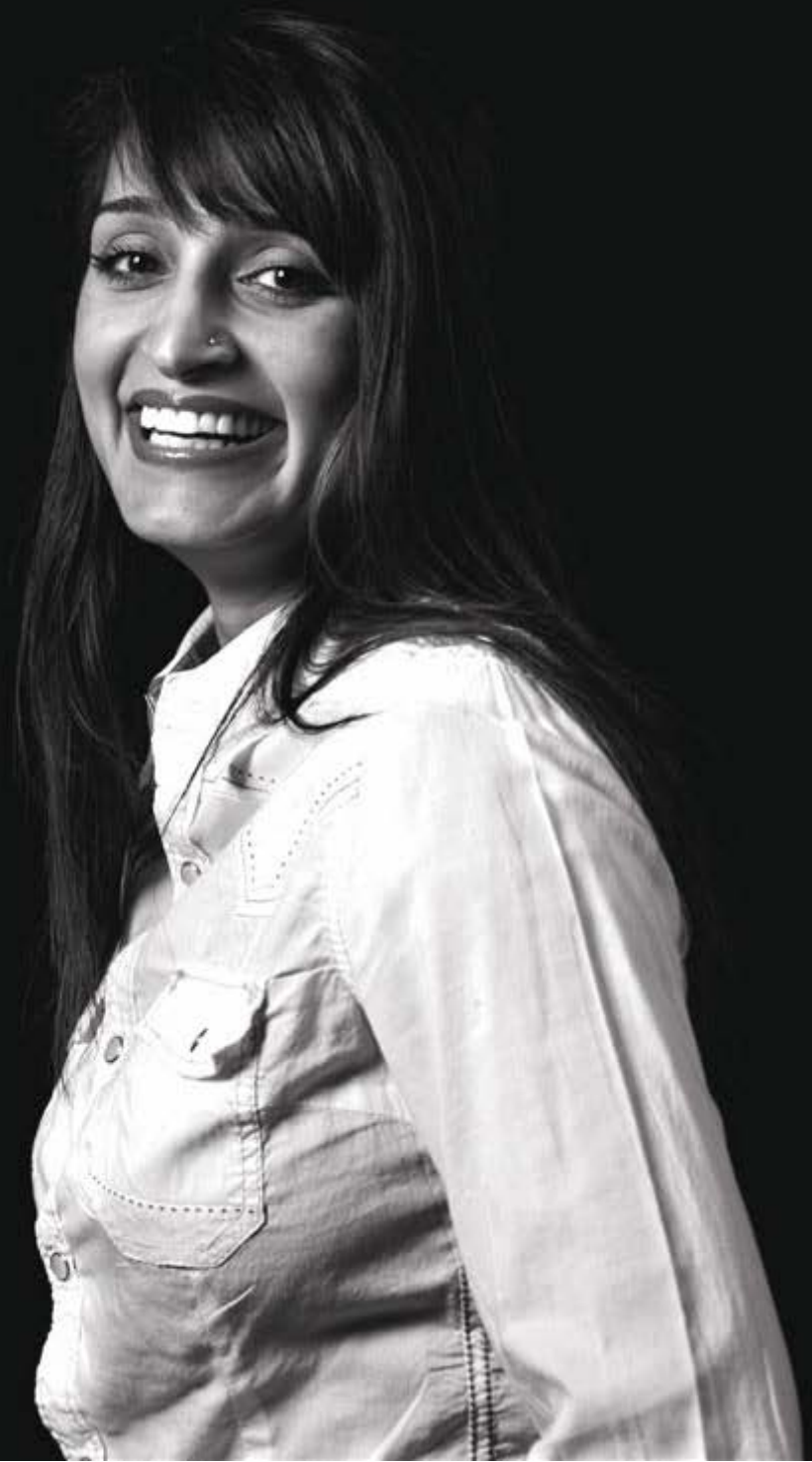
Thomas Duryea LOGICALIS

Business and technology working as one

Leveraging *mobility* in your organisation

Building an effective enterprise mobility environment that delivers competitive advantage



Creating an environment that provides employees with freedom in where and how they work and fosters innovation – without compromising security – requires commitment from the CIO across a broad spectrum of elements, both technological and organisational. Every organisation will need to respond differently given its particular circumstances.

