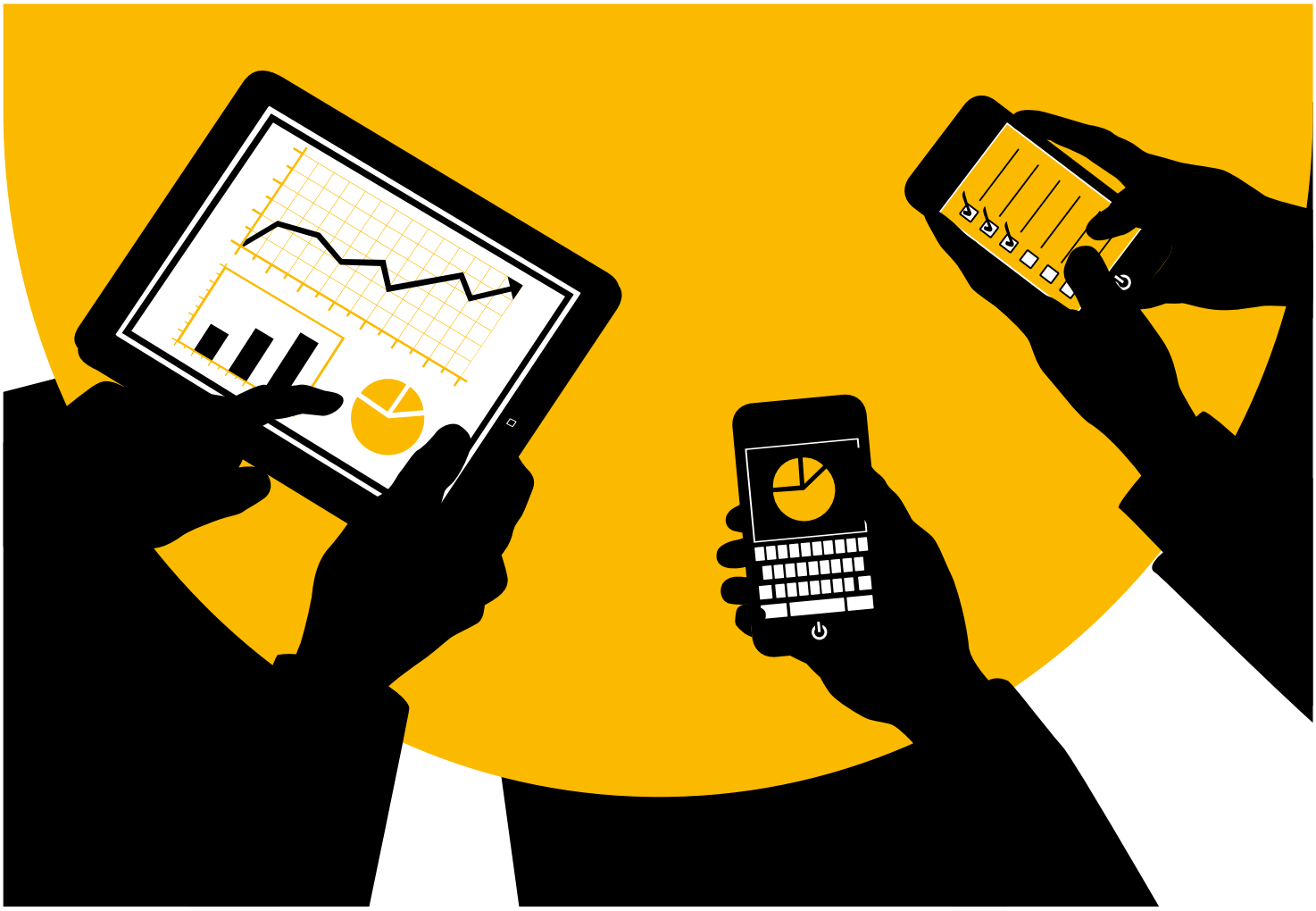
SAP White Paper
SAP Partner Organization

