Managing mobility as a business imperative: identifying savings and finding the right partner

Evan Kirchheimer

Most firms do not view mobile devices, applications and services as assets

The last decade witnessed relatively little progress

Over a decade ago, mobile telephony entered the enterprise through the back door: employees who could afford mobile phones occasionally used them for business; specific business units budgeted for employee mobiles and then procured them locally; policies surrounding the usage of mobile phones for work were – where they existed at all – haphazard; there was little means of policy enforcement; and in no case were these mobile phones integrated into a business's fixed telephony strategy, let alone its IT strategy. This stands in sharp contrast to other office technologies, such as PCs, faxes, and copiers.

Fast forward to 2010, and the picture painted above still applies to a majority of businesses, large and small. In short, most companies do not manage their mobile estate as if it were an asset and, therefore, miss out not only on opportunities to save costs, but also on the benefits which a strategic approach to mobile management can bring about.

But we are on the cusp of a major change

However, Ovum believes that the status quo is about to change. This is due to three crucial developments.

- First, the current economic climate has created a business imperative. Mobile expenditure continues to rise in a corporate environment in which the CFO has been charged with scrutinising every cost line and finding savings;
- Second, suppliers are beginning to offer more comprehensive, more global managed mobility services, giving firms, for the first time, a real choice in how they approach managed mobility and procure the services they deem most important;
- Third, the perception of the handset as a device has changed. The increasing prevalence of smart phones as both consumer and enterprise tools is beginning to open CIO minds. More and more senior IT managers think of mobile devices as mini-computers, capable of providing remote employees with access to critical enterprise applications, not just messaging.

Ovum recommends that businesses seriously consider a managed approach

In this paper, Ovum will offer a short guide for enterprises as they establish and then continue to evolve their managed mobility strategies. We will investigate:

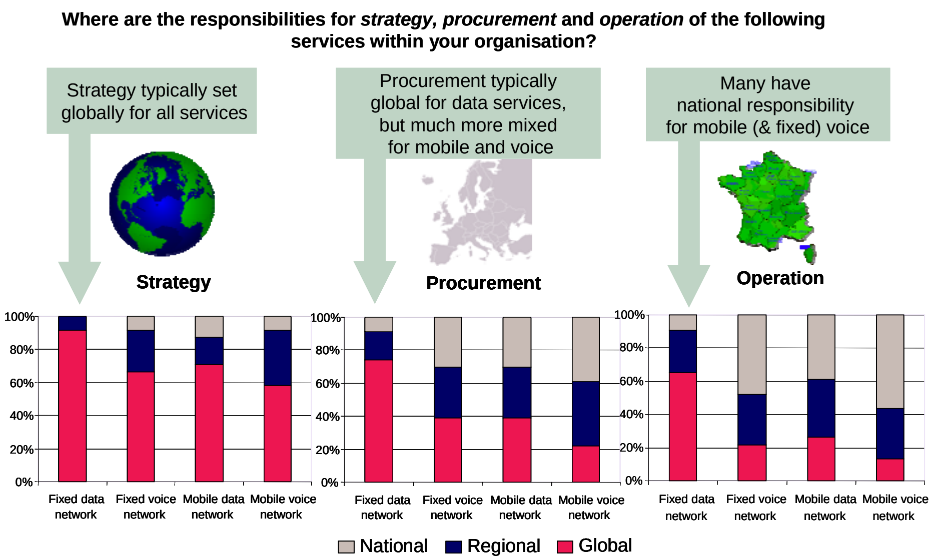
- the barriers to managing mobility and the potential benefits firms can realise from taking a more global, co-ordinated approach;
- the components of a complete managed mobility service, and which might create the most value for firms with differing requirements;
- how an enterprise can navigate the complex world of potential managed mobility partners, including specialists, systems integrators, and carriers;
- best practice with respect to how a business should manage an ongoing relationship with its mobility partners.

The first step? Think globally

A local, piecemeal approach has significant drawbacks

Because of the manner in which mobile phones began to enter businesses over a decade ago, mobile services are currently more likely to be bought and run at a national, or possibly regional, level. This is especially the case when viewed in comparison to more established services, such as fixed voice and data. The figure below shows that only one-fifth of multinational corporations (MNCs) procure mobile voice on a global basis and in the majority of MNCs responsibility for mobile voice remains at the national/local level.