While "mobility" until recently was often synonymous with providing email access on mobile phones, today the concept means a lot more. An effective mobility strategy provides "anytime, anywhere" access to corporate applications and data from any device based on a security policy. It extends controlled network (WiFi, LAN and VPN) access to guests, contractors and third parties. Supports voice and video. And incorporates location services to track devices or provide analysis of wireless users and devices.

This Guide describes the steps we recommend to building the foundation for an effective workplace environment, by enabling mobile devices to securely access the network. It also looks beyond the basic infrastructure and how mobility can provide a strategic business advantage.

There are six stages CIOs should consider:

1. Building the strategy
2. Auditing the current environment
3. Setting the policy framework
4. Managing devices on the network
5. Enforcing policies to secure applications and data
6. Analysing the data.

The Business Benefits

Our approach to designing and implementing a mobility strategy takes into account operational efficiency (is it easy to manage), security (is it secure) and productivity (does it make staff more effective, help employee retention or provide competitive advantage). An effective mobility environment allows organisations to:

- **Provide control over access to corporate resources** from the proliferating number of mobile devices (which are often beyond the reach of many IT management systems).
- **Consumerise their corporate IT** into a delivery format that is becoming the new standard; enabling users to select the relevant application/s and start using them. This self-service format delivers a better IT experience and reduces the administrative burden on IT.
- **Offer a seamless, consistent user experience,** across any device the user chooses work with - regardless of what location (whether it's the office, home or airport) that users are working at. This reduces user training requirements, increases employee productivity and improves staff retention.
- **Allow the IT department control** over the spread of corporate data and the ability to secure it across a range of mobile device platforms; but allow users to access the data they need to stay product across any mobile device. This not only increases security but can also assist with achieving regulatory and corporate compliance.
- **Reduce the "attack surface" of the organisation** by enabling a controlled and planned approach to device access. This results in allowing users to bring their own devices and connect to corporate resources, either in the office or remotely, in a secure and controlled manner.

1. Building the Strategic Plan

An effective enterprise mobility strategy starts with building a coherent plan for the business. Whilst this is a truism for most IT projects, it's particularly important as organisations break down traditional security and communications barriers to enable a more effective workplace. Work habits are shifting, work locations are varied and work devices are many. This requires a greater degree of change leadership than is typical, rather than simply change management, from the CIO and their team.

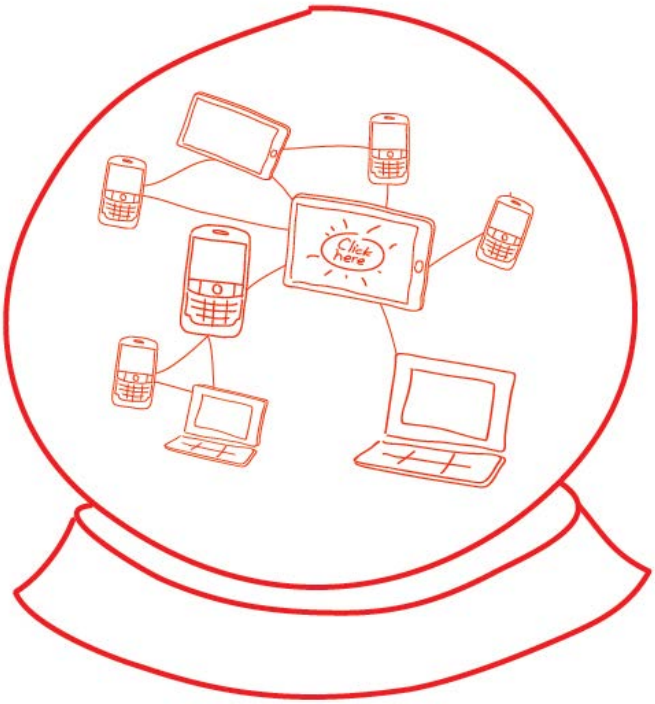
Rather than block or deny employees from using their own devices in the work environment, many organisations are encouraging this as a new form work practice (while being able to mitigate and manage the potential new risks this introduces). Increasingly, employees will attempt to do this anyway; creating a strategic plan offers a sanctioned method that will prevent unauthorised and insecure methods whilst increasing employee satisfaction.