Mobile Device Management

Managing Mobile Devices in a Device-Agnostic World

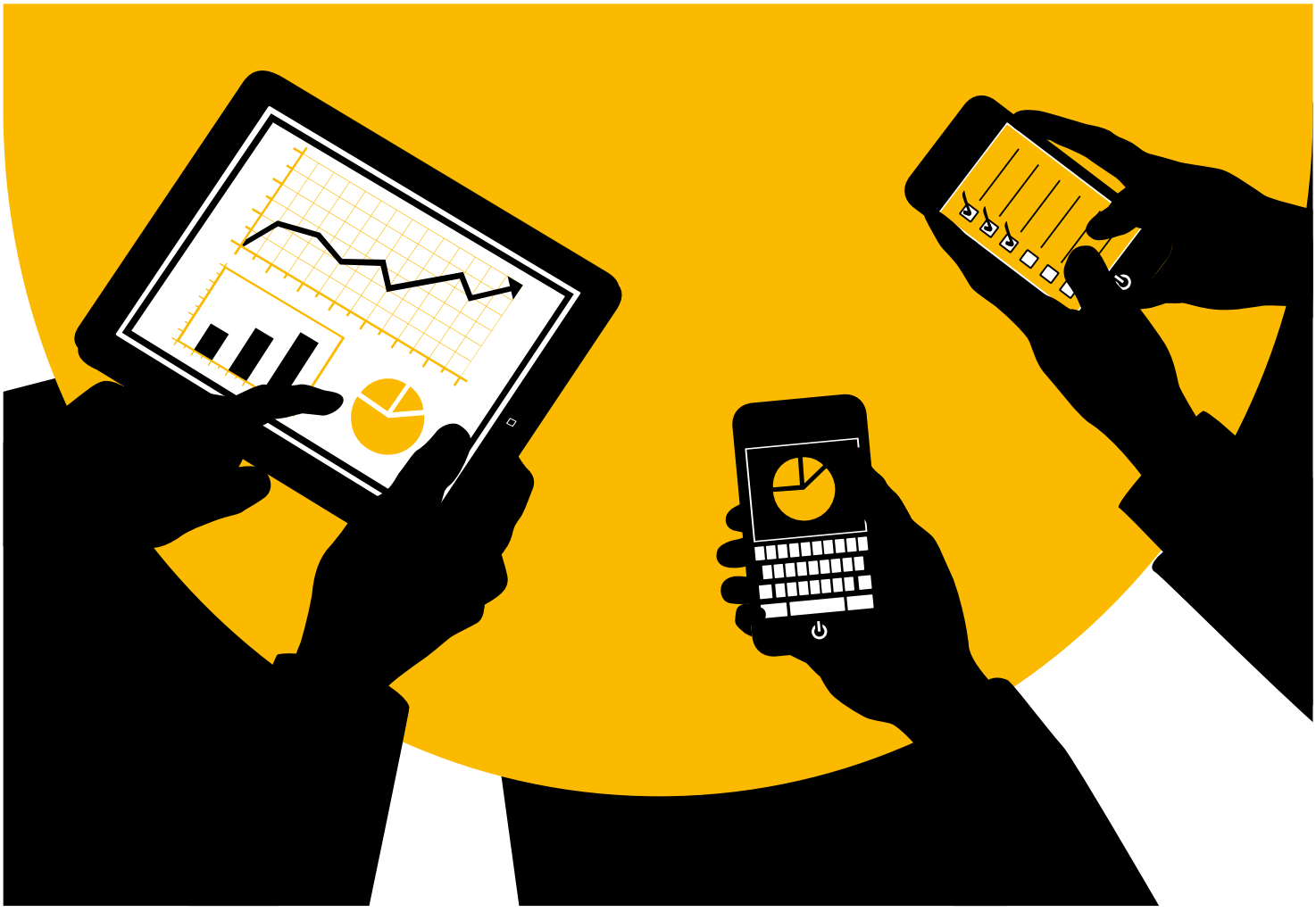
Finding and Enforcing a Policy That Makes Business Sense



The Best-Run Businesses Run SAP™

Table of Content

As the “bring your own device” (BYOD) trend sweeps across the business world, it raises a huge management challenge for many companies. It changes who within an organization gets access to mobility. It also affects the way a business operates, with implications that go far beyond simply IT. BYOD presents new, fundamental questions about security, liability, and cost. Answers depend on two aspects of mobility management: device management policy and the technology used to fulfill and enforce a policy.



