentials

VPN

- Central IPsec gateway up to 5000 concurrent users
- Generic access to SAP corporate network and internal scenarios (dev/demo/prod)
- Login with SecurID authentication

Citrix / Windows Terminal Server

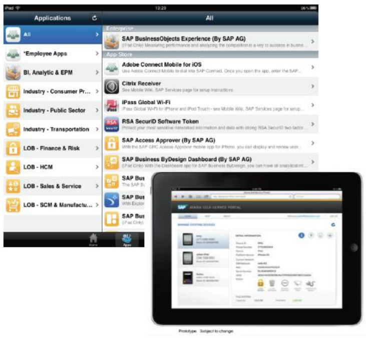
- External access (with SecurID authentication), also for personal devices
- Offers full windows desktop as well as selected published apps (e.g. SAPGUI)

Single Sign-On with client certificates has been adapted on mobile device

- Client certificates are SAPs preferred solution for backend system login
- User can transfer client certificates to the iPhone or iPad with a self-service

Mobile Device Mgmt. for iPhone/iPad – App Distribution

Afaria Client

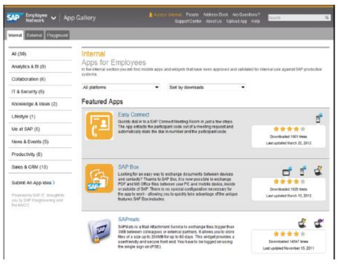


SAP BusinessObjects Experience (By SAP AG)
Adobe Connect Mobile for iOS
Use Adobe Connect Mobile to dial into SAP Connect. Once you open the app, enter the SAP...
Citrix Receiver
See Mobile Wiki, SAP Services page for setup instructions
iPass Global Wi-Fi
iPass Global Wi-Fi for iPhone and iPod Touch - see Mobile Wiki, SAP Services page for setup...
RSA SecurID Software Token
Protect your most sensitive networked information and data with strong RSA SecurID two-factor...
SAP Access Approver (By SAP AG)
With the SAP GRC Access Approver mobile app for iPhone, you can display and review user...
SAP Business ByDesign Dashboard (By SAP AG)
(iPad Only) With the Dashboard app for SAP Business ByDesign, you can have all analytical int...

Prototype. Subject to change

SAP Store for Mobile Solutions

App Gallery



All (39)
Analytics & BI (9)
Collaboration (6)
IT & Security (5)
Knowledge & Ideas (2)
Lifestyle (1)
Me at SAP (5)
News & Events (5)
Productivity (8)
Sales & CRM (13)
Submit An App Idea

Internal
Apps for Employees

Featured Apps

Easy Connect
Quickly dial in to a SAP Connect Meeting Room in just a few steps. The App extracts the participant code out of a meeting request and automatically dials the dial in number and the participant code.
Downloaded 1901 times
Last updated March 22, 2012

SAP Box
Looking for an easy way to exchange documents between devices and contacts? Thanks to SAP Box, it is now possible to exchange PDF and MS Office files between your PC and mobile device, inside or outside of SAP. There is no special configuration necessary for the app to work - allowing you to quickly take advantage of the unique features SAP Box includes.
Downloaded 1620 times
Last updated March 15, 2012

SAPmats
SAPMats is a Mail Attachment Service to exchange files bigger than 3MB between colleagues or external partners. It allows you to store files of a size up to 200MB for up to 60 days. This widget provides a userfriendly and secure front end. You have to be logged on using the simple sign on (PSE).
Downloaded 14547 times
Last updated November 15, 2011

Introduction of iPhone/iPad
#1 Challenge - Security

Challenge: Finding the right balance between **Business** requirements and **IT Security** requirements

Response: Definition of minimum security requirements / enforcement

Mobile devices to access/store corporate data

- Mandatory password
- Device (hardware) encryption
- Remote wipe/lock possibility

Corporate services / apps used on mobile devices

- Encryption of “data in transit”
- User authentication with certificates (default SAP Single Sign-On solution)
- Policy enforcement and remote administration for iOS devices using SAP Afaria

Bring your own device (BYOD)

Key requirements and stakeholders involved

Legal
- Privacy laws
- Country regulations
- Litigation requirements

HR
- Clear procedures
- HR team trained

Finance
- Reimbursement approach
- Contract obligations
- Tax implications

IT
- Manage with Afaria, custom for BYOD
- Support for device
- SAP security requirements

Communication
- Senior Executive
- Communication to employees

Key take-aways

The confluence of mobile, cloud and in-memory is a once-in-a-generation event

Embrace a "mobile first" mindset

Make your end users a core part of your design process

Consumerization and BYOD are here to stay

Access performance as easy as email

Ensure proper security and encryption

Learn from consumer innovation in the enterprise

9.6. Technology One

Property & Rating Mobile

iCouncil Inspections

TechnologyOne iCouncil Inspections for iPad® improves council service levels by maximising time spent in the field and allows information to be recorded once, accurately and easily.

Developed for iPhone® and iPad®

...ription
...erform Checkbox Health Inspection

Inspection ID
343545

Application ID
HLTHR/2008-0030

Application Description
Perform Health Inspection

Inspection Address
6 AUTUMN DRIVE EAST
DEVONPORT 7310

Contacts

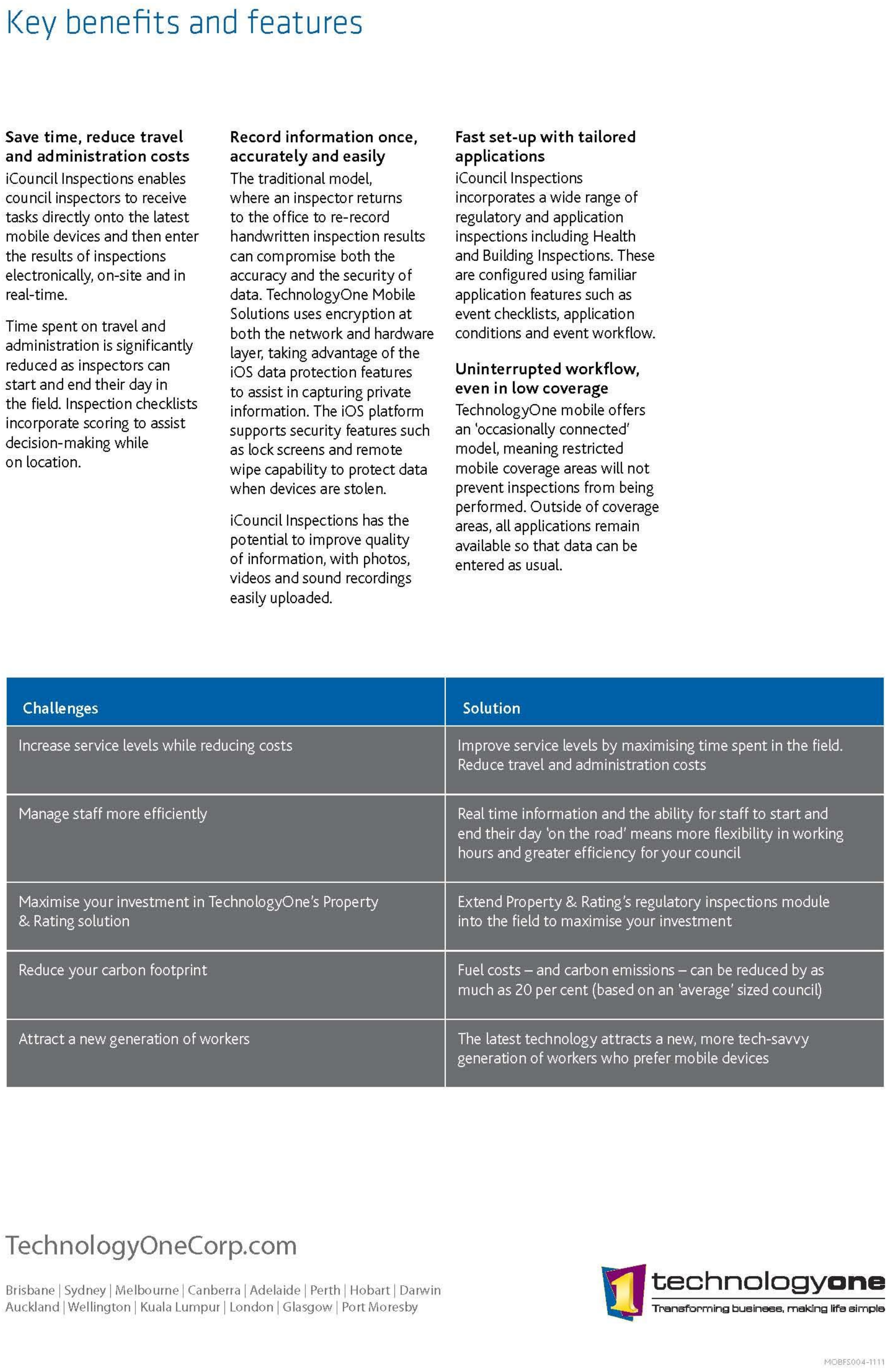
TIM CHARLES
WRIGHT
Applicant/Owner

Work: 9753
Mobile: 0439479063
Home: 0712348765
Fax:
Email: t.c.wright@doesntexist.org

Residential Address
6 AUTUMN DRIVE EAST
DEVONPORT 7310

- ✓ Designed specifically for mobile workers, with a focus on local government activities and workflows
- ✓ Tasks and information can be delivered directly to and from the mobile device, enabling staff to start and end their day in the field
- ✓ Delivers a wide range of regulatory and application inspections, including health and building inspections
- ✓ Uses familiar application features such as event checklists, application conditions and events workflow to minimise training and enable fast set-up
- ✓ Photographs, sound recordings and video can be easily uploaded to add greater context
- ✓ Work can continue uninterrupted even where no 3G or wi-fi coverage is available

technologyone
Transforming business, making life simple



Key benefits and features

Save time, reduce travel and administration costs
iCouncil Inspections enables council inspectors to receive tasks directly onto the latest mobile devices and then enter the results of inspections electronically, on-site and in real-time.

Time spent on travel and administration is significantly reduced as inspectors can start and end their day in the field. Inspection checklists incorporate scoring to assist decision-making while on location.

Record information once, accurately and easily
The traditional model, where an inspector returns to the office to re-record handwritten inspection results can compromise both the accuracy and the security of data. TechnologyOne Mobile Solutions uses encryption at both the network and hardware layer, taking advantage of the iOS data protection features to assist in capturing private information. The iOS platform supports security features such as lock screens and remote wipe capability to protect data when devices are stolen.

iCouncil Inspections has the potential to improve quality of information, with photos, videos and sound recordings easily uploaded.

Fast set-up with tailored applications
iCouncil Inspections incorporates a wide range of regulatory and application inspections including Health and Building Inspections. These are configured using familiar application features such as event checklists, application conditions and event workflow.

Uninterrupted workflow, even in low coverage
TechnologyOne mobile offers an 'occasionally connected' model, meaning restricted mobile coverage areas will not prevent inspections from being performed. Outside of coverage areas, all applications remain available so that data can be entered as usual.

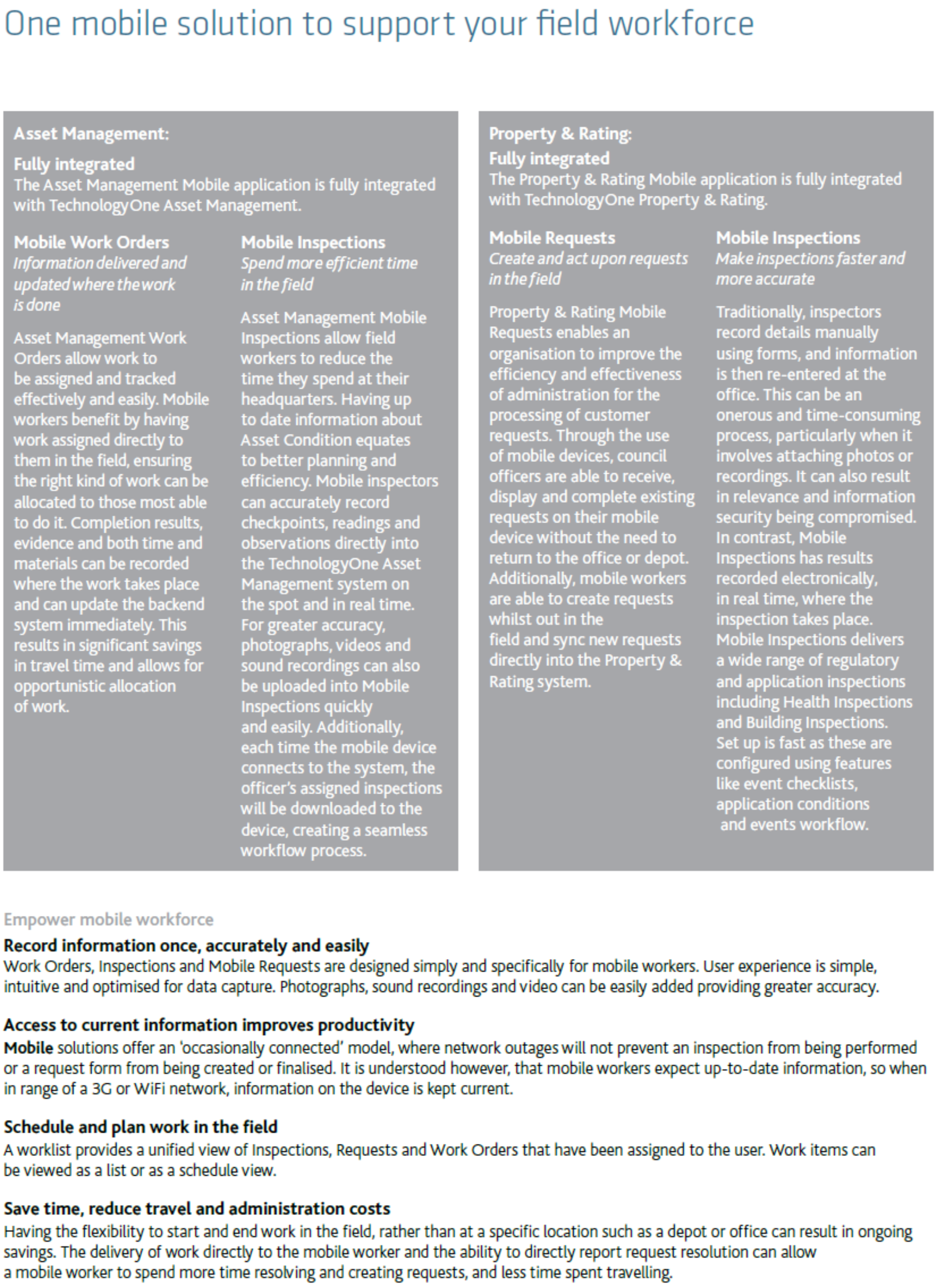
Challenges	Solution
Increase service levels while reducing costs	Improve service levels by maximising time spent in the field. Reduce travel and administration costs
Manage staff more efficiently	Real time information and the ability for staff to start and end their day 'on the road' means more flexibility in working hours and greater efficiency for your council
Maximise your investment in TechnologyOne's Property & Rating solution	Extend Property & Rating's regulatory inspections module into the field to maximise your investment
Reduce your carbon footprint	Fuel costs – and carbon emissions – can be reduced by as much as 20 per cent (based on an 'average' sized council)
Attract a new generation of workers	The latest technology attracts a new, more tech-savvy generation of workers who prefer mobile devices

TechnologyOneCorp.com

Brisbane | Sydney | Melbourne | Canberra | Adelaide | Perth | Hobart | Darwin
Auckland | Wellington | Kuala Lumpur | London | Glasgow | Port Moresby

technologyone
Transforming business, making life simple

MOBFS004-1111



One mobile solution to support your field workforce

Asset Management:

Fully integrated
The Asset Management Mobile application is fully integrated with TechnologyOne Asset Management.