Involving business functions such as Human Resources, Legal and Finance as well as relevant functional heads, such as sales is critical to building an accurate picture of the organisation's requirements. Many of the organisation's business processes will need to change to remain relevant in the evolving workplace.

"The challenge for CIOs is to think beyond simply what internal stakeholders say they want and deliver real innovation and a competitive advantage for the business. This is no easy task and CIOs must find the balance between being evangelists and demonstrating genuine value."

– Don Holley, Mindset Group

Time spent planning ensures a much greater chance of success. Some areas to consider are:



- **Business Objectives:** Capture the business objectives, which may stretch beyond the immediate business requirements driving the initial engagement. By gathering this information, the organisation ensures that the technologies supporting mobile devices are implemented within a strategic framework rather than just a simple tactical platform.
- **Business procedures:** How will allowing personal as well as work devices to be used in the workplace affect current policies and processes? How will this plan be positioned to benefit employees in a way that the organisation can use as a competitive differentiator to assist with staff retention as well as operational agility?
- **Operational procedures:** How will a secure data and application mobility policy impact users? Implementing a secure mobility strategy for data and applications with the supporting technology is assisted by the use of self-service enrolment, automatic device detection and the encouragement of user self-support. This forms what is called the 'social contract': the agreement between users and the organisation of the rights and responsibilities on each party engaged in the initiative.
- **Lifecycle management:** The rate of change in mobile operating systems requires the organisation to maintain a current list of devices and supported operating systems that users can base their purchasing decisions upon. This will require an administrative function, potentially calling on assistance from product champions within the wider organisation to test operating system updates for mobile devices and communicate update requirements to users.

2. Understanding the current environment

The first step before designing, implementing or extending an enterprise mobility management solution is understanding the current environment, and any potential risks that need to be addressed.

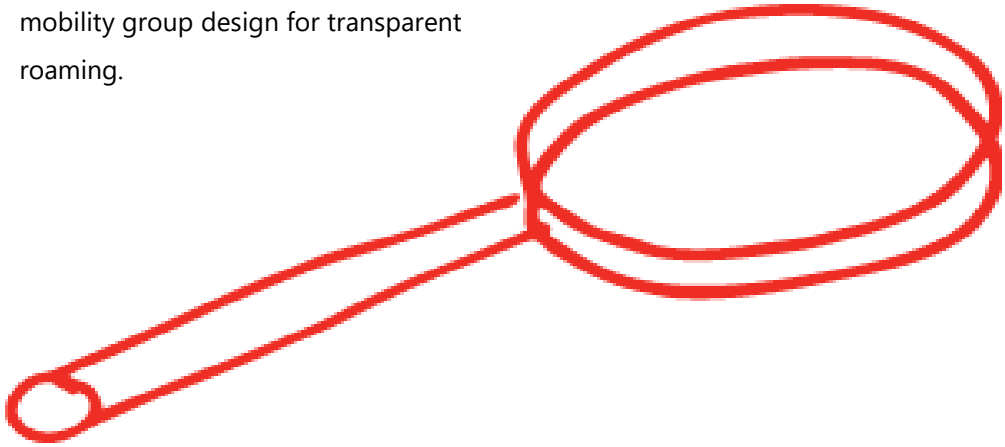
A mobility assessment looks at the current end devices to help ensure optimal performance for mobility applications. The assessment looks at:

- categorising data and applications to be mobilised including any restrictions based on device type, location and user type (employee, contractor or third party)
- hardware and software versions and configurations of primary wireless LAN network devices
- profile of all attached devices and their operating systems
- Wireless LAN client authentication and encryption, rogue access point detection, and intrusion detection
- QoS settings, including prioritization for control, voice, video, and data traffic
- mobility group design for transparent roaming.