Mobile Device Management 2.0

Mobile device management used to mean something.

Corporate IT reviewed and selected mobile devices for employees. Companies decided who should get devices and how they would be used. IT managers configured the devices, issued them to employees, tracked them, and decommissioned them.

Mobile device management was simpler in those days. It seems like just yesterday. In fact, for many companies, it **was** just yesterday. But things are changing fast in business mobility, and one of the greatest areas of change is how workers go mobile.

As soon as people figured out how to do e-mail on their iPhones and Androids, personally owned devices started popping up all over the workplace. Before long, employees were pushing for other kinds of business applications, downloading apps from app stores, and buying out-of-the-box business solutions. Then tablets started showing up. According to Strategy Analytics, the number of business tablets will grow to 56.2 million in 2015 from 30 million in 2011. The percentage of those that are corporate liable will more than double to 20% in 2015, up from 8% in 2011.

This "bring your own device" (BYOD) trend can have big advantages. Some companies are experimenting with providing employees a budget and allowing them to buy the devices and service plans of their choice, which can result in cost savings.

However, BYOD presents a big management challenge for many companies. It changes who within an organization gets access to mobility and how they get it. It also affects the way a business operates, and it has implications that go way beyond the IT department. BYOD raises new questions such as:

- How do you enforce security in a BYOD environment?
- How do you know who's mobile and what they are doing on their mobile devices?
- Is the company liable for what employees do on personal devices that they use for work?
- Is there a practical limit to how many devices a company can support, and what does it cost to manage a great diversity of devices?
- Can one device actually support both personal and corporate needs?

These are fundamentally significant questions. They are also questions that have different answers for different organizations. Finding the answers and acting on them depends on two pieces of the mobility management equation: device management policy and the technology you use to fulfill and enforce that policy. Let's first look at device management policy.

Building a Mobile Device Management Policy That Makes Business Sense

You don't have to look far to find plenty of good mobility management guidance (see *The Enterprise Mobility Policy Guidebook* published in May 2011 by the Enterprise Mobility Foundation). This guidance typically suggests policies that support essential mobility management tasks like asset inventory and management, expense management, security, operations management, and tech support.

Rather than replicate that device management advice here, we will take a business-value approach to developing a mobile device management policy.

The value of a mobile device management framework is directly related to how effectively it serves your business mobility objectives. So what are your business mobility objectives? Most organizations would agree that by mobilizing certain business operations, they hope to realize the following benefits:

- Make business operations more efficient
- Make workers more productive
- Keep company information assets secure
- Control costs of mobile IT

Let's begin by breaking down mobile device management policies according to the business objectives they are intended to serve. The challenge in creating a mobile device management strategy for any organization is balancing operational benefits with risks and cost. Some policy objectives may conflict with others. To have a successful mobile strategy, every organization needs to find the right balance.

POLICIES THAT HELP MAKE BUSINESS OPERATIONS MORE EFFICIENT

One of the greatest benefits of mobility is that it enables real-time access to people and information. This accelerates business activity, improves the quality and accuracy of decision making, and enables a more collaborative business process. Collaborative access to information and people is only possible if the business environment is "transparent" to everyone in it.

Note that transparency does not mean everyone has equal access to all information and all other people. It means there are not arbitrary technical barriers that prevent this kind of access. Collaboration and access need to be governed by business process needs, workflows, and security. They should not be arbitrarily restricted by technology-induced business process silos.

The following table shows what kinds of mobile device management policies help ensure mobile transparency that is manageable and flexible enough to change with business over time.