Mobile Work Orders
Information delivered and updated where the work is done

Asset Management Work Orders allow work to be assigned and tracked effectively and easily. Mobile workers benefit by having work assigned directly to them in the field, ensuring the right kind of work can be allocated to those most able to do it. Completion results, evidence and both time and materials can be recorded where the work takes place and can update the backend system immediately. This results in significant savings in travel time and allows for opportunistic allocation of work.

Mobile Inspections
Spend more efficient time in the field

Asset Management Mobile Inspections allow field workers to reduce the time they spend at their headquarters. Having up to date information about Asset Condition equates to better planning and efficiency. Mobile inspectors can accurately record checkpoints, readings and observations directly into the TechnologyOne Asset Management system on the spot and in real time. For greater accuracy, photographs, videos and sound recordings can also be uploaded into Mobile Inspections quickly and easily. Additionally, each time the mobile device connects to the system, the officer's assigned inspections will be downloaded to the device, creating a seamless workflow process.

Property & Rating:

Fully integrated
The Property & Rating Mobile application is fully integrated with TechnologyOne Property & Rating.

Mobile Requests
Create and act upon requests in the field

Property & Rating Mobile Requests enables an organisation to improve the efficiency and effectiveness of administration for the processing of customer requests. Through the use of mobile devices, council officers are able to receive, display and complete existing requests on their mobile device without the need to return to the office or depot. Additionally, mobile workers are able to create requests whilst out in the field and sync new requests directly into the Property & Rating system.

Mobile Inspections
Make inspections faster and more accurate

Traditionally, inspectors record details manually using forms, and information is then re-entered at the office. This can be an onerous and time-consuming process, particularly when it involves attaching photos or recordings. It can also result in relevance and information security being compromised. In contrast, Mobile Inspections has results recorded electronically, in real time, where the inspection takes place. Mobile Inspections delivers a wide range of regulatory and application inspections including Health Inspections and Building Inspections. Set up is fast as these are configured using features like event checklists, application conditions and events workflow.

Empower mobile workforce

Record information once, accurately and easily
Work Orders, Inspections and Mobile Requests are designed simply and specifically for mobile workers. User experience is simple, intuitive and optimised for data capture. Photographs, sound recordings and video can be easily added providing greater accuracy.

Access to current information improves productivity
Mobile solutions offer an 'occasionally connected' model, where network outages will not prevent an inspection from being performed or a request form from being created or finalised. It is understood however, that mobile workers expect up-to-date information, so when in range of a 3G or WiFi network, information on the device is kept current.

Schedule and plan work in the field
A worklist provides a unified view of Inspections, Requests and Work Orders that have been assigned to the user. Work items can be viewed as a list or as a schedule view.

Save time, reduce travel and administration costs
Having the flexibility to start and end work in the field, rather than at a specific location such as a depot or office can result in ongoing savings. The delivery of work directly to the mobile worker and the ability to directly report request resolution can allow a mobile worker to spend more time resolving and creating requests, and less time spent travelling.

9.7. BlinkMobile

BlinkMobile provides a Mobile Enterprise Application Platform (MEAP) for mobile solutions development, independent of mobile platform. It allows data capture in the field, replacing written forms with more efficient device-based electronic forms that can be used off-line and then be updated to back-end systems when connected.

Blink has many Case Studies of solutions for Councils both in Australia and in New Zealand. They provided aspects of the Auckland Civil Defence app system for mobile devices.

See Auburn City Council Case Study in section 8: Auburn City Council - BlinkMobile Forms into Pathway

1 - WE START WITH THE NEEDS OF THE END USER, THEN WORK BACK

This simple difference makes all the difference. Particularly to user adoption and productivity.

Instead of trying to shoehorn an entire solution built for PCs into smaller mobile devices, we concentrate on the specific demands of the end user. When you build a BlinkMobile-based solution you model and manage the Interactions that your users need when they're out and about. These Interactions work with the back-end or cloud-based service or services that can satisfy the user need. By focussing on the user need and not the expectations of the underlying systems you ensure that the user experience is one of intuitive, straightforward interactions providing just the information they actually need, where and when they need it.

BlinkMobile's Interaction-oriented Architecture, which underpins the Blink Mobility Platform, overcomes the problems of system complexity and information overload so prevalent in the mobile world.

2 - WE EMBRACE EVERY TYPE OF MOBILE DEVICE AND BEYOND…

The BlinkMobile MEAP accommodates every device (not just smartphones) from a single development effort. All managed content is accessible across every type of smart device including internet TVs, kiosks and smart appliances as well as SMS-only phones. And we're fully prepared for devices that haven't even left the drawing board yet.

Together, these features allow us to deliver mobile services built for optimum usability with the intelligence and context to fully leverage the investment already made in back-end systems. This is the only strategic path worth considering.

Post-PC device delivery needs to look beyond older "virtual desktop" and mobile application models to achieve its potential. Those enterprises that can increase productivity and deliver new business value by harnessing the current and future onslaught of delivery technologies will gain a significant business advantage.

The trouble is, whilst the hardware technology is changing fast, the software vision hasn't kept up. The industry is talking about the "Internet of Things" but the architectural vision isn't anywhere near it. Instead we're still considering "Virtual Desktops" and Applications. Surely these are concepts of the PC era? They're systems-oriented concepts rather than user-oriented and BlinkMobile believes this is a problem.

The opportunity is in the fact that the Internet gives us a way of viewing everything as a callable service that can either provide the information we're after or process what we have to offer. The information architectures that make this possible (Service-oriented Architectures) are well established and even where they are not, you can view almost any Internet-enabled application as a service.

This vision of the Internet as a cloud of services to be harnessed as needed is extremely exciting. However there's an architectural hurdle to be jumped before exploiting it properly in the world of ever-changing delivery technologies becomes a reality, and that's a move from "systems" thinking to "user" thinking. Put another way, it involves changing the focus of the software architectures we use to service our users from "information" or "system" focused to "user interaction" focused.

This thinking is at the core of BlinkMobile's Interaction-oriented Architecture.

I asked BlinkMobile some questions to help clarify its solutions and approach. Here are the questions and answers provided:

If a custom iOS, Android or HTML5 app is requested, who does the front end development?

> *The Blink Mobility Platform is a development and deployment environment that can deliver either hybrid apps (HTML5 with an OS specific app shell), HTML5 web apps or even "basic mode" HTML delivery from a single configuration exercise. You don't need high level development skills and either our customers or our partners can deliver the apps. The front end development is actually driven by design/layout configuration capabilities within the Platform.*

Does existing customer data sometimes need to be set up with API's or as a Web Service if the database or back-end app vendor does not have an appropriate option?

> *The ideal way for "Interactions" defined in the Blink Mobiliy Platform to access customer data is through a Web API/Web Service. However in a world where not everything has a web service there are other ways to access back end systems. The most common other methods are to "proxy" the existing web interface if there is one, or to use direct database access (although we'd generally advise against this for any complex system). If there is no other option then an "adapter" is typically written by the customer or partner that exposes a simple REST webservice on one side and talks to the application using whatever method is most appropriate on the other.*

Who does that development?

> *The customer or a partner is generally responsible for that development. In some instances (such as Sharepoint lists and SQL server backends) we have developed these ourselves, but we're finding there are a growing number of adapters available now for common back-end systems.*

Does the BlinkMobile Platform take data from customer servers on demand or have other data transfer arrangements to be made?

The data architecture is flexible and many scenarios can be delivered. Certainly interactive access 'on demand' is common and we can do this, but you can also batch up data into 'data suitcases' that can be delivered to the devices. These 'data suitcases' can be updated by different events at the discretion of the developer. The data suitcases are the best means to allow for offline operation.

Is the BlinkMobile platform data stored at BlinkMobile sites before downloading to devices for off-network use?

Not normally. Data suitcases are usually assembled in real time and shipped down to the requesting device without storage in the Blink Mobility Platform. However, one may configure two other storage options - one is to use the Content Distribution Network of the Blink Mobility Platform which is provided through AWS CloudFront to cache largely static data. The other is to assemble 'Systems or Shared Data Suitcases' which are effectively caches of data that can be downloaded onto devices but are regularly assembled on the platform. This approach can make performance markedly better but introduces the potentially greater security concern of data at rest within the Platform. As described above, offline operation can be enabled through 'Personal Data Suitcases' which are assembled and sent down to the device without being stored on the platform.

9.8. NCS

Mobility across the system

This update was provided by Greg Lee from NCS:

Introduction

NCS have adopted an HTML 5 compliant strategy across our application to deliver out-of-the-box anywhere, anytime, any device availability. We are delivering this through a presentation layer built in the Sencha Complete application environment. (www.sencha.com). I have sketched together these notes to assist with understanding where we are going.

Historically

Our original mobile strategy was to write specific mobile applications for the Windows Mobile platform. Over the years we have developed applications for Inspections, Parking, Dogs Management, Meter Reading amongst others. These all have the capability of working in a disconnected mode and go through a synchronisation process in a return to base scenario. Where applicable, they also go through an upload relevant data process before work begins. The fairly traditional way to construct and mobile app and have it work with an Enterprise system.

MagiQ

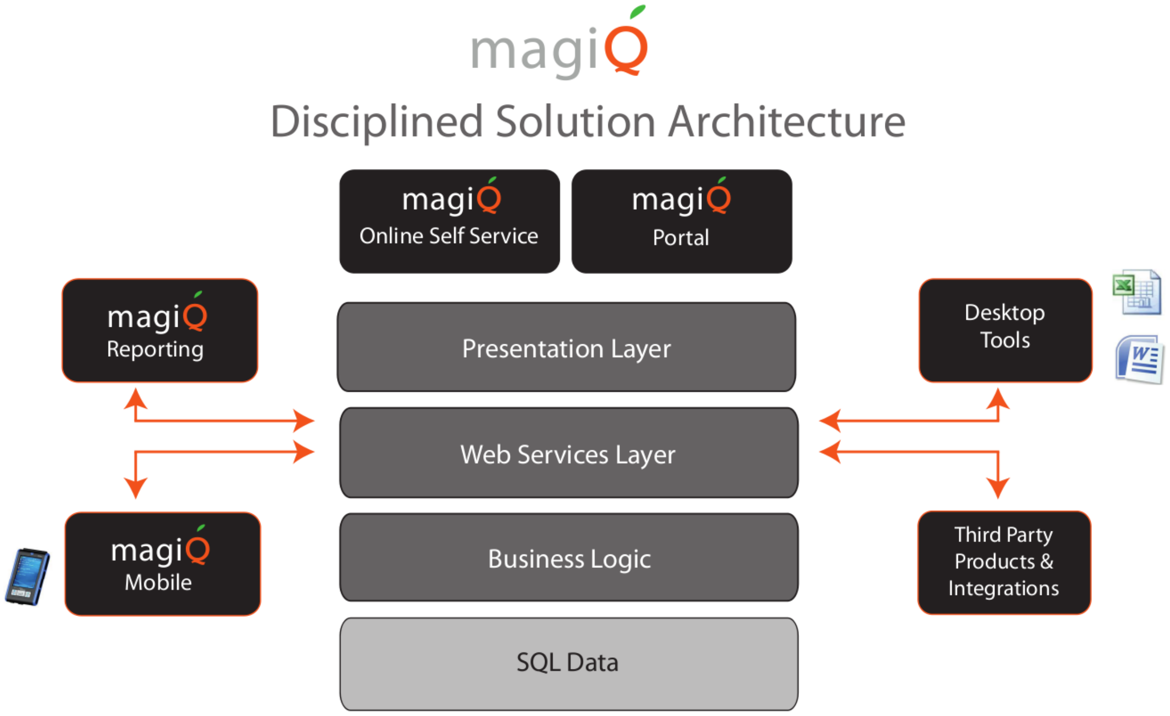
As our enterprise system, known as MagiQ , is already developed as a web application with good architecture (broadly an MVC approach) we are working through a project of replacing the Java, Ruby and Embedded HTML presentation layer screens with an entirely new layer constructed in the Sencha environment.

Sitting underneath this layer is a full web service layer connecting our traditional business logic layer with the presentation layer. This means that the rich application capability in our financial, transactional, and Council line of business applications can be delivered through to the presentation layer without having to move through the time consuming and difficult process of redevelopment.

To my knowledge we are the only enterprise local government line of business application currently available in the market in NZ (and Australia) that is a fully server side web delivered application. This significantly enhances our ability to move from Web 1 delivery to a full HTML 5 web/mobile delivery reasonably seamlessly.

The capability and portability of this architecture makes it significantly more appealing for a user base that increasingly wants to interface with an application from wherever they are and from whatever device they have.

NCS Architecture



Online or Offline

The significant issue with delivery of cross device applications is doing so in environments where internet, either via WiFi or 3G, may not always be available.

Mobile Delivery Options

If a user has internet available our entire application is currently available delivered through a browser. However many screens have not been designed specifically for the style of device the user might be using.

Sencha Browser

Via our Sencha presentation layer project we are using the tools to ensure the system auto-detects the device and delivers the appropriate layout as designed for the particular screen.

Of course this is still delivering the app via the browser on the device and requires an internet connection. The auto-detect function is a native feature of SenchaTouch 2.

Sencha Mobile Packaging

Using the tool we will also be packaging our apps as hybrid iOS, Android, or Windows 8 apps. This will provide full support for offline storage for each app.

Device API accessibility and native wrapping capability

“Web applications work everywhere. But there are still a few features uniquely available to native apps — like camera access and app store distribution — that are essential to app developers. Sencha SDK Tools give you the best of both worlds, providing a way to seamlessly “package” your web app in a native shell and instantly making it app-store-ready. With Sencha Touch SDK Tools, getting ready to submit to the Apple App Store or Android Market is just one command away.”

Offline support

HTML 5 specifies an API and process for managing Offline storage. The Sencha environment supports this capability. Technically the AppCache and database make it possible for mobile developers to store things locally on the device and interruptions in connectivity will not affect the ability for someone to get their work done.

Each application developed in the Sencha presentation layer will be given a full Offline support mobile treatment. We are currently working on our first application.