The result will depend upon the requirements of the organisation and can include a comprehensive suite of reports on non-compliant client devices that have been detected. Non-compliance in this context refers to any client device (desktop, SOE laptop, third party laptop, mobile device) that does not meet a baseline minimum standard acceptable to your IT and Security team.

These reports provide a clean and accurate view of the current state of these devices, as well as the best steps to remediate any issues. Analysis of the data and applications that are required enables the most suitable delivery method to be chosen to meet the workstyle of that group of users. Options include secure caching data on local devices for offline access, online application access or deployment of mobile applications to the chosen device platforms.

As well as identifying any security issues, this approach can assist with PCI audits and compliance, demonstrating that you have a comprehensive plan to deal with any shortcomings.



"Herein lies a major risk. A badly implemented BYOD policy can have catastrophic consequences; something that's recognised as a concern by many respondents."

– Ovum Research study commissioned by Logicalis Group

3. Setting the Policy Framework

A key requirement for mobilising data and application securely and controlling devices is the ability to create and apply a policy that governs the access too corporate resources whilst maintaining security:

- Controlling who accesses the network (from a LAN, Wi-Fi and VPN perspective) – and what they can access once connected
- Applying policies that determine what corporate data can be accessed and how it can be stored.
- Managing the retention and deletion of that data on devices
- Minimising the risk associated with lost or stolen devices and partitioning corporate data on personal devices.
- Enabling access to internal resources (file shares, intranets, SharePoint) from external devices
- Creating a consistent user experience when accessing corporate data and applications

An effective policy should facilitate the use of various consumer devices or corporate devices from other organisations in the corporate environment, while exercising policy controls and giving IT control over the corporate data that is contained on those devices, and the ability to remotely wipe or remove such data in the event that such devices are lost or compromised.

Thomas Duryea Logicalis (TDL) uses **Cisco ISE (Identity Services Engine)** and **Citrix Workspace Suite** to provide effective implementation of very granular access policies while allowing organisations to develop the necessary workstyles. The concept of a workstyles is that the IT Department can map access to corporate data and applications in a manner that suits the requirements, or workstyle, of each group of users.

"More than 70% of Australian IT managers believe their users are removing corporate data from the network with consumer based Cloud services"

– Australian Reseller News

4. Managing Devices on the Network

Not long ago, it was termed "mobile device management" or MDM – but that was really just about the device. The next evolution of is **Enterprise Mobility Management**, which encompasses mobile devices, apps and data.

EMM offers the CIO a way to address the management and control of both corporate owned and non-corporate owned mobile devices and the corporate data they hold across the main tablet platforms. It enables the IT Department the ability to provide mobile versions of corporate applications that drive productivity and provide a consumer-like experience on a corporate device (a unified corporate app store).

Of course, EMM also gives you the ability to analyse a mobile device, establish its current configuration and enforce a policy on the device regarding the access that it has to corporate resources. Organisations should seek to not only enforce this policy but control the configuration of the mobile device; such as its ability to connect to corporate resources or access corporate email based upon its current compliance status. This allows you to take selected actions as a device falls out of compliance. This might be from an incorrect password, through to rogue application installation or detecting that a device has been compromised (ie jail broken).

Organisations should seek the ability to control not only the applications and connections from the device to the corporate environment, but to collect real time device usage information and selectively wipe corporate data from non-corporate devices as required.