The value of a mobile device management framework is directly related to how effectively it serves your business mobility objectives.

Policy Objectives	Policy Rules
Policies that help ensure the greatest acceptance, and therefore penetration, of mobility use in the enterprise	Whether mobile devices used at work are owned by the employee or company, policies should permit a wide choice in device types and carriers. Some tips are: • The more prescriptive you make your list of acceptable devices, the more resources you will use managing the list. • Some job roles and work functions will require different device types than others. • Support dual-use (personal and work) devices. This bring-your-own-device approach has economic and user productivity advantages.
Policies that help ensure the portability of data and applications	Require that internally developed mobile applications, including hybrid Web applications, be built on a common mobile enterprise application platform (MEAP). This simplifies porting applications to different devices, and it helps ensure data compatibility between applications and devices, thus avoiding isolated "silos" of mobile business activity. One tip is to mandate that third-party contractors who develop mobile applications for you leverage your MEAP platform.
Policies that limit the use of third-party mobile apps that rely on proprietary data sets incompatible with existing corporate databases	Mobile operations often begin as extensions of conventional operations. Rules should encourage the extension of existing data to mobile devices rather than adopting new applications with new data form factors to fulfill mobility needs. This helps ensure data compatibility between mobile and conventional operations. Some tips are: • Employees can be the best source of information about new third-party applications. Establish a process whereby employees submit "free" or commercial third-party mobile apps for business use review. • Prohibit downloads of unapproved business applications.

One of the greatest benefits of mobility is that it enables real-time access to people and information. This accelerates business activity, improves the quality and accuracy of decision making, and enables a more collaborative business process.

POLICIES THAT MAKE WORKERS MORE PRODUCTIVE

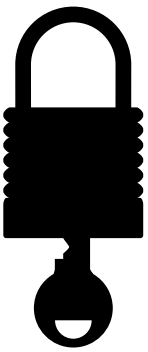
More efficient business operations go hand in hand with more productive workers. It is not difficult to see why workers become more productive when they use their time more effectively. Mobility allows them to communicate and find information more quickly, answer e-mail and perform workflow tasks on the run, and generally accomplish more in smaller time bites. People know this, which is a major reason why up until now the driving force behind enterprise mobility has been the employees themselves.

The following table shows how mobile device management policies maximize worker productivity.

Note that many device management policies relate to managing the applications that users run on their devices. For more information about mobile application management, see the SAP white paper *Mobile Applications May Be Running the Business, But Who's Running the Apps?*

Policy Objective	Policy Rules
Policies that help ensure workers use mobility to their greatest professional advantage	Workers are inventive when it comes to finding better ways to do their work. Mobile device management rules can encourage productive use of business mobility in these ways: • Rules allowing employees to choose the devices they want, or to bring their own devices to work, result in higher levels of employee adoption and use. • Rules that enable employees to participate in mobile application acquisition and development result in higher levels of employee engagement. • Initiatives to mobilize business workflows that enable "anytime" work make workers more productive.

The principal objective of mobile policies should be to establish mobility as a secure, cost-effective business enabler in an organization.



POLICIES THAT KEEP COMPANY INFORMATION ASSETS SECURE

Some IT managers worry that policies encouraging wide use of mobility in the enterprise are a threat to information security. They have plenty of reason for concern. Consumers' phones are lost or stolen. Companies may be lax in their implementation of mobile security. Even when there are security policies in place, employees may be unaware of them.

One approach to mobile security is to limit risk by limiting mobility in the company. From a security perspective, that works. However, this strategy also puts the company at a massive competitive disadvantage, and in the long run it could actually drive the company out of business. Companies that turn their backs on mobility are not realizing the operational efficiencies and worker productivity gains that are achieved by more mobile organizations (including their competition).

A better approach is to effectively implement a mobile security policy. The following table shows what kinds of policies will keep corporate information assets secure without stifling capabilities that make workers more productive and business operations more efficient.