We will need to work with practical cases to ensure we are keeping and managing the data storage requirements appropriately. This is to ensure users have a full functioning app as required in the field with only “necessary” data stored locally.

So we see the future of mobile as heavily linked with delivering a seamless user experience between the desktop, office, tablet and smartphone. Our strategy is to aggressively adopt the HTML 5 standard and we are very well placed to deliver in this space.

We anticipate having our entire system through the revitalization and transformation into the new presentation layer over the next 18 months. At the moment we are slightly ahead of schedule.

Greg Lee.

9.9. Infor

The Infor Public Sector Suite for local government incorporates two core line of business systems of which are used by around half of the Councils in NZ.

- Infor Pathway People, Property, Revenue and Regulatory System
- Infor Hansen Asset and Work Management System

Infor has a mobile technology called Infor Motion which is incorporated in our Infor ION technology stack that all our enterprise applications (Pathway and Hansen included) are plumbed to use.

For asset related mobility, Infor has partnered with KernMobile because of their extensive experience in delivering mobile solutions for utilities and Councils.

Waitaki District Council provides a good NZ case study of how a Council has benefited from implementing Infor Hansen and KernMobile:

> *"Through Infor Mobile Solution (Kern), provided on-site engineers and contractors with the ability to better access information, perform tasks, and update back-office systems, minimizing trips to local offices for paperwork and maximizing on field planning and decision making." Infor Case Study.*

INFOR PATHWAY MOBILE

Infor announced the availability of Infor Pathway Mobile in March 2012.

Mobile Applications Available

- Inspections i.e. Building, environmental health
- Animal Enquiry
- Customer Service for Council Staff i.e. graffiti, pot holes

Key Features

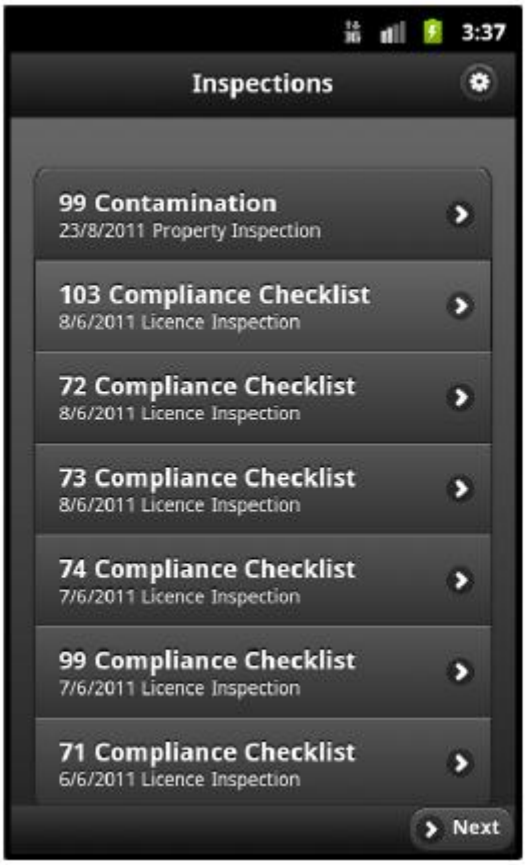
- Supports the following devices: iPhone, Blackberry, Android, Windows, iPads.
- Configurable Web Services to allow mobile applications to communicate directly to Pathway.
- Ability to provide information to your community on Council initiatives, events and breaking news.
- Facilitates secure transactions between your device and Infor Pathway.

- Transfers information from the mobile device automatically into Infor Pathway Customer Request with associated workflow.

Infor Pathway Mobile Computing Applications are compatible with the following devices: iPhone, Blackberry, Android, Windows, iPad.

Infor is also providing outward facing web services and a choice of communication methods via Infor’s ION platform. This will enable you to develop your own mobile applications and yet still take advantage of Infor’s communication layer to implement an in-house or third party mobility suite fully integrated with Infor Pathway. This approach can also be used to allow Councils to select other 3rd Party mobile applications in addition to Pathway Mobile and communicate directly to Infor Pathway

The Infor Pathway mobile applications will also include powerful, secure transaction entry and editing facilities. Further flexibility is achieved through strong integration with Infor Pathway allowing pre-population of fields on mobile devices as well as taking advantage of location data in the mobile devices.



99 Contamination
23/8/2011 Property Inspection

103 Compliance Checklist
8/6/2011 Licence Inspection

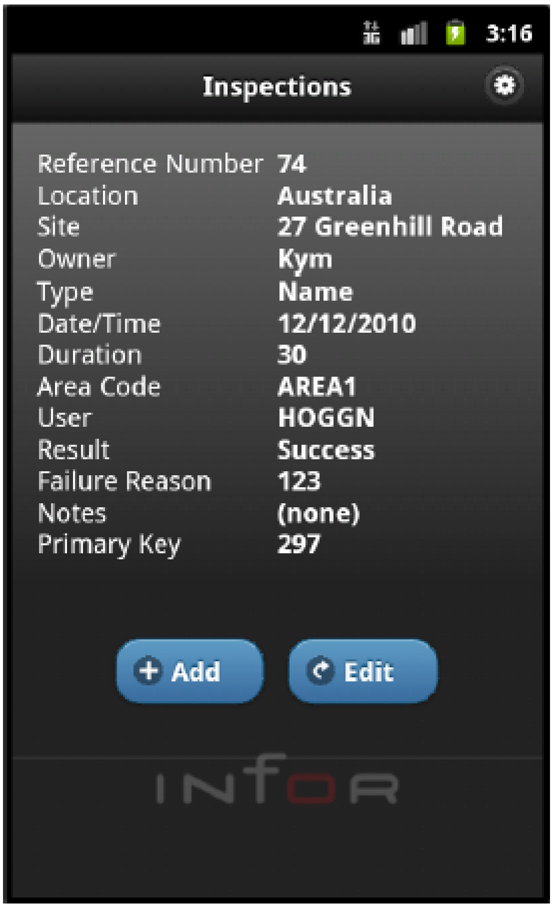
72 Compliance Checklist
8/6/2011 Licence Inspection

73 Compliance Checklist
8/6/2011 Licence Inspection

74 Compliance Checklist
7/6/2011 Licence Inspection

99 Compliance Checklist
7/6/2011 Licence Inspection

71 Compliance Checklist
6/6/2011 Licence Inspection



Reference Number	74
Location	Australia
Site	27 Greenhill Road
Owner	Kym
Type	Name
Date/Time	12/12/2010
Duration	30
Area Code	AREA1
User	HOGGN
Result	Success
Failure Reason	123
Notes	(none)
Primary Key	297

9.10. Civica Authority

Civica provides specialist systems and business process services for local government.

Authority Mobile is designed to help Council meet mobility challenges, delivering increased productivity and improved customer service as field workers are empowered to capture and act on information at the source and synchronise directly back to Council.

Operating in the Authority Enterprise Wide Solution environment, Authority Mobile shares information as appropriate with all of Council's corporate systems. This effectively eliminates paper forms and manual re-entry, ensuring both the field workers and Council's office staff have accurate, up-to-date information allowing them to provide more responsive and efficient service to customers. With full GIS integration Council staff can quickly locate assets or work order task sites and also have the capability to record GIS information for future reference.

Designed specifically for local government, Authority Mobile is highly flexible and highly scaleable, delivering a complete range of mobile applications across all of Council's business operations, with the convenience and simplicity of a single platform and a single database.

Council can also utilise its existing asset attributes, register details and workflow processes for building mobile data entry forms, eliminating any duplication of effort and ensuring consistency and ease of use.

The Authority Mobile platform does not require data connectivity to operate in the field, ensuring that workers are always productive regardless of whether network coverage is available. Where workers have access to an internet connection in the field they are able to interact with Authority via our Java based functions. This environment provides all of Council's workers with real time access to view, enter and update data.

Key Benefits

- Designed to synchronise directly with Council's Authority corporate applications to ensure data accuracy and consistency
- Empowers Council's field workforce to capture and act upon information at the source providing more responsive customer service and improving productivity
- Full GIS integration for efficient location of assets and workflow sites including ability to record GIS data in the field for future reference
- Highly flexible and scalable solution delivering mobile applications across Council's entire business on a single platform
- Transforms Council's existing data definitions and workflow processes to mobile applications eliminating duplication of effort and delivering ease of use for field workers

Easy to Set-up

- Unlimited user-definable items, checklists, attributes

- Easily configurable to your specific needs
- User defined industry terminology
- Full imaging support

Mobile Deployment

- Full integration with portable devices providing inspections, tasks, routing, multiple result capture and a very intuitive interface for use in the field
- Most portable devices supported including ruggedised laptops, PDA's and tablet PC's
- Full barcode functionality

Full reporting Capability

- Full report building capabilities
- No extra software required
- Output to screen, printer, fax, email or document register

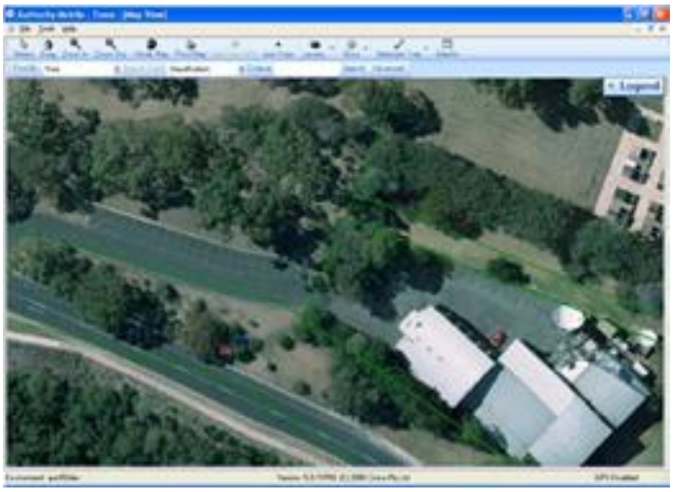
Geographical Information System

- Support for all major mapping systems
- GPS Location plotting
- Thematic Mapping
- Support for compressed aerial photography

Scalable Architecture

- 3-Tier product architecture
- Highly scalable covering single-user right through to full enterprise level deployment via LAN/WAN or the Internet
- Multi-level user security
- Multiple application support using Authority Mobile Solution Definition Builder

Authority supports aerial photography to clearly identify assets such as this highlighted tree



Authority Mobile: Meter Read

The easy and efficient way for Council's field workers to read, capture and manage meter data.

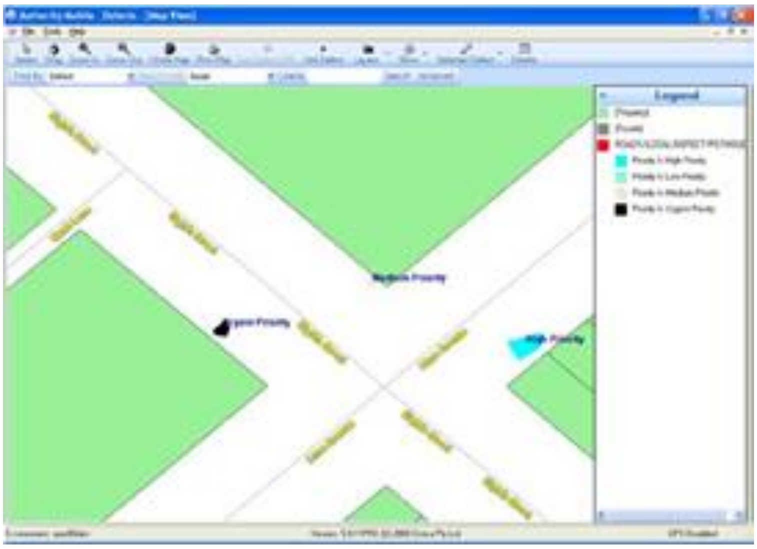
Easy Meter Read & Capture

- Complete access to property information in the field with the ability to view and edit location details
- Provides ability to capture notes and images in the field for instant action on damaged meters
- Ability to provide warning notices for unusually high or low readings to ensure read accuracy

Efficient Data and Route Management

- Easy integration to the Authority Meter Read interface ensures efficient data transfer with instant updating of relevant Council data
- Allows multiple routes to be managed simultaneously for improved productivity
- Easy view summary provides workers with instant access to workload and status
- Access to comprehensive reporting information

With full GIS integration, Authority allows Council staff to quickly identify defects, assets or work order task sites and their associated priority level



Authority Mobile: Infringements

The Authority Mobile Infringements application allows Council's officers to record and print infringements notices in the field and provides the ability to capture images, voice recordings and other evidence of the infringement and record officer notations.

The application features user-definable templates allowing Council the ability to easily transform their data to the mobile application for a range of infringements including parking, traffic, DFNAA (Animals), littering and local law. Definable templates also provide Council with flexibility in the design of printed notices.

Authority Mobile: Animal Catalogue

The Authority Mobile Application provides the ability for field workers to search for and identify animals out in the field. The field officer has the ability to customise the search using any combination of fields such as tag no, breed, colour and also microchip. The field officer can also use GPS to locate animals that are registered within a certain radius, using the animals kept at address. The details of the animals displayed back to the field officer can be customised by an administrator and include details such animal number, tag, breed, colour, gender, neutered indicator, dangerous animal flags, owner details, contact details, warning memos, photos of the animal, and kept at address details.

The animal catalogue can also be linked to the Authority Mobile Infringement application for the purposes of issuing of infringements.

Authority Mobile: Asset Management

Asset Data Collection

The Authority Mobile Asset Data Collection application allows Council's field workers to capture information at the source for any asset defined by Council, for example footpaths, bridges, signs, bus shelters, playground equipment or significant trees. Field workers may be capturing initial details regarding the asset, for example the asset attributes, or they may be completing a remote maintenance report. Using Authority Mobile and mobile devices such as PDA's or Tablet PC's, asset information is quickly and easily captured. Individual data entry forms can be designed for each asset type and are based on Council's existing Authority Asset & Infrastructure asset attribute definitions.

Inspections and Defects

The Authority Mobile application allows field officers the ability to complete inspections whilst actually doing the inspections. Inspections checklists can be completed and the type of information recorded is based on the type of inspection. Scoring and comments may also be captured together with additional notes and photos. Whilst in the field, Council officers may identify defects which can also be recorded and are automatically associated with the inspection, for example defects such as pot holes, cracked footpaths, vandalised assets or over-grown weeds. Individual data entry forms can be designed for each inspection and defect type and are based on Council's existing Authority Work Order Classifications and checklist definitions.

Authority Mobile: Registers

The Authority Mobile Registers application allows Council's field workers to capture a range of information pertaining to Council's specific register types. For example Council may be using Authority Registers to store details of Weeds, Food Premises, Swimming Pools or Cemeteries. The register definitions, checklists and workflows that Council has already specified within their Authority Register can be easily transformed to a mobile application, eliminating duplication of effort and ensuring staff are familiar with the data entry requirements.