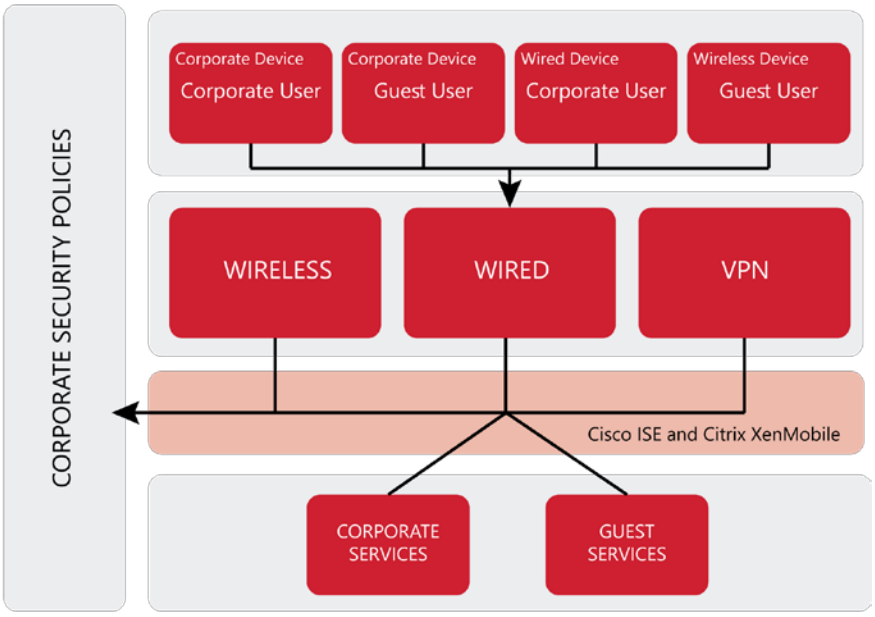
5. Enforcing policies to secure data and applications

An important goal is to set up an identity and access control policy platform that allows you to enable new business services, enhance infrastructure security, enforce compliance, and streamline service operations.

Organisations have to gather real-time contextual information from networks, users, and devices to make proactive governance decisions by enforcing policy across the networking infrastructure - wired, wireless, and remote.

The services that need to be provided are:

- Authentication
- Authorisation
- Accounting
- Posture
- Profiling
- Device on-boarding
- Guest management.



CIOs should try, wherever possible, to unify these services on a common platform to reduce complexity and provide consistency across the enterprise. Administrators can then centrally create and manage access control policies for users and endpoints in a consistent fashion and gain end-to-end visibility into everything that is connected to the network.

Having a clear and complete security policy for users and devices authenticating to the network is key to a successful implementation. This enables CIOs to:

- Apply corporate security polices to all wired and wireless authentication requests.
- Enable corporate devices to securely authenticate to the corporate network.
- Apply differentiated policies based on the type of user, location and the device they are attempting to connect on.
- Enforce traffic segregation for non-corporate users and devices.
- Provide a basic self-service guest wireless portal.

6. Analysing the data

In development as a suite of overlay capabilities specifically for Cisco-based Wi-Fi infrastructure, Thomas Duryea Logicalis Location Analytics Services provides enhanced data capture, analysis and reporting of the behaviour of wireless assets and users as they connect to and move about a wireless network.

This improves the integration and utility of wireless networks within the business, whether it's making intelligence about clients or devices more accessible to decision-makers, improving the experience and services available to employees or customers or providing more avenues to engage and interact with wireless users. Applicability is broad-based and includes entertainment, hospitality, education and healthcare industries, but essentially can extend to any business with wireless users or assets that would benefit from tracking or improved interaction.

TDL Location Analytics Services are structured around three main pillars of functionality that are aligned to easier and more comprehensive business outcomes using location intelligence than are ordinarily available from a standard Cisco Wi-Fi solution. While the portfolio makes the analytics available from a Cisco solution more visible and available to the IT Department, it specifically provides the tools and interfaces that allow business stakeholders outside of IT (marketing, brand alliances, HR or property/facilities) to view, interact and influence wireless users themselves.