Figure 1 **Local control of mobile procurement and operation**



Source: Ovum

Local procurement and responsibility, even within the scope of a global strategy, bring with them certain benefits (for example, local negotiators may have secured better tariffs than central procurement); but more often than not, they bring greater risk to the organisation as a whole.

The danger of local responsibility is that it exacerbates the challenges which corporates face when trying to rein in mobile expenditure, which is often the first priority of a company with respect to its mobile phone assets. But the risks extend beyond mere cost to a host of issues which, in the coming two years, will only grow more important in the minds of ICT directors and their board-level overseers.

Key risks include difficulty, if not inability, to:

- account for assets;
- establish, analyse and control costs;
- streamline procurement;
- roll out business-critical applications;
- integrate mobility into IT management;
- enforce policies;
- successfully manage a variety of carrier and supplier relationships.

Local control hinders mobile asset optimisation

In the world of IT, asset management and optimisation are well-established principles of good governance. This includes streamlined procurement, with most firms reducing the number of suppliers under management and introducing centralised sign-off , authorisation and budgeting for core IT assets.

This extends to the use of the technologies themselves: the huge interest and investment in virtualisation technologies stems from a desire to get the most out of existing assets in the given environment.

Without wishing to oversimplify what is indeed a highly complex exercise, the first step to optimisation is having a concrete understanding of the number of assets and where they are. In short, how can a firm get the most of its assets if it does not know what it has, where it is, and who manages it?

This is the situation that most firms face with respect to their mobile devices, many of which are now mini-computers in themselves, with the ability to reach into corporate applications and access innumerable web-services for both business and personal purposes. Local procurement and control of these assets, while not necessarily always, is more often than not a significant barrier to even the simplest asset audits, let alone the realisation of savings from streamlining procurement (which can result in major economies of scale).

Analysing and cutting costs is difficult when dealing with multiple local carriers

While the benefits of supporting a mobile workforce are well understood, the major driver for one element of managed mobility, expense management, is the need to control costs. Major expense management vendors have supplied information to Ovum which indicates that despite the recession and subsequent reduction in employee numbers, mobile telephony costs continue to increase. Our own research supports this contention. More than 40% of large multinational respondents to a recent Ovum survey stated that their data roaming costs have increased over 10% compared to last year, despite the worsening economy and, in many cases, shrinking payrolls. At the same time, one-third of the same set of respondents admitted they carried the cost of personal mobile usage by employees.

But cost analysis can be especially challenging because most multinationals and large corporates have contracted with more than ten carriers, support dozens of device models, and sometimes far more, to provide them with global mobile connectivity. Aside from the obvious point that a pan-regional or global approach is more likely to achieve more advantageous roaming tariffs, local control and responsibility also complicates the centre's ability to understand costs, analyse invoices for possible savings and detect major outliers which might call for corrective action and result in immediate savings.

Rolling out business-critical applications requires IT alignment

The increasing prevalence of smart phones in the enterprise provides businesses with an opportunity to extend critical enterprise applications to employees who work remotely for a variety of reasons. Such mobilisation of enterprise applications can range from the relatively well-established mobile field service and field sales applications to more niche applications such as fleet management and inventory control. Employees towards the top of the corporate food chain would likely benefit from remote access to management dashboards or exception alerts should critical corporate processes fail.

The successful implementation, roll out and continued management of an increasing number of enterprise applications on mobile devices implies that IT departments have a full and complete understanding of the device and application estate, including user profiles, location (with associated data costs), permissions, device operating systems, and last but not least – security. Employees importing their own business productivity applications on their smartphones may only raise the cost of application management for the enterprise, while at the same time having a deleterious impact on security. The dominance of the local over the pan-national or global makes the governance of a firm's application estate significantly more complex and time-consuming.

Local procurement makes integrating mobility into IT management a dim prospect

The more mobile phones run enterprise applications, connect to corporate networks over WiFi or another private or public network, and access company and customer data, the more they need to feature as a component of a formal IT management framework, be it ITIL, COBIT or a number of other industry-accepted protocols. As such, the mobile angle will increasingly feature in application development and maintenance cycles, upgrades and integration projects.

Local or piecemeal control of mobile assets, along with continued local power to procure new types of mobile devices which have not been centrally checked for compliance with existing applications or security policies, will hinder this evolution and put organisations at a disadvantage as they attempt to integrate mobility into their IT asset base and apply standard management frameworks.