Authority Mobile: Noxious Weed Register

The easy and efficient way for Council to track, audit and manage noxious weed infestations.

Tracking

- Authority Mobile gives you complete property information in the field with the ability to issue inspection reports on the spot

- Authority Mobile allows you to use GPS receivers in the field and import maps from all popular mapping systems

- Authority Mobile provides access to notes, images and fact sheets of weeds in the field

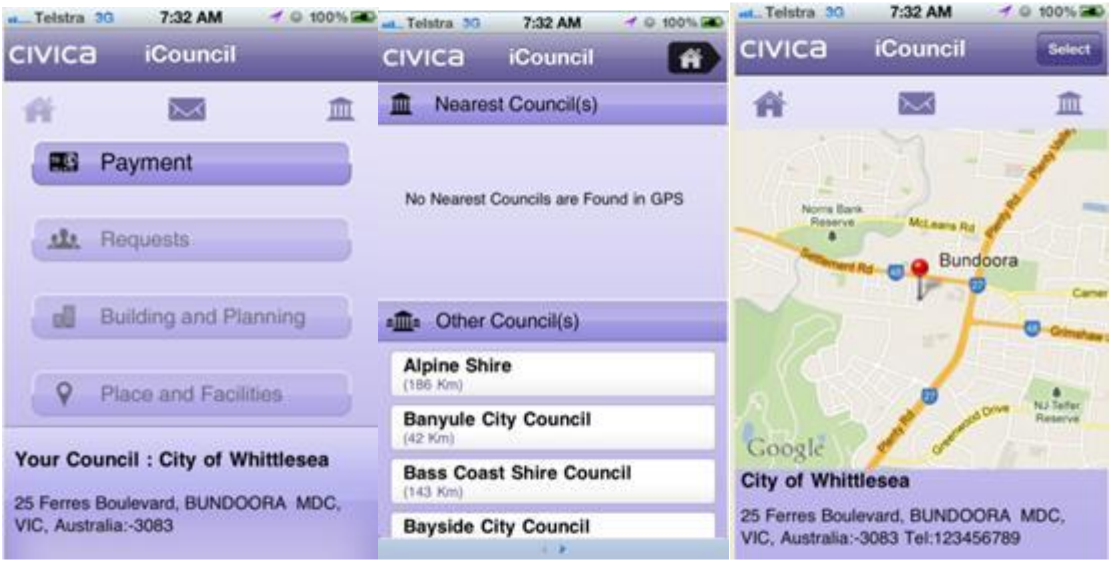
- Authority is a multi-user system and can be deployed across the web

Management

- Authority Mobile comes with complete reporting capabilities, no extra software is required
- Authority Mobile document register allows saving of all issued notices and reports
- Authority Mobile allows workers to schedule re-inspections and track activities in the field

Development

For many years mobile computing has been a key component of the Authority application and Civica is committed to its ongoing evolution. Significant new capabilities are planned in versions 6.7 (September 2012) and 6.8 (April 2013) of the platform.



Your Council : City of Whittlesea

25 Ferres Boulevard, BUNDOORA MDC, VIC, Australia:-3083

No Nearest Councils are Found in GPS

Alpine Shire (186 Km)

Banyule City Council (42 Km)

Bass Coast Shire Council (143 Km)

Bayside City Council

City of Whittlesea

25 Ferres Boulevard, BUNDOORA MDC, VIC, Australia:-3083 Tel:123456789

- Provide seamless synchronisation services delivering data to and from mobile devices when network connectivity is available.
- Provide web service interfaces to Authority integration services that manage both the delivery of data to devices and the updating of mobile transaction data to the corporate database.
- Re-architecting the mobile device software to enable its deployment on a broad range of mobile devices (e.g. IOS & Android devices).

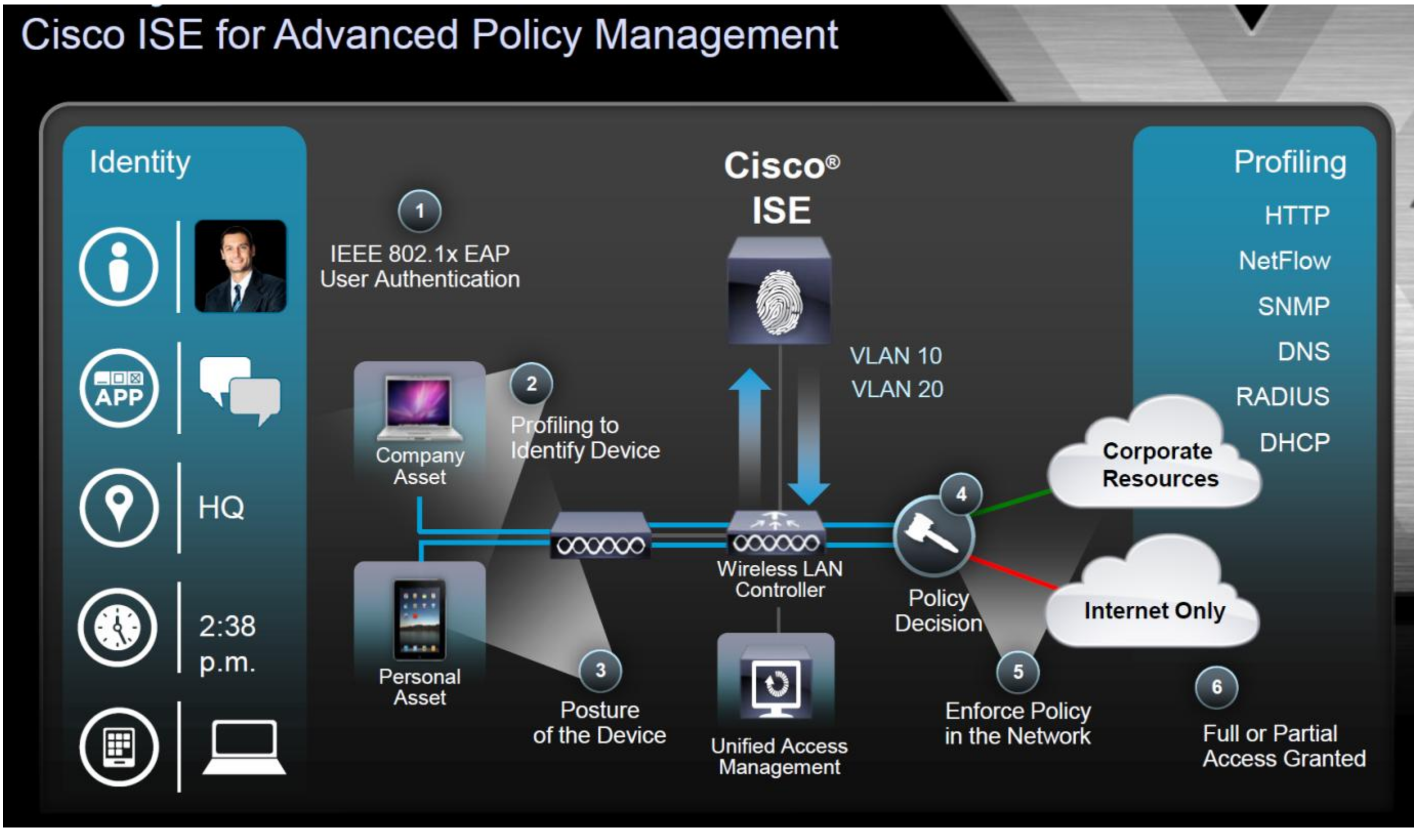
Enabling third party applications to interact with the Authority mobile platform web and integration services

9.11. Cisco

The Cisco approach allows devices to be self-enrolled the first time they connect to the network. Each device is fingerprinted so it can be identified upon returning to the network.

The Cisco Identity Services Engine (ISE) provides a centralized single source of policy across the organization that can be enforced across different wired and wireless network access types.

> *The Cisco BYOD solution provides a means to identify devices and users and provides differentiated services based on custom policy options. For example, employees using corporate-owned and managed devices can be treated differently than employees using their own unmanaged devices at work. Similarly, contract employees, partners, guests, customers, students, and other classifications that are important to the business or entity can be identified and treated according to the business policies, restricting access to only the set of services and access to which they are entitled.*
>
> *The Cisco BYOD solution strategy is to provide a common approach anywhere devices connect to the network, including wired, WiFi, public WiFi, and 3G/4G mobile and also regardless of whether the connectivity occurs in the main campus, branch office, home office, or mobile Teleworker location.*



The Cisco Identity Services Engine (ISE) is a core component of the Cisco BYOD solution architecture and provides a number of services including:

- Authentication

- Authorization
- Device profiling
- Certificate enrollment
- Posture assessment
- Policy definition and enforcement
- Interface to identity stores (e.g., Active Directory® [AD], RSA® SecurID®)

In addition to core functions such as authentication and authorization, Cisco ISE provides intelligence about devices connecting to the network through device profiling. Device profiling can be used for discovering, locating, and determining the type and capabilities of endpoints that attach to the network to deny or enforce specific authorization rules.

For example, the combination of device profiling, posture assessment, and policy enforcement can be used to enforce BYOD policies such as:

- Allow employee-owned iPads® access to the network, but only HTTP traffic
- Deny iPhones® access to the network if they have been jail broken
- If the Android device is corporate owned, grant full access

Cisco Identity Services Engine provides unified, policy-based, management. Talks to Active Directory, applies policies and role-based access control for secure, self-service BYOD.

Device Management

MDM Is a Key Element—But There Is More

MDM Partners

- ✓ Device inventory
- ✓ Device provisioning and deprovisioning
- ✓ Device data security
- ✓ Device application security
- ✓ Cost management
- ✓ Full or selective device remote wipe

Cisco

- ✓ User and device authentication
- ✓ Posture assessment
- ✓ Policy enforcement
- ✓ Context-aware access control

Cisco® ISE

- ✓ Threat defense
- ✓ Web use policy
- ✓ Web application DLP

Cisco ScanSafe

Cisco WSA

- ✓ Secure remote access

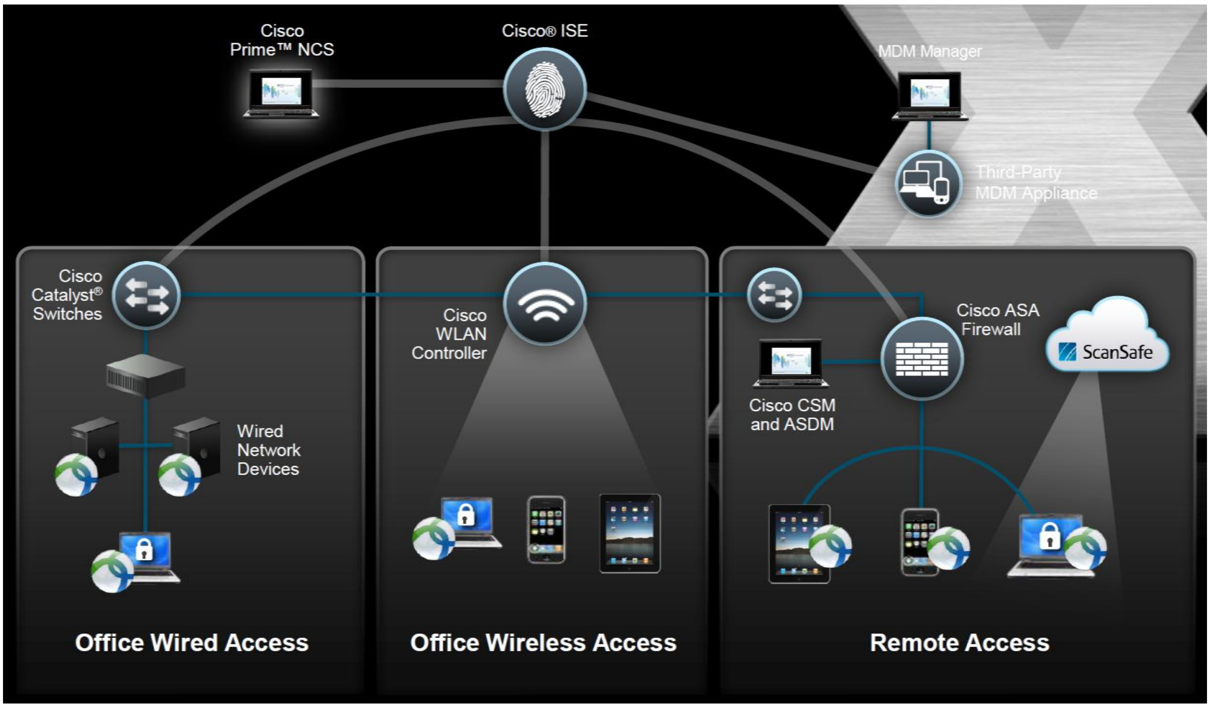
Cisco AnyConnect™

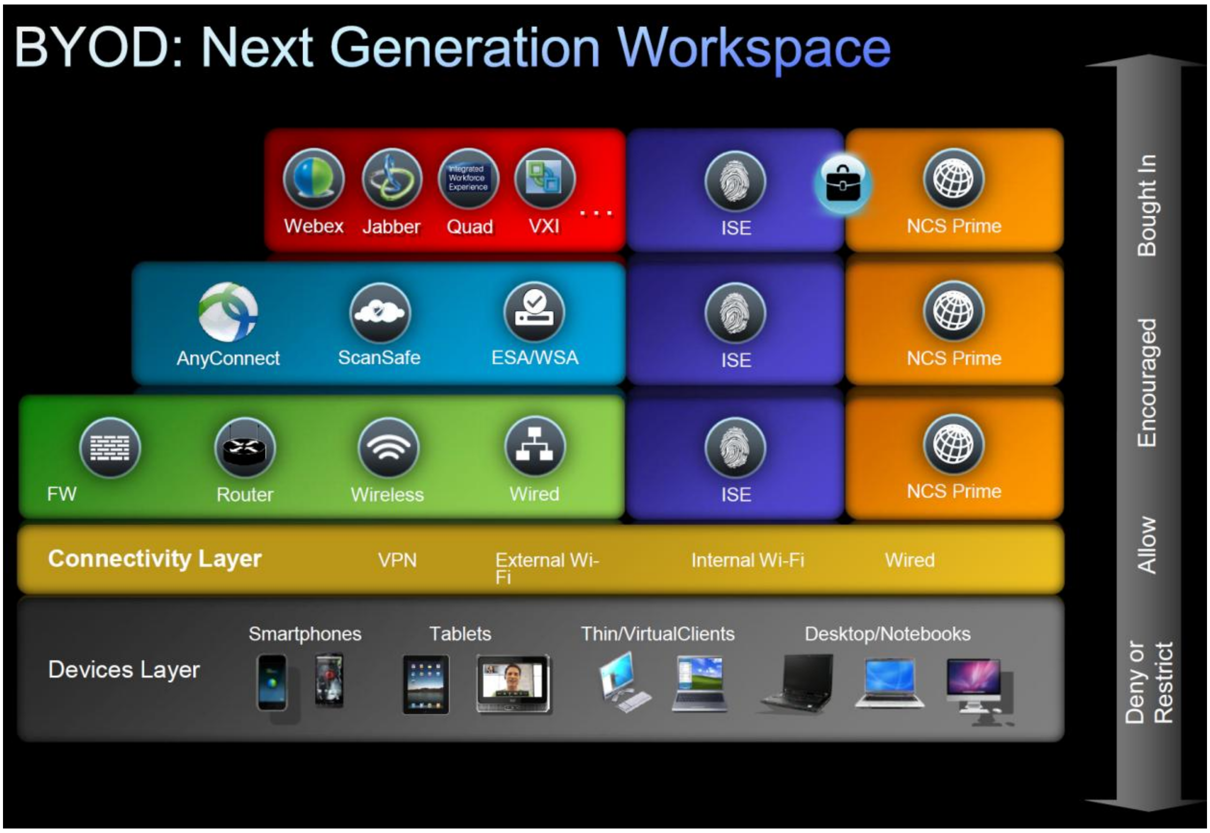
Cisco ASA

Cisco partners for MDM include AirWatch and Sophos. AirWatch agent sits on the mobile device.