TDL Location Analytics Services transform Cisco Wi-Fi infrastructure into a strategic asset and business-enabler, introducing the notion of a 'Connected User' that by connecting to the wireless network also becomes connected to the business, both passively and actively. While the services provide the ability to build point-in-time and extended period understanding of the time and motion behaviour of users and their devices, their true benefit is the ability to drive a series of engagement actions and outcomes within the business.

Thomas Duryea Logicalis Location Analytics Services are structured around three main pillars of functionality

An effective way to demonstrate the power of secure mobility is to demonstrate a number of applications that showcase the technology in use in a variety of commercial settings – including, retail, services, utilities and health.

Secure Mobility Use Cases

TDL has delivered secure mobility solutions across almost every industry: the technology (Citrix XenMobile, Cisco ISE, switching, remote access and wireless) and services are similar but the outcomes achieved are varied. The use cases below highlight some of the business solutions we've delivered customers through our approach to secure mobility.

Retail – Dealership	
The business	A large national car dealership.
Business Driver	The dealership wanted to provide an enhanced showroom experience where visitors could access and interact with relevant content without necessarily engaging with a salesperson.
Use Case	Thomas Duryea Logicalis enabled a guest wireless network and a guest portal. Dealership visitors could log onto the network by entering their contact details and then access specialised web pages that provided information and content about the vehicles on display. The contact information was supplied to marketing for subsequent follow-up. At the same time a separate secure wireless network enabled sales staff to access sales specific content on an iPad, for use when speaking with prospective buyers.

Professional Services

The business	A global management consultancy
Business Driver	The firm wanted to enable a truly mobile workforce
Use Case	This global management consultancy wanted to enable true activity based working in a brand new facility in one of its state-based offices. Staff members typically work on multiple projects, at multiple locations all hours of the day and night. In order to create a genuinely mobile workforce users had to be able to log on using any device at any time and from anywhere. Thomas Duryea Logicalis enabled a simplified environment where users could seamlessly onboard their device and provision it themselves without the intervention of the IT department.

Infrastructure Provider

The business	A state owned power company and a public private partnership infrastructure provider.
Business Driver	Both organisations had a number of critical compliance requirements.
Use Case	The finance function was responsible for ensuring the organisational governance and compliance requirements with regard to data access and security. Thomas Duryea Logicalis provided a means to authenticate all devices wishing to access both the wired and wireless networks, regardless of whether it was an employee's device, guest contractor, a printer or even a device on a remote network. In one case there was an additional level of required security, each device had to have up to date anti virus protection before the device could be authenticated.

Airline

The business	A low cost international carrier.
Business Driver	The need to control secure access to different sets of data.
Use Case	Each mobile device used by the staff members was loaded with a virtual desktop. In order to control secure access to data, the airline needed to know each time the virtual workstation was fired up. The

	airline would then apply strict segregated data access policies based on the profile of the virtual desktop.

Financial Services

The business	A major financial services institution.
Business Driver	A PCI auditing requirement to be able to report on the status of compliant and non-compliant devices connected to the company's wired/wireless network.

Government health agency

The business	Government Local Health Districts
Business Driver	A requirement to enforce a minimum standard of compliance on over 900 devices that have in the past been notoriously difficult to control and manage.
Use Case	The government Local Health Districts upgraded and revamped their Cisco ISE installation to performing posture assessment on their mobile client devices, as well as deploying full Enterprise Mobile Management (EMM) from Citrix XenMobile to gain integration to fully leverage ISE's capabilities. With over 500 Android and iOS devices and 400 Windows 8 laptops/tablet PCs potentially containing sensitive information, they are proving a real challenge to manage and secure. Cisco ISE allow the Local Health Districts to not only have detailed visibility and reporting on any device connecting into their network resources.

Thomas Duryea LOGICALIS
Business and technology working as one

Next Step: developing the Roadmap

Most organisations already have some wireless infrastructure in place; many don't have a granular security policy or the ability to utilise location services or analytics. We can help.