Managing a host of locally-based supplier relationships can be time consuming

Enterprise mobility, especially for large firms, is complex, and mobility management is not, and likely will never be, a simple service. No single operator can provide global wireless coverage on its own, and no single supplier - whether an operator, specialist mobility technology firm or systems integrator - can yet provide all the pieces of a comprehensive managed mobility service (see *Figure 2* below for Ovum's definition of managed mobility). Supplier relationship management is therefore a critical service for any managed mobility provider.

Enterprises rarely measure the massive internal costs associated with local management of ten or more carrier contracts, local renegotiation of tariffs, and local device management. Large enterprises may be duplicating efforts in each operating country. While costs associated with local origination of contracts may not be easy to quantify, they are undoubtedly substantial.

A more centralised approach to co-ordinating carrier relationships will not only help reduce overall resource allocated to supplier management, but enable ICT management to focus on projects which deliver new functionalities and capabilities to the business. Indeed, in a recent Ovum study, over one-third of CIOs of major multinationals indicated that carrier contract management was one of the tasks they are most willing and keen to offload onto a managed mobility provider.

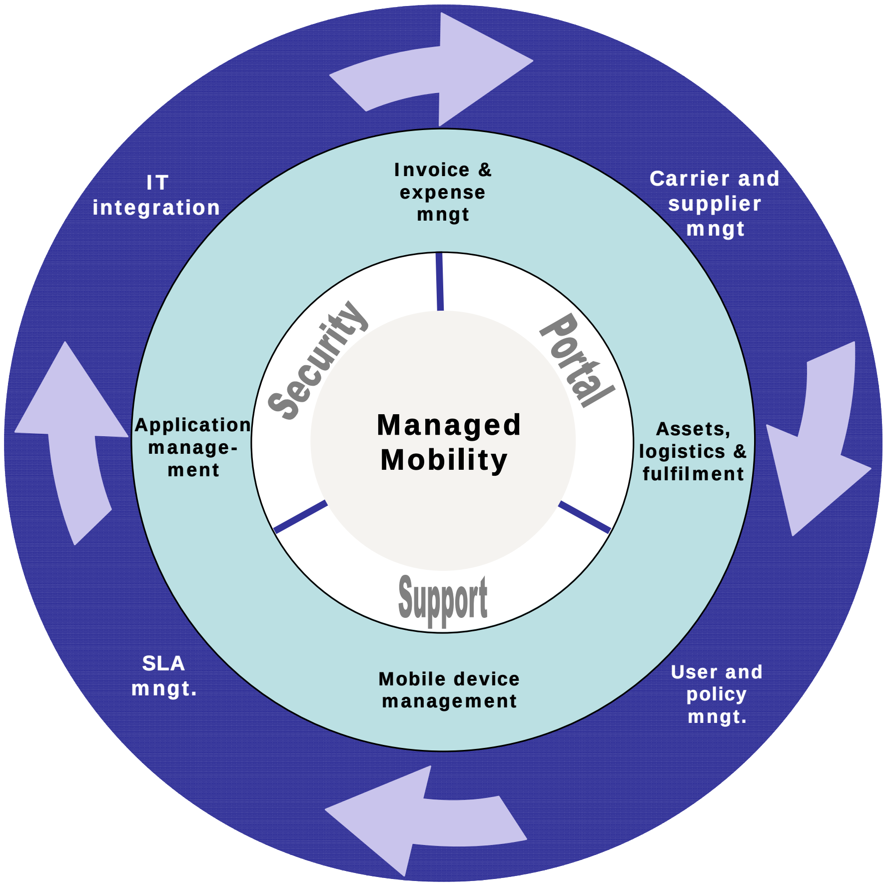
Understanding managed mobility services

The complete service cycle has only just emerged

Given the diverse and, in some cases, relatively new imperatives outlined above, it is not surprising that despite growing enterprise requirements, a comprehensive managed mobility service covering all enterprise needs has yet to emerge from a single provider. Ovum expects that throughout 2010, a variety of providers will build out ever-more comprehensive services, but that despite this, several years remain before businesses will be able to go to a 'one-stop shop' to meet all their mobility needs.

Nevertheless, a consensus on the shape and content of a comprehensive managed mobility service is emerging. The figure below outlines what Ovum believes are the essential components.

Figure 2 **The complete managed mobility service cycle**



Source: Ovum

At the centre sit the aspects of a managed mobility service which are shared by nearly all suppliers that claim to offer a solution:

1. Security. It is essential that suppliers offer guarantees that their solutions will adhere to IT security protocols and policies set within the enterprise. The proliferation of so-called smart phones, which run business applications could put corporate data at increased risk.