The Cisco Adaptive Security Appliance (ASA) provides traditional edge security functions, including firewall and Intrusion Prevention System (IPS), as well as providing the critical secure VPN termination point for mobile devices connecting over the Internet from home offices, public WiFi hotspots, and 3G/4G mobile networks.

Cisco BYOD Solution:





BYOD: Next Generation Workspace

Webex Jabber Quad VXI . . .

ISE

NCS Prime

AnyConnect ScanSafe ESA/WSA

ISE

NCS Prime

FW Router Wireless Wired

ISE

NCS Prime

Connectivity Layer VPN External Wi-Fi Internal Wi-Fi Wired

Devices Layer Smartphones Tablets Thin/VirtualClients Desktop/Notebooks

Bought In

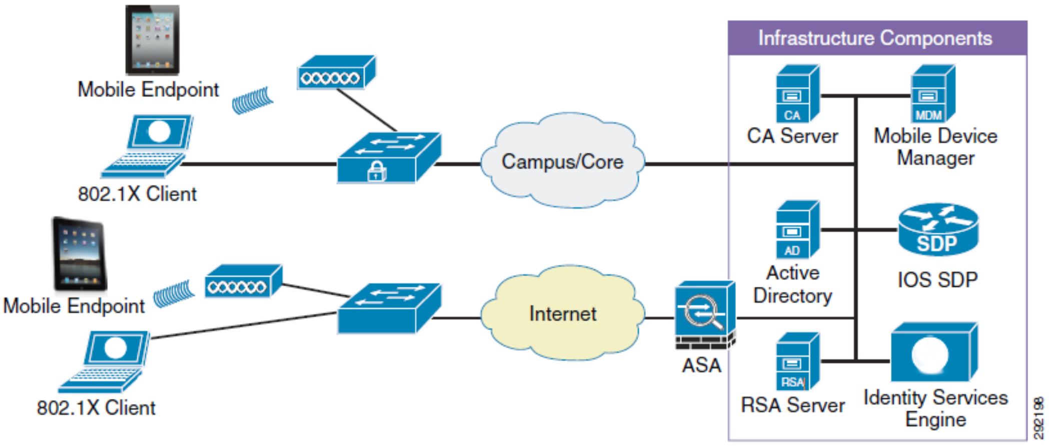
Encouraged

Allow

Deny or Restrict

Cisco BYOD Architecture

Figure 7 *HIgh-Level BYOD Solution Architecture*



9.12. Aerohive

Aerohive Networks are designed to reduce costs and complexity with a distributed Wi-Fi (Controller-less) Architecture. It is well suited to medium sized organisations, branch offices and teleworkers.

> *"Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing and VPN solutions eliminate costly controllers and single points of failure. This gives its customers mission critical reliability with granular security and policy enforcement and the ability to start small and expand without limitations."*

It provides a "self-healing mesh architecture" with distributed intelligence (FW, RADIUS, CWP, BYOD, Bonjour GW):

- QoS & Spectrum analysis included
- Stateful TCP/IP firewall
- Authentication support for common directory servers
- Eliminates standalone RADIUS server
- Cost effectiveness - ability to start small and grow
- RADIUS Server Built into HiveAPs

Councils using Aerohive:

- Regional Facilities Auckland – 90 + Aerohive Wi-Fi AP's installed in the Aotea Center, AKL Town Hall, Civic and Viaduct Events Center. Providing Public, Events and Back Office Wi-Fi Access.
- Porirua City Council - Recent
- Tasman District Council
- Tauranga District Council
- BOP District Council
- Greater Wellington Regional Council and Wellington City Council - Recent

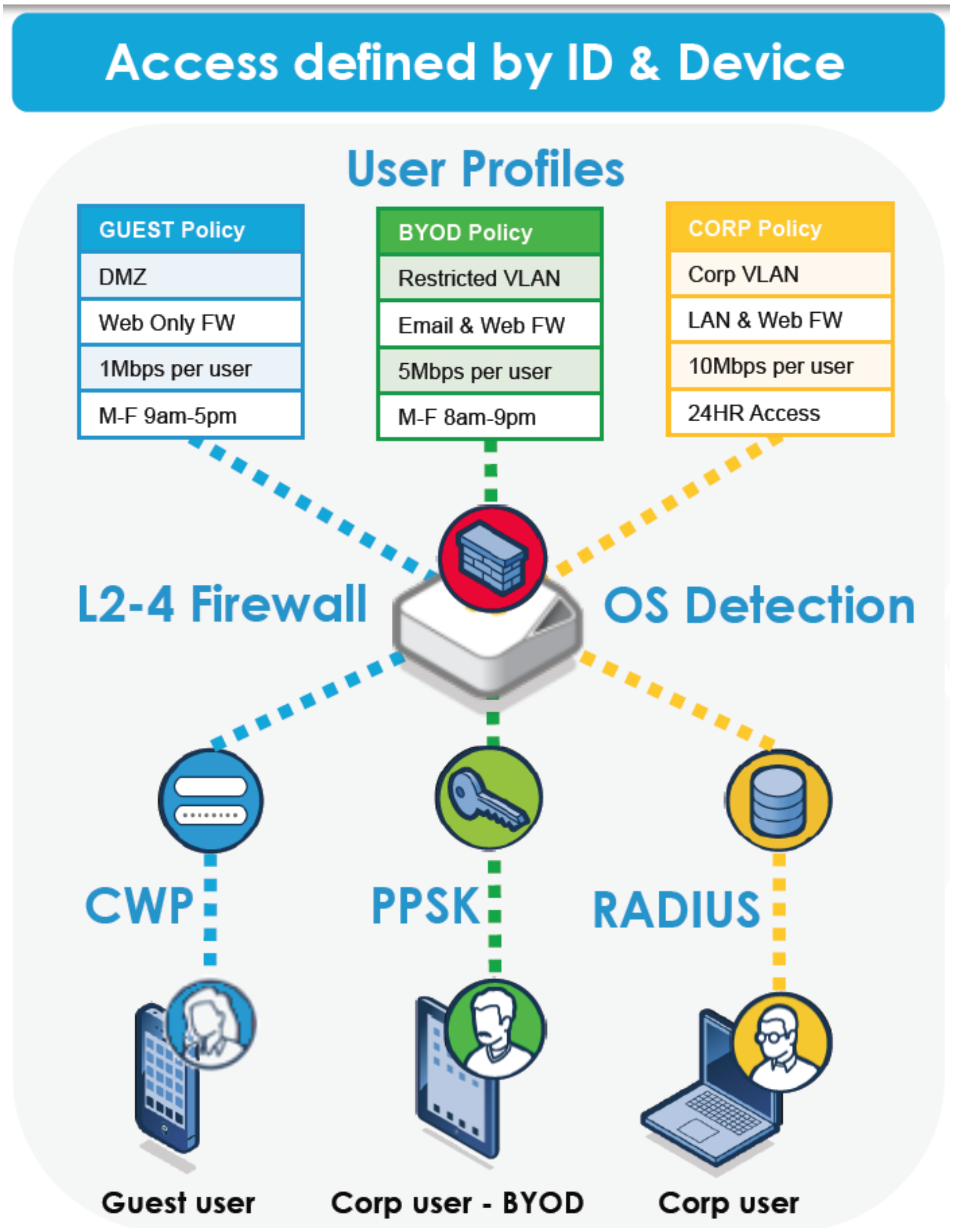
Other NZ Corporate Customers :

- Vector
- Toyota NZ
- Bayles
- The Radio Network

- AA
- Sime Darby

Many Education Customers in NZ:

- Manakau Institute of Technology (500 + APs)
- Otago Polytechnic
- Waimea Cluster
- Greater Christchurch School Network (Cluster) all 100 + AP's



Access defined by ID & Device

User Profiles

GUEST Policy	BYOD Policy	CORP Policy
DMZ	Restricted VLAN	Corp VLAN
Web Only FW	Email & Web FW	LAN & Web FW
1Mbps per user	5Mbps per user	10Mbps per user
M-F 9am-5pm	M-F 8am-9pm	24HR Access

L2-4 Firewall

OS Detection

CWP

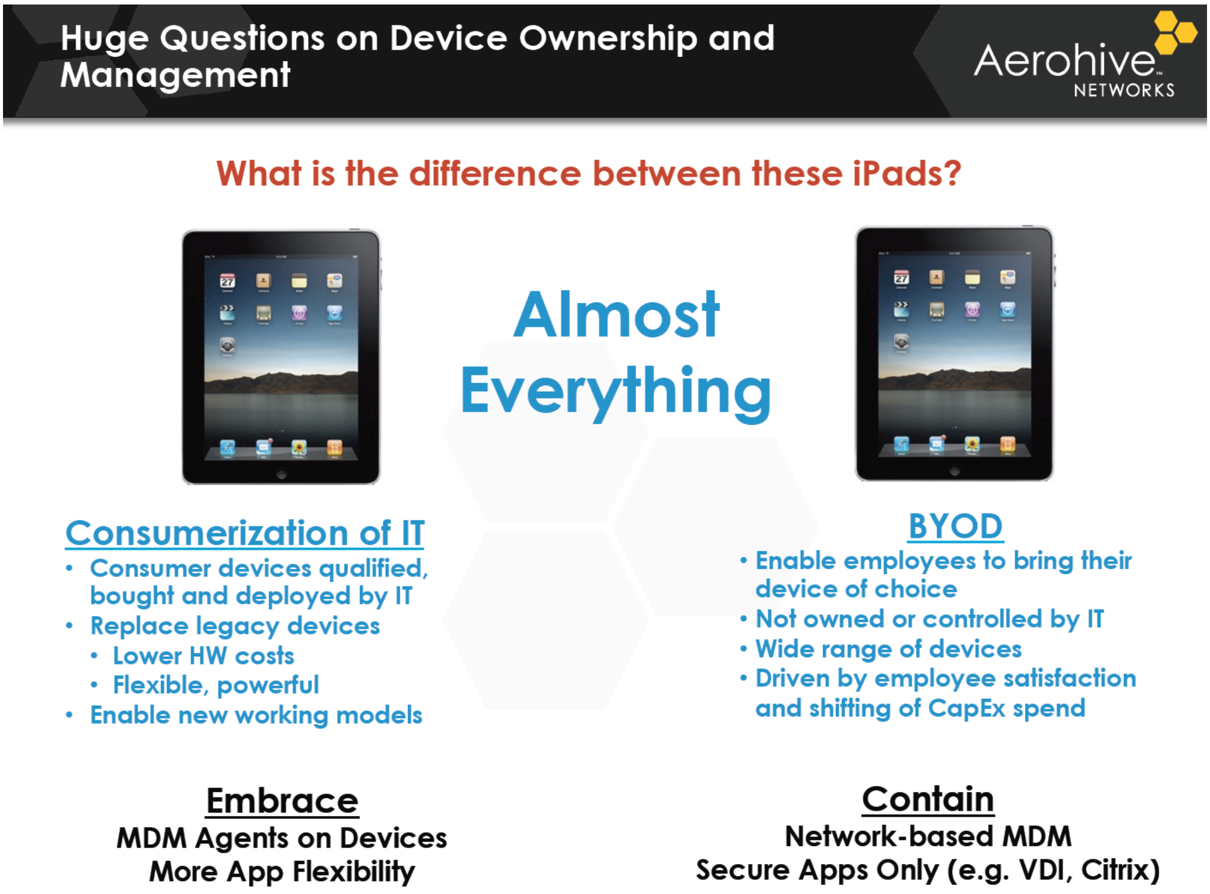
PPSK

RADIUS

Guest user

Corp user - BYOD

Corp user



Huge Questions on Device Ownership and Management

Aerohive NETWORKS

What is the difference between these iPads?

Almost Everything

Consumerization of IT

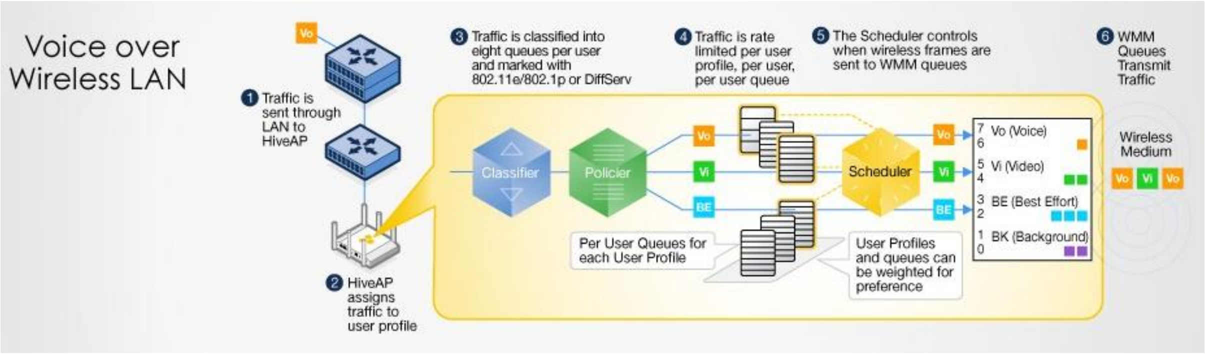
- Consumer devices qualified, bought and deployed by IT
- Replace legacy devices
  - Lower HW costs
  - Flexible, powerful
- Enable new working models

BYOD

- Enable employees to bring their device of choice
- Not owned or controlled by IT
- Wide range of devices
- Driven by employee satisfaction and shifting of CapEx spend

Embrace
MDM Agents on Devices
More App Flexibility

Contain
Network-based MDM
Secure Apps Only (e.g. VDI, Citrix)


Voice over Wireless LAN
Vo
1 Traffic is sent through LAN to HiveAP
2 HiveAP assigns traffic to user profile
3 Traffic is classified into eight queues per user and marked with 802.11e/802.1p or DiffServ
4 Traffic is rate limited per user profile, per user, per user queue
5 The Scheduler controls when wireless frames are sent to WMM queues
6 WMM Queues Transmit Traffic
Classifier
Policier
Vo
Vi
BE
Per User Queues for each User Profile
Scheduler
User Profiles and queues can be weighted for preference
7 Vo (Voice) 6
5 Vi (Video) 4
3 BE (Best Effort) 2
1 BK (Background) 0
Wireless Medium
Vo Vi Vo

Voice over Wi-Fi enterprise deployments

Successfully deploying an application like voice over wireless LAN requires the underlying infrastructure to be highly available, and have low latency and sophisticated quality-of-service (QoS) capabilities. Aerohive's unique stateful high availability, mesh redundancy, and stateful failover ensure that the network is always up. The best path forwarding ensures the data path is continuously optimized to provide the lowest latency, and the lack of a controller means there is no added latency or jitter due to backhauling the wireless traffic.