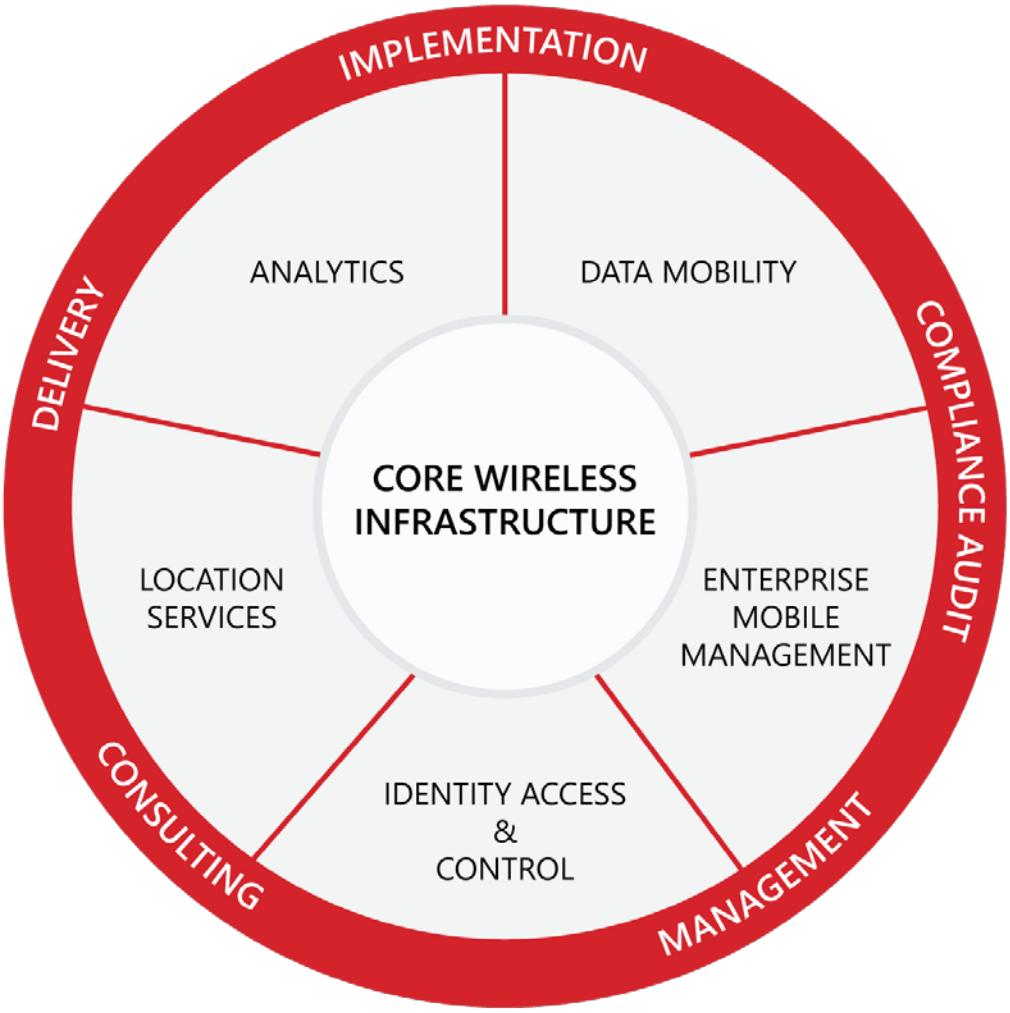
A relatively small investment in developing an effective mobility infrastructure can yield significant business outcomes (as well as improved security). The first step is to develop a roadmap that aligns with your organisation's IT strategy and to review the effectiveness of the current infrastructure.

What can we do for your organisation

Contact Thomas Duryea Logicalis to learn how we can help.

Visit
tdlogicalis.com.au

Call
1800 453 454



cisco Gold Partner

CITRIX®

DISCOVERY TECHNOLOGY