2. Support. While levels of support may vary for individual services or contract-by-contract, the underlying principle of any managed mobility service is that users will have access to a contractually defined, reasonable level of support from the service provider.

3. Portal. While not all managed services providers give their clients access to a service management portal, Ovum firmly believes that enterprises expect service management portal availability when contracting for mobile managed services. While portals could legitimately be viewed as an access

point for managing a service, Ovum has observed that operators that are developing managed mobility suites consider portals, more often than not, to be a service offer like any other. Many are investing huge sums (upwards of $13m in one case) in developing their own portal technologies.

Beyond these fundamentals, carriers and other suppliers currently offer a variety of managed mobility service components, with very few offering a full suite. This is reflective of enterprise demand: many businesses are simply not ready operationally, organisationally or culturally to adopt most of all of the managed mobility service cycle. However, Ovum believes the time is right for enterprises to give expense management and device management serious consideration.

Invoice and expense management is often the first step for many enterprises

A carrier or service provider may have developed its own invoice and expense management software, or may provide it through a white-label partnership with the likes of specialists such as Sybase or Ezwim, to name but two.

Key features which Ovum deems essential include:

- invoice analysis across multiple contracts in multiple countries;
- reports by organisation, geography, contract or class of employee;
- support for multiple user policies.

Some solutions allow for pro-active mining of billing data in order to help enterprises identify red flags, whether they be due to employee activity, operator mis-billing; some systems may even identify more advantageous tariffs.

Assets, logistics and fulfilment services are critical components

As with invoice and expense management, a managed mobility service provider may have its own logistics solution or may resell and support a partner’s. The aim of asset and logistics management is simple: deliver the right mobile device, in the agreed timeframe, to the right person. In addition, the service should track the order process and expose the status via a portal or other system.

Fundamental to this is an audit of assets and the development and roll out of a company-wide policy on which employees have the right to order phones, and which phones are available to which employee groups, be these limited by seniority, function or geography. A credible mobile asset management and logistics provider should offer this as a core component of its service.

Mobile device management services should support complexity

As enterprise adoption of smart phones increases, so does the need for device management. Central to this service is the enforcement of usage and security policies, ensuring critical or sensitive enterprise applications and the data associated with them are not compromised. But equally important is the ability to more easily roll out new applications which support the business's objectives.

It is this element of managed mobile services which is perhaps the first which goes beyond assessing and controlling a resource and into the territory of turning an enterprise's mobile estate into something which can itself allow for more efficient working practices and faster decision making. While the main driver for many enterprises to begin to consider a managed mobility solution is cost or risk control, the opportunity which mobile device management offers is potentially very large indeed.

Enterprises should ensure that potential mobile device management suppliers support all the devices used by the business and also have a convincing track record at:

- rolling out support for newly released devices on the market;
- delivering service and policy updates;
- installing applications;
- remotely activating or locking phones.

The need to be able to accomplish the above over the air (OTA) is essential: the cost of physically recalling devices to a local IT department or a central management point is high and such costs erode much of the value gained through a pan-regional or global managed approach.

Mobile application management must align to a firm's overall application strategy

Fixed applications can be a tether – this is especially true for employees whose roles are process-oriented but who are not desk-bound, or for field service and sales teams. There are still many organisations in which field sales team members must update their CRM system in the office or from a fixed VPN connection. Mobile application management should focus not just on application deployment, but also on the pro-active extension of new applications to mobile employees.

Several global operators have rolled out mobile enterprise application platforms, and Ovum expects these will be a catalyst for increased interest in mobile application development from enterprises. In line with device management, application management offers enterprises not just the ability to control access to existing applications on mobile handsets, but the opportunity to steadily increase the speed at which business-critical enterprise applications are manifested on mobile devices.

Enterprises should ensure that their mobile application management partner demonstrates a knowledge of the industry-specific applications the business is likely to need. Such an understanding will prove especially important for those businesses which have already rolled out industry-neutral applications (e.g., mobile sales force automation) and are now progressing to the industry-specific stage (e.g., insurance claims adjustment applications).

Service management is often overlooked, but essential

Managed mobility providers typically offer a host of professional services wrapped around the components of a managed mobility service described above. These are, in Ovum's view, essential parts of helping an enterprise extract as much value out of its mobile estate as possible.