While standards-based IEEE 802.11e/ WMM (Wireless Multi-Media) extensions are also implemented – WMM alone isn't enough. To manage the flow of traffic into the WMM *queues, Aerohive implements QoS, with eight queues per client station right at the network edge where they can immediately respond to the dynamically changing RF link, rather than at a centralized controller multiple hops away from the radio.*

Aerohive dubbed "Visionary" in first combined wired and WLAN Access Infrastructure Magic Quadrant

Tuesday, June 19, 2012 Posted by *Queen Bee*

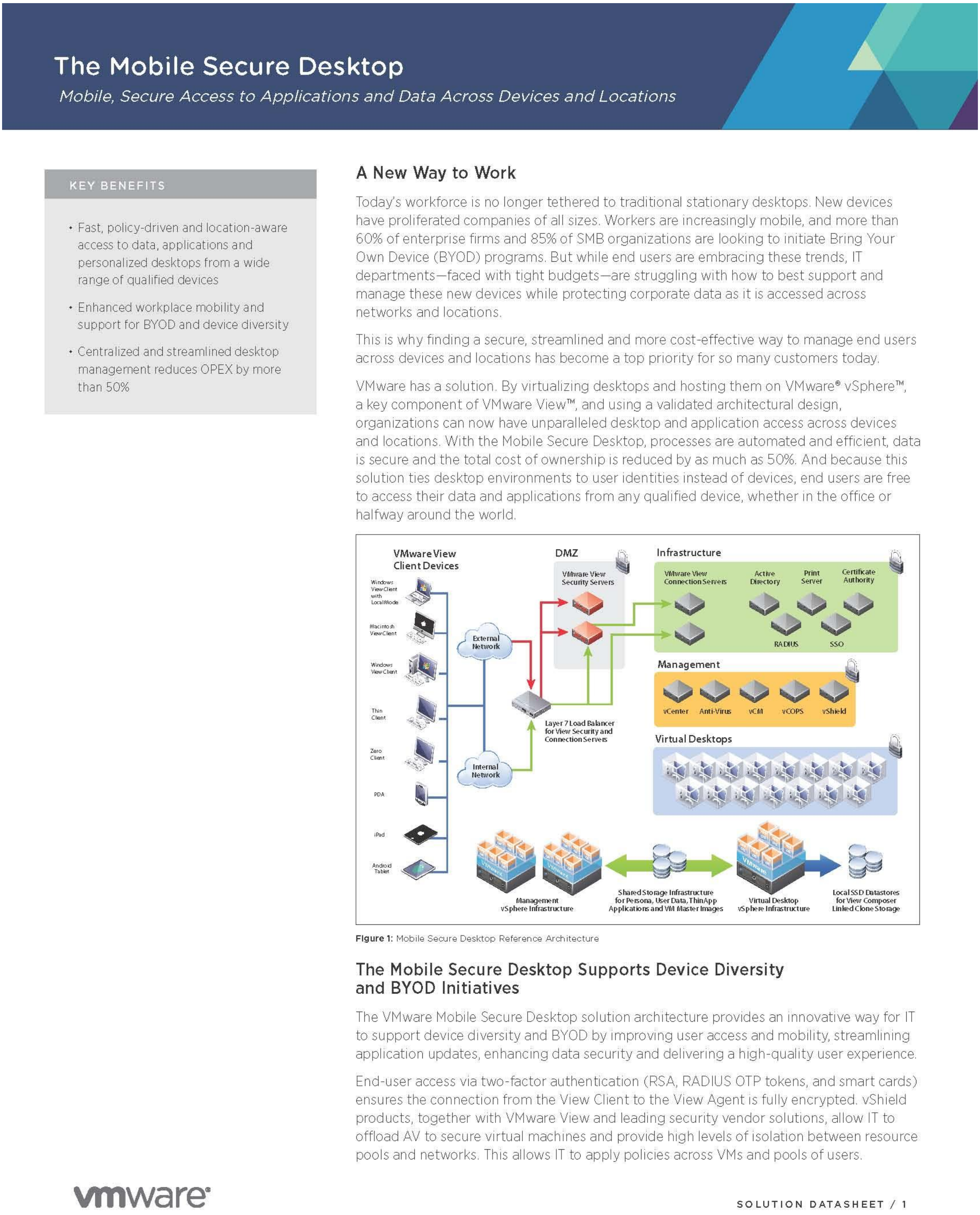
Firsts are always fun, right? Here's a good one that I'm pleased to be writing about today - for the first time, Gartner has combined wired and wireless LAN access infrastructure into a single Magic Quadrant. And Aerohive has been positioned as a "Visionary" in that MQ, called the 2012 Magic Quadrant for Wired and Wireless LAN Access Infrastructure.

"Aerohive continues to be strongly positioned for growth at the edge of the network, due to the innovation provided by the Bonjour Gateway and its breadth of internally developed network service applications for security, network management, policy enforcement, client remediation and the stateful firewall," according to the Gartner report. "Aerohive offers clients options as to where the network-based services will reside — either within the AP on-premises or in the cloud. This gives Aerohive customers a wide range of choices for deploying wired or wireless architectures."

Gartner also recommends that Aerohive should be considered for any overlay WLAN enterprise opportunities in North America, Western Europe or Australia/New Zealand, especially in the education, healthcare and retail markets. According to Gartner's report.

Of Aerohive, Gartner said, "Its controller-less, mesh-based architecture provides an easy-to-use and robust solution with lower operational costs, which makes it a standard bearer for market pricing of equivalent functionality. Aerohive's innovation and market messaging are driving annual growth of ~130% higher than the 30% compound annual growth rate (CAGR) the WLAN part of the access layer market is currently experiencing. Network service applications for security, guest access, network management and policy enforcement can be defined on an appliance or in the cloud before being deployed to the edge of the enterprise network."

9.13. VMware Mobile Secure Desktops and Mobility



The Mobile Secure Desktop

Mobile, Secure Access to Applications and Data Across Devices and Locations

KEY BENEFITS

- Fast, policy-driven and location-aware access to data, applications and personalized desktops from a wide range of qualified devices
- Enhanced workplace mobility and support for BYOD and device diversity
- Centralized and streamlined desktop management reduces OPEX by more than 50%

A New Way to Work

Today's workforce is no longer tethered to traditional stationary desktops. New devices have proliferated companies of all sizes. Workers are increasingly mobile, and more than 60% of enterprise firms and 85% of SMB organizations are looking to initiate Bring Your Own Device (BYOD) programs. But while end users are embracing these trends, IT departments—faced with tight budgets—are struggling with how to best support and manage these new devices while protecting corporate data as it is accessed across networks and locations.

This is why finding a secure, streamlined and more cost-effective way to manage end users across devices and locations has become a top priority for so many customers today.

VMware has a solution. By virtualizing desktops and hosting them on VMware® vSphere™, a key component of VMware View™, and using a validated architectural design, organizations can now have unparalleled desktop and application access across devices and locations. With the Mobile Secure Desktop, processes are automated and efficient, data is secure and the total cost of ownership is reduced by as much as 50%. And because this solution ties desktop environments to user identities instead of devices, end users are free to access their data and applications from any qualified device, whether in the office or halfway around the world.

VMware View Client Devices
Windows View Client with Local Mode
Macintosh View Client
Windows View Client
Thin Client
Zero Client
PDA
iPad
Android Tablet
External Network
Internal Network
DMZ
VMware View Security Servers
Layer 7 Load Balancer for View Security and Connection Servers
Infrastructure
VMware View Connection Servers
Active Directory
Print Server
Certificate Authority
RADIUS
SSO
Management
vCenter
Anti-Virus
vCM
vCOPS
vShield
Virtual Desktops
Management vSphere Infrastructure
Shared Storage Infrastructure for Persona, User Data, ThinApp Applications and VM Master Images
Virtual Desktop vSphere Infrastructure
Local SSD Datastores for View Composer Linked Clone Storage

Figure 1: Mobile Secure Desktop Reference Architecture

The Mobile Secure Desktop Supports Device Diversity and BYOD Initiatives

The VMware Mobile Secure Desktop solution architecture provides an innovative way for IT to support device diversity and BYOD by improving user access and mobility, streamlining application updates, enhancing data security and delivering a high-quality user experience.

End-user access via two-factor authentication (RSA, RADIUS OTP tokens, and smart cards) ensures the connection from the View Client to the View Agent is fully encrypted. vShield products, together with VMware View and leading security vendor solutions, allow IT to offload AV to secure virtual machines and provide high levels of isolation between resource pools and networks. This allows IT to apply policies across VMs and pools of users.

vmware®

SOLUTION DATASHEET / 1

> *"If you think about mobility today, it's really changed from just a few years ago. Wherever we are now is ubiquitous computing in a post-PC era. The PC and the Laptop used to be King of the Mountain and it really isn't anymore with the consumerization of IT and BYOD."*
>
> – Doug Cadell
> CIO, Foley and Lardner

vCOPs for View provides analytic dashboards and end-to-end monitoring of desktops, users and network to help IT troubleshoot, trend and proactively address potential issues across the end-user environment in order to maximize uptime and compliance.

The VMware View Mobile Secure Desktop with PCoIP™ additionally delivers end users a seamless experience across devices, networks and locations—and supports end users who may need applications, printing, unified communications and 3D graphics as part of their daily workspace.

And by leveraging desktops with persona management, the Mobile Secure Desktop ensures end users can carry their persona with them across sessions and devices for a more personalized desktop experience.

Solution Elements

The Mobile Secure Desktop is a validated solution architecture offered by VMware and VMware Ready Partners. It is specifically built to meet the needs of organizations looking to securely support end users across devices and locations. It combines VMware and ecosystem products and services to meet the necessary requirements for supporting security, rapid and automated provisioning and mobile access across devices. Key solution elements include:

VMware View

The cornerstone of the Mobile Secure Desktop solution, VMware View modernizes desktops and applications by moving them into the cloud and delivering them as a managed service. With VMware View and ThinApp™, IT has the ability to grant or restrict access to desktops, data and applications based on endpoint device configuration, network location and user identity.

From the end user's perspective, View with persona management makes it possible to work from virtually any location using any qualified device to access their personal desktops—including corporate and personally owned PCs, thin clients, zero clients, iPads and other tablets. The user's familiar desktop appears across devices and locations with everything in the right place; with all authorized applications, files, and data available; and with everything functioning as expected.

vCOPs for View

vCenter Operations Management for View allows IT administrators to have broad insight into desktop performance, quickly pinpoint and troubleshoot issues, optimize resource utilization and proactively manage their desktop environment.

vShield

The vShield suite of products, including vShield App and vShield Edge, allow IT to effectively firewall virtual machines and partition networks and resource pools. With vShield App, IT can apply rules to VMs based on IP addresses as well as business or application requirements. vShield Edge allows for segmentation of resource pools and allows IT to provide a common set of services to VMs that reside within a defined perimeter.

In addition, vShield Endpoint provides the intermediary for anti-malware and deep packet inspection. This allows IT to enhance endpoint performance across the desktop environment by offloading virus scanning to secure VMs—effectively eliminating the need to install complex antivirus agents inside each individual virtual machine.

Summary

The Mobile Secure Desktop from VMware is a managed solution that integrates technology from VMware and our partner ecosystem. The solution leverages mobile, wireless and wired networks; vShield security services and monitoring components to better protect data and monitor IT infrastructure and endpoints across locations.

This solution is optimized for organizations looking to drive higher levels of productivity by improving end-user access across devices and locations, reduce costs by streamlining desktop management, and enhance security and compliance.

Learn More about the Mobile Secure Desktop

For additional information about how the Mobile Secure Desktop solution is built and validated, read the Mobile Secure Desktop Reference Validation document at vmware.com.

Or call VMware for an assessment today. Our experts will help you determine the opportunity for your organization—and chart your course to mobile, secure desktop access. For more information or to purchase VMware products, call 1-877-4VMWARE (outside of North America dial +1-650-427-5000), or visit www.vmware.com/products, or search online for an authorized reseller.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

10.Appendicies

10.1. Sample Draft Mobile Device Policy Document by ALGIM

Algimville District Council
Mobile Device Policy

Mobile Device Policy:

Purpose:
The purpose of this document is to set policy as to the appropriate use, security, support of, assignment of, governance, and employee responsibilities as to the use of mobile devices whether owned solely by Algimville District Council or supplied by the employees for any purpose subject to the work flow processes of the Algimville District Council, NZ government, associated Authorities, contractors, agencies, or any person or organization that receives any benefit by any council resource used on mobile devices enabled with Council provided resources such as email, telephony, messaging of any type, and other forms of communication. This policy also includes the use of intellectual property used, downloaded, stored, etc by mobile technology and communication devices.

Definitions:

1. Mobile Device: Any device or medium not permanently connected to the Algimville District Council network used for the purpose of receiving, sending, or storing information. This may include, but is not limited to, cell phones, laptops, computers, smart phones, tablets, USB thumb drives; digital storage media (CD, DVD, Thumb Drives, floppy disks, hard drives, etc.)

Responsibilities and Enforcement of this Policy:

1. Algimville District Council, has set forth this policy in an effort to meet or organisational goals, improve employee satisfaction, to improve efficiency for Council departments, agencies, authorities, and employees by enabling the use of mobile devices, and enabling those devices with access to Council resources (such as email).

2. Each employee, associate, etc. is responsible for the conditions set forth within this policy, as well as any other employee policy set forth within the HR Employee Policy Manual, and any subsequent policy set forth by the department, agency, authority, etc. for which an employee works, or has worked in the past within Algimville District Council.

3. The Council Manager, Division reports, Directors, Managers, and Supervisors at all levels shall fully understand this policy and be held responsible for any employee under his/her management for meeting the requirements set forth within this policy, and shall communicate the requirements of this policy for any and all persons that this policy applies.

4. The Technology Services department director or designee shall oversee all technical aspects of enforcing this policy, including creating and updating all approval forms, etc. which enable mobile devices to access Council resources.

5. Information used or stored on any mobile device shall be considered as important for security as any paper document in the operation of Council business.

6. Violations of this policy will be subject to normal departmental and/or Council enforcement policies, including termination as per the Employee Policy.