This service management layer includes:

- Global carrier management. Managed mobility providers often act as the prime for securing mobile connectivity contracts with major carriers in each of the enterprise's operating geographies. They are usually able to strike advantageous tariff agreements given the volume of minutes or data likely to be channeled through multiple client relationships. Enterprise CIOs often report that the burden of negotiating and managing multiple contracts is something they would be more than keen to transfer to a partner.
- User and policy management. Many managed mobility providers often have a significant amount of expertise in terms of setting up mobile device usage policies and frameworks. They can use their experience in similar industries to help advise firms on issues such as which employees should be allowed access to which devices, how to deal with expensed mobile costs, and which applications should be available to whom and in what circumstances.
- SLA management. Service levels are at the center of any contractual relationship, not only between the enterprise and its managed mobility provider, but between the various carriers which have been contracted to supply access and the enterprise. Unless the enterprise employs a number of staff to actively check adherence to service level agreements across multiple contracts and for multiple types of service, it is often desirable to off-load this to a third party.
- Integration with IT. Many managed mobility providers have broader or IT-related capabilities. The integration of mobility with IT is, in most organisations, currently a remote prospect. However, Ovum does not believe this will remain the case: in the medium term, a number of enterprises will treat their mobile assets as they do their fixed IT assets and integrate them into IT governance frameworks. This means enterprise IT initiatives will no longer treat mobile as an appendage. A managed mobility supplier with IT services expertise could be an advantage in this environment.

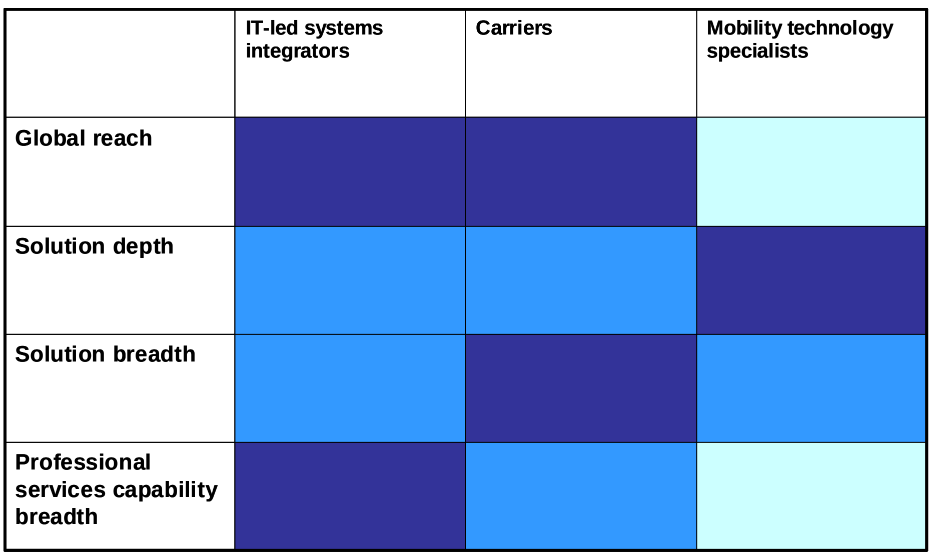
Navigate the supplier landscape

No single type of provider dominates

Given the evolving nature of managed mobility, the nascent state of the market, and suppliers that are continuously launching new managed services, it is no surprise that many enterprises are at a loss as to how to navigate a complex and changing managed mobility landscape.

The figure below is a generalisation of the relative strengths of different categories of players offering managed mobility solutions. The darker the colour, the stronger are providers in a given category, on average.

Figure 3 **No single type of supplier dominates**



Source: Ovum

Consider both single and multi-vendor options

There are a handful of carriers and IT-led systems integrators with broad and deep managed mobility services, but for the most part, portfolios are still taking shape and there are many major carriers and integrators without full service offerings. At the same time, many mobility services specialists provide best-in-class solutions in one or more of the areas an enterprise might prioritise. Good examples include mobile expense management and mobile device management. A business might simply not be ready to undertake a comprehensive approach to managing mobility; other IT priorities might preclude this.

Until the market matures, Ovum believes there are many valid reasons for enterprises to consider multiple partners for managing their mobility estate. In the long run, however, opting for one 'prime' supplier will yield the most benefits in terms of service rollout and management.

Systems integrators – an IT-led approach

Systems integrators (SIs) generally bring with them scale, blue-chip clients and significant capabilities in IT infrastructure management, applications management, and business process outsourcing. Combined with their ability to call on sub-contracting partners to deliver elements of the service, global SIs are in a prime position to help large enterprises develop a managed mobility strategy and roll out comprehensive services.