Cell Phones, Smart Phones, Tables, etc. (General):

1. All cell phones, smart phones, tablets, etc. purchased by Algimville District Council shall be purchased in accordance and from approved vendors as established by the Purchasing guidelines and policy, including any service contract accompanying any device.

2. Algimville District Council Technology Services in coordination with the Purchasing Department shall from time to time re-negotiate all mobile connectivity contracts, such as to establish best service for the best pricing possible under the constraints of the public bidding process or through RFP.

3. The need for a Council purchased mobile device, and securing all necessary funds is determined by each Department Director and/or Division Director. Costs include any cost for the device, monthly service fees, licensing fees, client access licenses, and MDM (Mobile Device Management) licensing.

4. Any mobile device that connects to the Algimville District Council network shall be managed by MDM (Mobile Device Management) software and licensing. This includes any device that accesses Council Email, Council Phone System, or other system or resource located within the Council Network or Networks.

5. Conditions which must be met for any device to be enabled to access Council email:
   a. Employee must complete a mobile Device Security Request Form signed by the Employee and the Employee’s Department Director.

b. All requests for email enabled devices must be approved by the Department Director or Equivalent.

c. All Department Directors and/or Equivalent shall be aware of appropriate use of email for employees.

d. If at any time any email enabled device is lost or stolen, the employee for which the device is assigned is responsible for immediately reporting the loss to the Technology Services Department. The Technology Services Department shall then remotely disable, lock, and/or "wipe" the device, therefore rendering the device inoperable.

e. All email enabled devices shall be required to automatically "Lock" after a reasonable period of inactivity (no longer than 2 minutes), and must be password protected to "unlock" the device.

f. All email shall be archived, and stored on central servers. Email may be accessed, but never permanently removed from central servers, archiving solutions, etc. in accordance with the email retention policy.

g. Employees granted access to email on mobile devices shall strictly follow protocols for replying to any email request during any time even while not at work, without explicit written directions from the Department Director or Equivalent and/or the Council Manager.

BYOD (Bring Your Own Device):
Algimville District Council Recognizes the following:
The consumerisation of technology has had its greatest impact on mobility during recent years. The iPAD triggered a monumental shift in the tablet market, which has sparked a consumer-driven revolution. End users continue the push to allow their own devices on the enterprise network. Many other personally mobile devices have entered the market and are owned by Algimville District Council employees. These include, but are not limited to, smart phones, tablets, laptops, GPS, etc. utilizing a variety of operating systems and varied technologies.

In an effort to satisfy demand from Algimville District Council employees and/or Departments, Algimville District Council sets forth the following policies to allow for personal technology enabled devices to access resources within the Algimville District Council network:

1. Any personal device enabled to access any resource provided within the Algimville District Council network and the employee given access to said resources on his/her personal device SHALL adhere to all policy statements within this Mobile Device Policy, Employee Policy, any supplemental

departmental policies that are more stringent such as SOPs (Standard Operating Procedures).

2. Any employee requesting for their personal device to be enabled to access Algimville District Council network resources (such as email) must read and fully complete a Personal Device Access form which must include the signature of the employee requesting access AND the Department Director or Equivalent (Highest Ranking Manager in the Department).

3. Employees granted access to Council network resources on their personal devices shall allow the Technology Services Department to install MDM (Mobile Device Management) software on the device for which access is granted. Employee understands this gives the Technology Services Department the ability to Manage, Copy, See, Retrieve, Download, Install, Disable, Lock, Change Passwords, Track, and Wipe any device under the management platform.

4. Employee acknowledges that if lost or stolen, he/she must report the loss to Technology Services Immediately.

5. Personal Devices enabled with access to Algimville District Council network resources shall be capable of remotely disabling, locking, wiping, and or any combination. Employee's personal device and/or data will not be the responsibility of Algimville District Council, or Algimville District Council Technology Services Department to maintain, safeguard, backup, protect in any shape form or fashion.

6. Personal Devices enabled with access to Council network resources shall, upon request by employee's Manager or Equivalent, Human Resources Director, , Council Chief Executive, or Technology Services Director be relinquished into the custody of the requesting officer of the Council for examination at any time with no set time of return to the employee. Employee must provide all necessary passwords and any information requested for appropriate examination of a personal device.

7. All information contained on any personal device shall be considered as public record and subject to Official Information requests, discovery, investigations, etc. but not limited to.

8. At no time may a personal device enabled with access to any Council network resource (such as email) be used by any personnel other than the employee granted access. (Example: If ADC enables your iPAD with Council email, you cannot share your iPAD with a spouse, child, friend, neighbour, colleague, etc.) Employee shall not share passwords with anyone other than those indicated in this policy.

9. The Technology Services Department will not provide technical support for any personal mobile device, except to provide initial setup, security, MDM software, and to disable, “lock”, and/or wipe devices when needed to ensure the security and integrity of the Algimville District Council Network. Employees are encouraged to utilize the Internet (www.google.com, youtube.com, user groups, and their devices manufacture resources) for any problem resolution with their personal device.

10. Failure to meet any of the conditions set forth within this policy may result in the termination of access to Algimville District Council Network resources, disciplinary procedures by the employee’s department, Human Resources, or the Council Manager up to and including termination and seizure of the device used in the violation.

Other General Issues:

1. From time to time employees approved for Council purchased mobile devices request a premium upgrade beyond and above budgeted amounts for certain requested devices. Upon approval by the Department Director or Equivalent an employee may choose to supplement Council funds to acquire a premium product at the employees own expense. When this is approved, employee understands that providing “the difference” in price to be provided a device other than what is budgeted for that a payment must be made to Algimville District Council, and is given as a donation to the Council at the time of payment. No premium device shall be ordered until after Finance has approved the transaction. Employee also agrees that the entire device is owned by Algimville District Council and is treated as such no matter how long the device is used by the employee. Premium service charges may also apply for premium products and it shall be the employees responsibility to cover any additional charges per month/year/etc. as long as they use the device in the course of their assignment with Algimville District Council.

2. APPS (Applications) on mobile devices:
   a. Unless previously approved by the Department Head and budged for, no applications shall be downloaded to any device that cause a charge, invoice, withdrawal, etc. to any Council Funding mechanism, credit mechanism, or purchasing mechanism.

   b. Consumer Grade mobile devices are mostly capable of downloading and the use of APPS (Applications or programs). The Technology Services Department may at its disgression limit, restrict, or allow the capability for devices granted access to Algimville District Council network resources the ability to download and use commercially available Apps.

c. If at any point Technology Services discovers any downloaded app has or has the potential to compromise security to the network, Technology Services shall disable, lock, and/or wipe the compromised device. As soon as possible, and render it unusable for network access. The Technology Services Department will report the incident to the Department Director or Equivalent of the employee whose device was deemed to be compromised.

d. Other “for a fee” downloads such as Music, Videos, Movies, etc. : It is the sole responsibility of the end user / employee to pay for any downloaded media of any type for which a fee is charged. It shall not be the responsibility of the Council, Technology Services, to backup, maintain, or otherwise protect any personally downloaded applications, content, music, videos, movies, etc. unless expressly approved and paid for by Algimville District Council.

Attachments (coming later): See the Security Request form

Also see Section 5.3 “Mobility Device Policy Considerations” for some additional policy topics to bring into the policy discussion.

10.2. Kaon Mobile Device Policy (Abbreviated), SecurITy Overview

IT POLICIES AND PROCEDURES

Mobile Device Policy (abbrev) This policy is an extract from the Kaon SecurITy Ltd IT Policy System.	**Approved By EMT:**		Kaon SecurITy
	Date Created:	31/10/2012	
	Date/s Revised:	30/10/2012	
	Next Review Date:	31/10/2013	
	Document No:		
	Directorate:	Information Technology	

PURPOSE

The purpose of the Mobile Device Policy is to advise acceptable use with regard to devices and systems used for business communication. With the convergence of data and voice systems, the ability to connect remotely to internal systems and the wide range of options offered by mobile devices it is essential that these systems be used by authorised persons for legitimate business activities.

POLICIES

1 Acceptable Use of Council Mobile Devices

1.1 Mobile devices and communications systems are provided to facilitate business activities. Personal use is permitted as follows:-

- Calls and text messages to the value of $20 per month
- The data plan must not be exceeded due to personal use

Managers are provided with monthly reports and personal use over this level may be required to be reimbursed.

1.2 A phone supplied by *MY COUNCIL* may not be used in connection with any personal commercial business activities. The number may not be published in any non-Council publication or business card.

1.3 The allocation of Council mobile devices and usage plans must be approved by a Department Manager. Mobile devices that are to be connected to, or synchronised with Council's network must be a type and model approved by the IT Manager and procured through the IT Department.

1.4 The user will be required to sign the Loan Equipment Form when allocated the device. This form is resigned when the device is returned to Council.

1.5 Mobile devices provided by *MY COUNCIL* are to be used in an effective, safe, ethical and lawful manner. Use will be monitored.

1.6 Users of *MY COUNCIL*'s mobile devices must not use these systems to engage in any activity which violates or infringes upon the rights of others or which a reasonable person would consider to be abusive, profane, offensive or defamatory.

1.7 Users of mobile devices with the ability to connect to the internet must abide by the provisions of the Internet Use Policy. The downloading and use of mobile applications on devices provided by Council must be approved by the IT Manager.

1.8 Where communication systems support synchronisation with mobile phones for the purposes of receiving and sending email the provisions of the Email Policy apply.

1.9 Emails, instant messages, tweets and text messages that are of a commercial nature and are being sent to external parties must comply with the requirements of the Unsolicited Electronic Messages Act 2007. This policy is particularly relevant to those sending multiple emails using distribution lists or sending text messages to multiple recipients using server technology like Twitter. If you are unsure please contact the IT Helpdesk for assistance.

1.10 Mobile devices must have a current and supported operating system installed to mitigate security risks.

1.11 Mobile devices supplied by *MY COUNCIL* must not be altered or added to in any way including:-

- unauthorised upgrades
- addition of components
- removal of components
- altering configuration or security settings
- installation of non-approved applications

All devices will be centrally managed and any changes or maintenance carried out by the IT Helpdesk or designated agent.

1.2 Users allocated mobile devices are expected to act with due care and diligence in protecting it from theft or harm. In the event of loss, damage or misuse staff may be required to contribute towards replacement or repair or to repay the insurance excess.

1.13 If a mobile device in the care of the user is lost, stolen, damaged or unavailable for normal business activities this must be reported to the IT Helpdesk immediately.

1.14 *MY COUNCIL* maintains the right to conduct inspections of any communications equipment it owns or manages without prior notice to the user or custodian.

1.15 Mobile devices are to be returned to the IT Helpdesk upon request for updates to the device or applications, upgrading to a new version, if damaged or not working properly and when employment ceases.

1.16 Users shall not lend the mobile devices allocated to them for business activities to others external to Council including friends and family.

1.17 Mobile devices must be used in a way that does not void manufacturer or vendor warranties or insurance.

1.18 Games, freeware, shareware, movie clips or music may not be downloaded, copied, accessed, stored or used on any Council provided mobile device unless specifically required for Council business.

1.19 Users of devices that have the ability to transfer information through networking capabilities must be aware of the possibility of information leakage and the potential for data to be intercepted by another device.

1.20 Mobile devices supplied by Council must be protected by a PIN number or password and auto-lock. Voice authentication (if used), must be coupled with password or PIN authentication.

1.21 Users allocated a mobile broadband card for mobile computing are responsible for their care, use and charges against those cards.

1.22 Mobile telephones must not be used while operating a vehicle unless a hands-free or blue tooth kit has been installed and is operational.

1.23 When travelling overseas users must turn global roaming functionality off as international data termination costs are prohibitive. Staff are advised to use hotel wifi connections for internet access or only enable global roaming for a short period for the purposes of collecting email.

2. Bring Your Own Device (BYOD)

2.1 Personally owned communication devices may not be connected to or synchronised with *MY COUNCIL*'s computer systems or networks unless approved by the IT Manager and the device owner agrees to the policies regarding the management of the device. BYOD policies include:-

- Agreement that the device will be managed by *MY COUNCIL*
- Agreement for the Council security profile to be applied to the device

2.2 The *MY COUNCIL* security profile will be enforced on all personally owned devices connecting to or synchronising with *MY COUNCIL*'s computer systems and networks and must not be changed by the user. The device will be remote wiped if lost, stolen and when the user no longer provides services to *MY COUNCIL* they will be required to bring the phone in so that Council data and the management application can be removed. Security policies may include:-

- PIN or Password Protection
- Autolock
- Anti Virus installed where available
- Personal firewall installed where available
- Encryption turned on
- Certificates installed
- Disabling non-essential communications functionality
- Limiting applications to those required for business purposes (e.g. disable Apps Store, Camera, iTunes, Cloud Storage Services, YouTube etc)
- The ability to remote wipe the device
- Auto update of the operating system

2.3 The costs associated with the use of a personally owned device for *MY COUNCIL* business will be reimbursed on receipt of an expense claim authorised by the Manager responsible for the user's cost centre. Proof of the expense incurred is required to be attached to the expense claim. Excessive costs such as the unauthorised use of global roaming will not be reimbursed.

2.4 Maintenance responsibilities for devices are as follows:-

- *MY COUNCIL* owned and supplied devices will be fully maintained by *MY COUNCIL*
- Personally owned devices connected to *MY COUNCIL* systems will be managed by *MY COUNCIL* but maintained by user.
- Personally owned devices not connected to *MY COUNCIL* systems will be managed and maintained by the user

Any issues must be logged with the IT Helpdesk.

2.5 Corporate data must be separated from personal data through the implementation of sandboxing or a no data at rest policy imposed which prevents data being stored on the device.

IT Policy System

Many organisations now rely totally on their electronic environment for the day to day processing and the management of their business. The issues of information management, confidentiality, competitive edge and profitability are intrinsically linked, but unfortunately, information in the electronic world is not attributed with the same degree of respect with regard to security as the paper document managed to achieve in its heyday.

The first step towards creating a secure electronic environment is to define the rules and guidelines for managing, operating and using corporate information systems.

This first step is critical and involves developing policies and procedures that document the intention to diligently manage electronic information throughout its life cycle and keep it safe from unauthorised persons.

To be successful, Information Systems Security Policies must be based on plain old common sense and all staff, contractors and third parties should be required to understand their obligations associated with the use of the Council's information systems.

Kaon SecurITy Ltd has developed a generic set of policies and procedures that are then uniquely tailored to match your organisation's specific environment in order to ensure that the policy set that your have matches what you do.

The policies are provided in a user friendly, web format that is easily deployed in any intranet environment or can be remotely hosted by Kaon SecurITy.

All Policies are presented by category of user so that general users do not need to read all the technical jargon to find the policies which affect them.

Editable Word documents and PDF images generated off these Word documents are also included should their be a requirement to present them for external audit purposes or for possible inclusion in a document management system.

What the Policies Do

Help protect the assets of the business.