Enterprises that value co-ordinating their mobility management within a larger IT management framework may find that their trusted SI will deliver the best value managed mobility services.

Carriers – the access experts

Carriers with successful global services arms can be a match for SIs – especially in the field of infrastructure outsourcing (networks, data centers and mobile). In addition, they often have a level of practical experience with mobile networks that non-carriers simply can't match. Finally, due to their core access services, many carriers have relationships with partner carriers through which they are theoretically able to deliver preferential tariffs to their global enterprise customers. This background, however, does not always translate into expertise in domains such as applications and device management.

Enterprises with a strong relationship with a global carrier should investigate how that carrier addresses enterprise challenges regarding remote access, mobilising unified communications, extending enterprise applications to mobile devices and policy creation and enforcement. Even many leading global carriers are at significantly different stages of managed mobility services development: due diligence in evaluating the carrier whose services and roadmap map best to an enterprise's specific goals will be required.

Specialists – pros and cons

In less mature technology and services markets, specialists can offer capabilities which often leave the larger providers behind. Smaller, specialist managed mobility experts jockey for customers and mindshare in markets such as device management, mobile expense management, application development and application management. If an enterprise benefits from significant internal IT management resource with mobile competencies, and has complex needs in a domain such as mobile application management, a specialist may make sense. Indeed, at the other end of the spectrum, if a CIO has only been given the budget or mandate to focus on one key mobility headache, a specialist may provide exactly what is required.

In the long run, though, an enterprise which opts for a specialist approach will need to keep an eye on how its chosen provider is broadening its offer to support its customers' emerging requirements, or whether the specialist's partner relationships are robust enough to deliver against a potential future set of more complex requirements.

Translate your needs into supplier selection

Ovum cannot formulate a hard-and-fast set of rules for selecting a managed mobility partner: enterprises are all distinct and have unique sets of requirements; in the case of managed mobility, the supplier landscape is largely immature and, as a consequence, changes month-by-month.

In selecting a partner for managed mobility, Ovum therefore recommends enterprises ask themselves the following questions:

- How broad are your requirements? If your primary focus is on cost control and mobilising applications is not a short or medium-term priority, a specialist may be the right option. In contrast, if your business has moved beyond controlling costs being the only priority, how well do your potential supplier's capabilities match your requirements?
- How great is your global professional services need? Do you have working policies in place, or do you require guidance with respect to setting up a framework for ongoing management of employee mobile device usage?
- Are senior members of your IT staff bogged down negotiating multiple carrier contracts? Are efforts duplicated in each operating geography? Which is a higher priority from your supplier – technology expertise or service management credentials?
- Do you have existing relationships with carriers or systems integrators which have delivered significant savings and value, and do these current partners have managed mobility capabilities?

Manage the ongoing relationship

Once an enterprise selects a managed mobility partner, it should focus on successful management of an ongoing relationship. This sounds simple, but in fact can prove more difficult than many firms expect.

The mobile industry has traditionally offered few service guarantees to enterprises beyond the availability of the mobile network and billing timeliness. If a more complex problem arises, the enterprise has generally not had remedial options.

Now that providers from different backgrounds are beginning to offer pan-regional managed mobility services, and an increasing number of businesses are buying them, new commercial principles are required in order to safeguard a standard for the management task being handed to the service provider.

Ovum believes enterprises should focus on two core areas to ensure quality of service.

1. Accepted IT governance frameworks, such as ITIL. While systems integrators are skilled ITIL practitioners, a number of operators are re-orientating their businesses and are introducing new service performance measures by widely adopting ITIL, which clearly defines the service management discipline and details best practice problem and incident management. ITIL also introduces a common language between supplier and customer, giving rise to opportunities to mutually formulate new service performance measures.

2. SLAs. While typical incident resolution times in the mobile industry currently stand at the eight hour mark, in the fixed services sector response times are often 5-30 minutes and resolution times of 2-4 hours are the norm. Enterprises should therefore look to improve on the standardised SLA frameworks now available from managed mobility providers and evolve a service framework which includes penalties that account for incident resolution, the impact of service failure, and the frequency of failure.

Enterprises are coming to grips with their mobile assets and bringing them under control. Businesses increasingly view their mobile devices and applications as strategic assets through which business productivity and business process can be improved. The more that these same businesses view managed mobility as a strategic service, the more they will gain from mutually beneficial relationships with their chosen service providers.