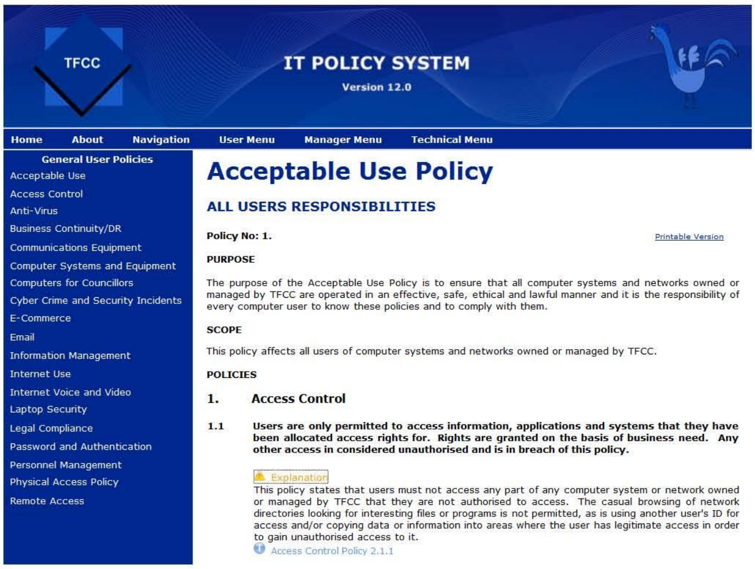
Provide the computer security framework for your organisation.

Provide a uniform level of control and consistent guidelines for management.

Communicate one computer security message to all in a format that is easily available and readily understood by staff.

Advise staff about computer security and about their responsibilities.

Endorse the commitment of the CEO and senior management in protecting valuable information assets.



Acceptable Use Policy

ALL USERS RESPONSIBILITIES

Policy No: 1.

PURPOSE

The purpose of the Acceptable Use Policy is to ensure that all computer systems and networks owned or managed by TFCC are operated in an effective, safe, ethical and lawful manner and it is the responsibility of every computer user to know these policies and to comply with them.

SCOPE

This policy affects all users of computer systems and networks owned or managed by TFCC.

POLICIES

1. Access Control

1.1 **Users are only permitted to access information, applications and systems that they have been allocated access rights for. Rights are granted on the basis of business need. Any other access in considered unauthorised and is in breach of this policy.**

This policy states that users must not access any part of any computer system or network owned or managed by TFCC that they are not authorised to access. The casual browsing of network directories looking for interesting files or programs is not permitted, as is using another user's ID for access and/or copying data or information into areas where the user has legitimate access in order to gain unauthorised access to it.

How the Policies are Organised

The policies are set out by category of user be it for User, Manager or Technical members of staff. In the past with paper versions of information systems policies, the general users found it very difficult to identify which policies related to them and generally had to wade through a lot of technical information that made the policies too difficult to understand.

Everyone who uses computer systems, communications systems or networks that make up the computing environment need to be familiar with the policies listed under the User menu.

Managers should be familiar with polices listed under both the User and Management menus while Technical staff need to be familiar with the policies listed under the Technical menu.

Security Audits

Security threats can manifest in a variety of ways involving human and non-human intervention. A typical audit involves an in-depth examination of servers, network components, the physical environment, operational procedures and an intrusion test.

The Kaon SecurITy audit process is a hands on test of how your systems operate and are being managed.

The level of protection is assessed against the amount of risk to the organisation. Policies, procedures, overall management and other mitigating factors are also scrutinised to ascertain compliance to corporate mandates and a comprehensive report is produced for the client highlighting the major areas of concern.

Risk management is becoming a big issue for large organisations and the Government sector. Auditing completes the compliance loop by highlighting the areas where you are at risk. In some cases you may already have policies that mitigate the risks, but are not complying with them and in other cases you will need to develop policy and procedures to ensure that gaps are closed in the future.

Audits can be customised to target specific areas of concern should a client suspect that anomalies exist within their IT environment.

All work is scheduled with the agreement of the client and carried out on the basis of a fixed price quote with a typical technical security audit taking two days on site. A full report is provided detailing vulnerabilities observed and providing recommendations for remediation.

Web Site Testing

Websites are developed with a variety of purposes in mind and this is reflected in the complexity of the design.

Should the website be compromised, the effects may not only damage the reputation of the organisation, but include the flow on effect of loss of sales, loss of customers, legal actions and even reparation.

Unfortunately, developers of websites range in competency from very bad to excellent and if the website functions, it is not always apparent if the code has been written well or is sub-standard.

How well your web site has been developed will have a huge bearing on how easy it is to gain unauthorised access to the site.

Kaon SecurITy has the tools and the expertise to provide an independent assessment of websites in order to determine vulnerabilities and weaknesses.

A comprehensive report and test results are provided at the end of the analysis highlighting any areas susceptible to attack and providing guidance how to remediate the vulnerabilities.

During the vulnerability process we perform a thorough investigation of the site, exploring it for code, pages and links that may have been left as a result of default installation or the development process.

Incident Response

Unfortunately there are times where things do go wrong and Kaon SecurITy has the skills to assist if you do ever have an incident.

In the event of an activity that may result in prosecution it is absolutely essential that every part of the process is followed according to the letter of the law if the prosecution is to be successful.

Kaon SecurITy already has experience in handling information security related incidents in Victoria and can assist with securing evidence, analysing evidence, liaising with the Victorian Police services and providing an expert witness at Court.

Even if your incident doesn't go that far we can provide you with post incident testing services and assist with providing advice about closing to vulnerability so that you can have a level of confidence that it won't happen again.

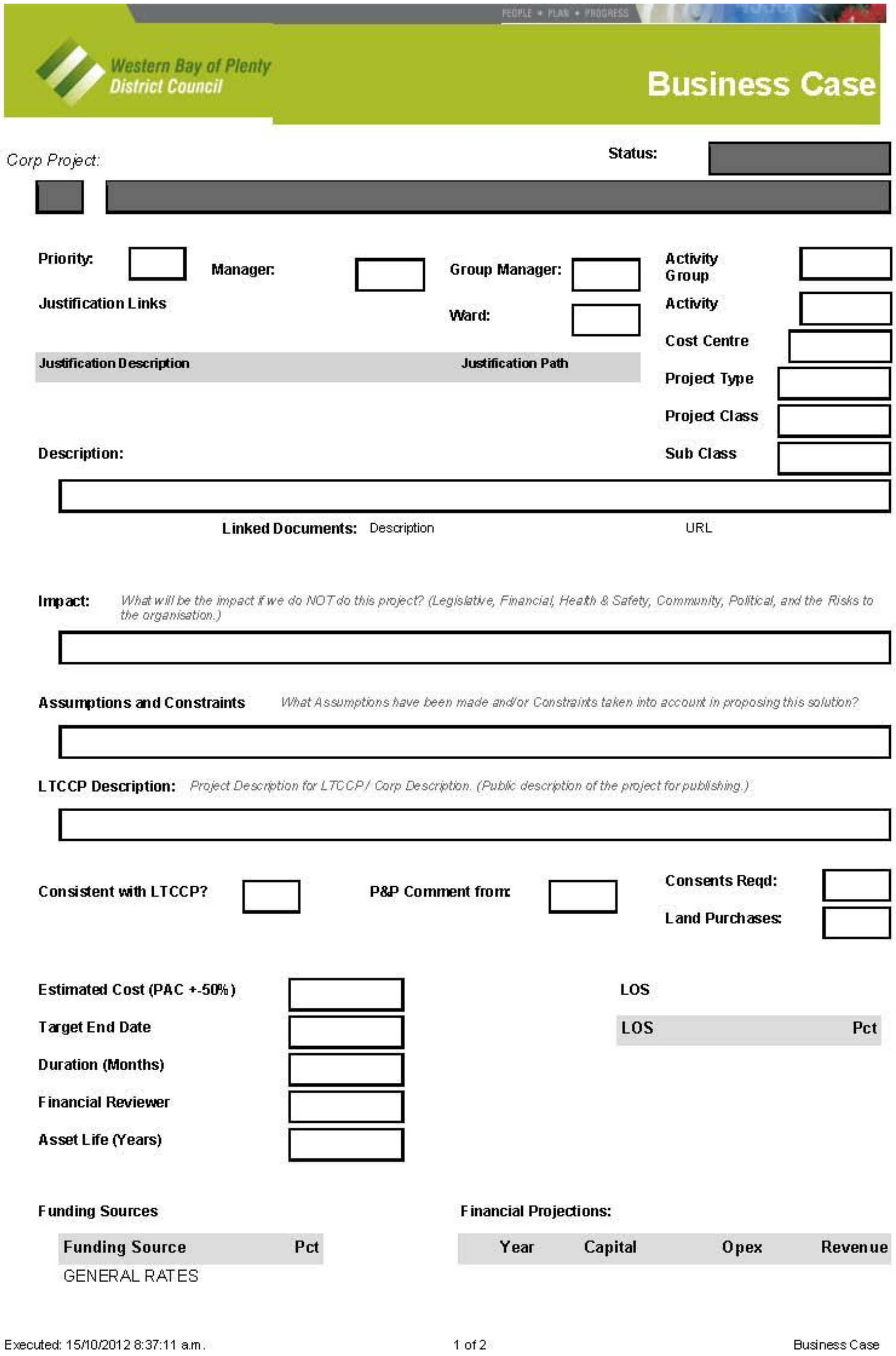
Kaon
SecurITy

Kaon SecurITy Ltd
PO Box 58521
Botany, Auckland

sales@kaon.co.nz
0011 64 9 274 1590
www.kaonsecurity.com

Or contact MAV Procurement for further information on contract IT8010

10.3. Business Case Template



PEOPLE • PLAN • PROGRESS
Western Bay of Plenty District Council

Business Case

Corp Project:

Status:

Priority:

Manager:

Group Manager:

Activity Group

Justification Links

Ward:

Activity

Cost Centre

Justification Description	Justification Path

Project Type

Project Class

Description:

Sub Class

Linked Documents: Description URL

Impact: *What will be the impact if we do NOT do this project? (Legislative, Financial, Health & Safety, Community, Political, and the Risks to the organisation.)*

Assumptions and Constraints *What Assumptions have been made and/or Constraints taken into account in proposing this solution?*

LTCCP Description: *Project Description for LTCCP / Corp Description. (Public description of the project for publishing.)*

Consistent with LTCCP?

P&P Comment from:

Consents Reqd:

Land Purchases:

Estimated Cost (PAC +-50%)

Target End Date

Duration (Months)

Financial Reviewer

Asset Life (Years)

LOS

LOS	Pct

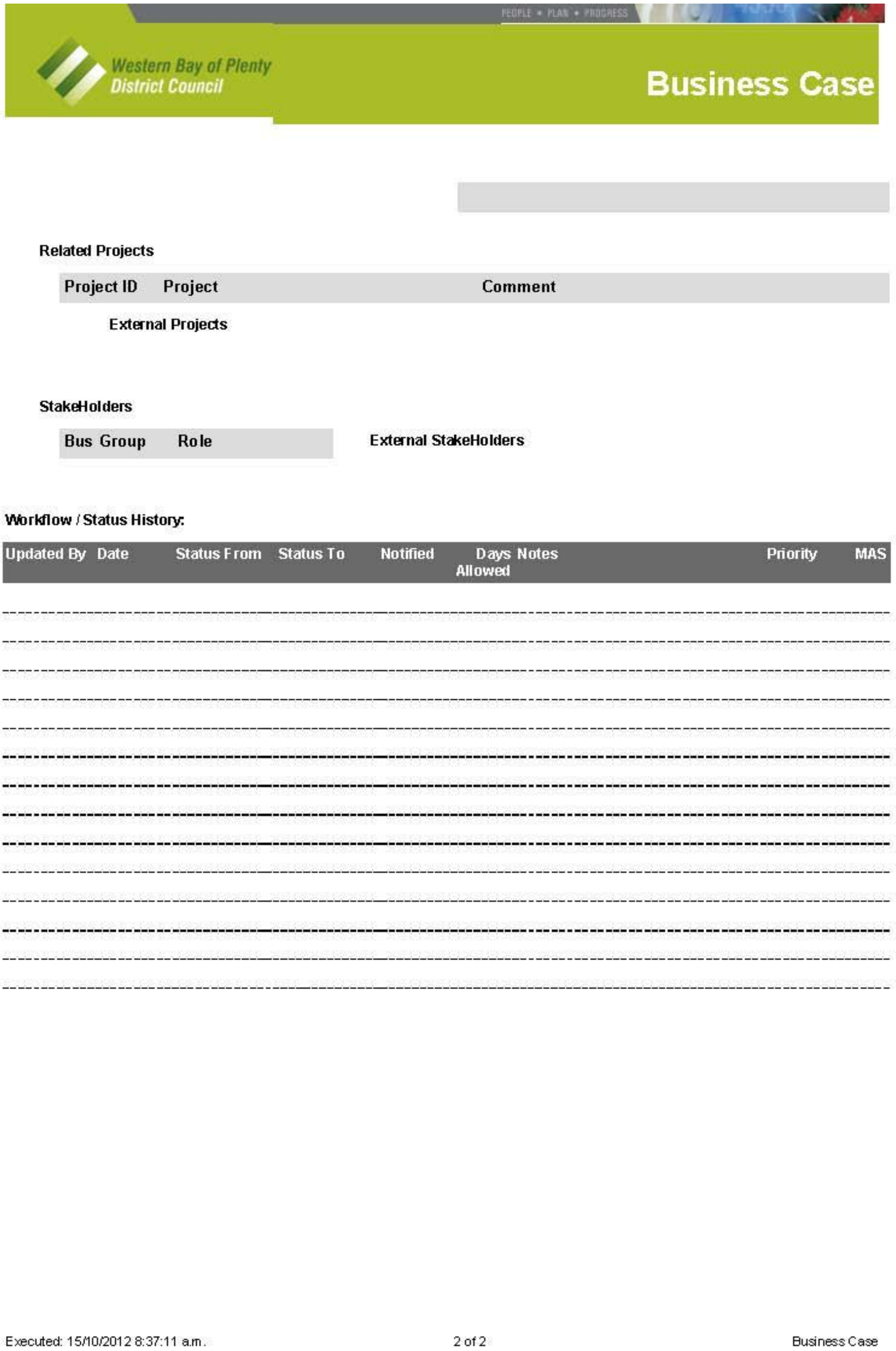
Funding Sources

Funding Source	Pct
GENERAL RATES	

Financial Projections:

Year	Capital	Opex	Revenue

Executed: 15/10/2012 8:37:11 a.m. 1 of 2 Business Case



PEOPLE • PLAN • PROGRESS

Western Bay of Plenty District Council

Business Case

Related Projects

Project ID	Project	Comment

External Projects

StakeHolders

Bus Group	Role

External StakeHolders

Workflow / Status History:

Updated By	Date	Status From	Status To	Notified	Days Allowed	Notes	Priority	MAS

Executed: 15/10/2012 8:37:11 a.m. 2 of 2 Business Case