The key to implementing and enforcing security policies is an enterprise-grade mobile device management platform. We'll talk more about platform capabilities below. For a more detailed discussion of developing and implementing a mobile security strategy, see the SAP white paper *Mobility Advantage: Why Secure Your Mobile Devices?*

Policy Objectives	Policy Rules
Policies that protect data	• Require encryption of all business-related data (both transmitted and stored). • Implement a mobile device management platform that enables you to remotely lock and wipe devices, and remotely monitor data activity for purposes of breach detection. • In dual-use devices, use application and device management to segregate business and personal use functions on the devices.
Policies that manage access	• Require password authentication before users can launch business applications. • Use mobile application functionality to manage data access, and use group policies to manage which devices and job roles are able to run which applications.
Policies that sustain a culture of security best practices in a business ecosystem	• Develop a lifecycle or service-cycle strategy that includes a process to enable a device for business use. • The "enablement" process should include standard steps like encrypting data, setting a password, and installing antivirus and antimalware software. • Require immediate reporting of a lost or stolen device. • Promote safe mobility practices.

POLICIES THAT CONTROL MOBILE IT COSTS

When people think of the costs of mobility, they often think of direct costs of devices, service plans, data plans, and exceptional charges that traveling workers might incur.

Beyond these direct costs, there are many indirect – or let us say "less-visible" – costs associated with business mobility. These less-visible costs can be far greater than the direct costs. Less-visible mobility costs include:

- **Costs associated with the mobility infrastructure** – These are costs of systems needed to manage devices and security and to provide back-end support for proprietary mobile business applications and data access.
- **Mobile application development and management** – Costs associated with building, acquiring, customizing, distributing, and maintaining mobile applications can be significant. If your company has BYOD policies that include supporting multiple device types, this can have a huge multiplier effect on the costs of application development and support. As companies become more mobile over time, they will be supporting ever larger numbers of mobile applications. Costs associated with mobile application management (MAM) can vary tremendously depending on how you implement a MAM strategy.

One way to limit mobility costs is to standardize around one device type and a standard rate plan. This approach limits the benefits of mobility in these ways:

- Employees are less likely to use the company-issued device for anything more than bare necessities.
- In this world of rapidly changing mobile technology, companies will be stuck with old technology and will find themselves at a disadvantage compared to their more mobile competitors.

The reality is that there are more mobile devices coming to market and more ways to adapt them to different aspects of the business process, and more companies are shifting to BYOD policies for knowledge workers. As companies develop policies to control mobility costs, they will need to support a variety of devices. The following table shows policies that work to control costs in such a dynamic mobility environment.

A large part of developing mobile management policies suitable for any operation is balancing potential policy conflicts. For instance, a highly restrictive mobile device policy may be easier to secure, but it will take a toll on worker productivity. In fact, there is no one right set of policies. Different organizations with different security and operational constraints will have vastly different mobile policies.

The principal objective of mobile policies should be to establish mobility as a secure, cost-effective business enabler in an organization. However, developing mobile policies is only one part of the equation. The other is implementing and enforcing those policies.

The heart of any mobile device management policy enforcement is a mobile device management platform. What exactly is that?

Policy Objectives	Policy Rules
Policies that regulate direct costs	• Establish an approved list of carriers. • Define permitted rate plans that are appropriate for different job functions (some employees may have larger data requirements than others). • Define rules for plans and plan adjustments that cover the needs of international travelers; define rules of usage when traveling internationally. • Define rules around allowances and expense reimbursements.
Policies that reduce less-visible costs	• Adopt a device and application management platform with a common set of management tools for all applications and devices. Investing in an enterprise-grade platform vastly reduces long-term costs of managing a dynamic device and application portfolio. • Develop a lifecycle or service-cycle approach to device management that includes a process to enable a device for business use. • Adopt an application development platform standard that enables all business applications to share common back-end data. • Use a hybrid Web-app strategy to reduce the cost of developing and maintaining custom business applications.

Implementing Policy

Whether you are relying on a service provider to manage your corporate mobility or you are building in-house IT infrastructure to do this, effective mobile management depends on a mobile device management platform. Why?

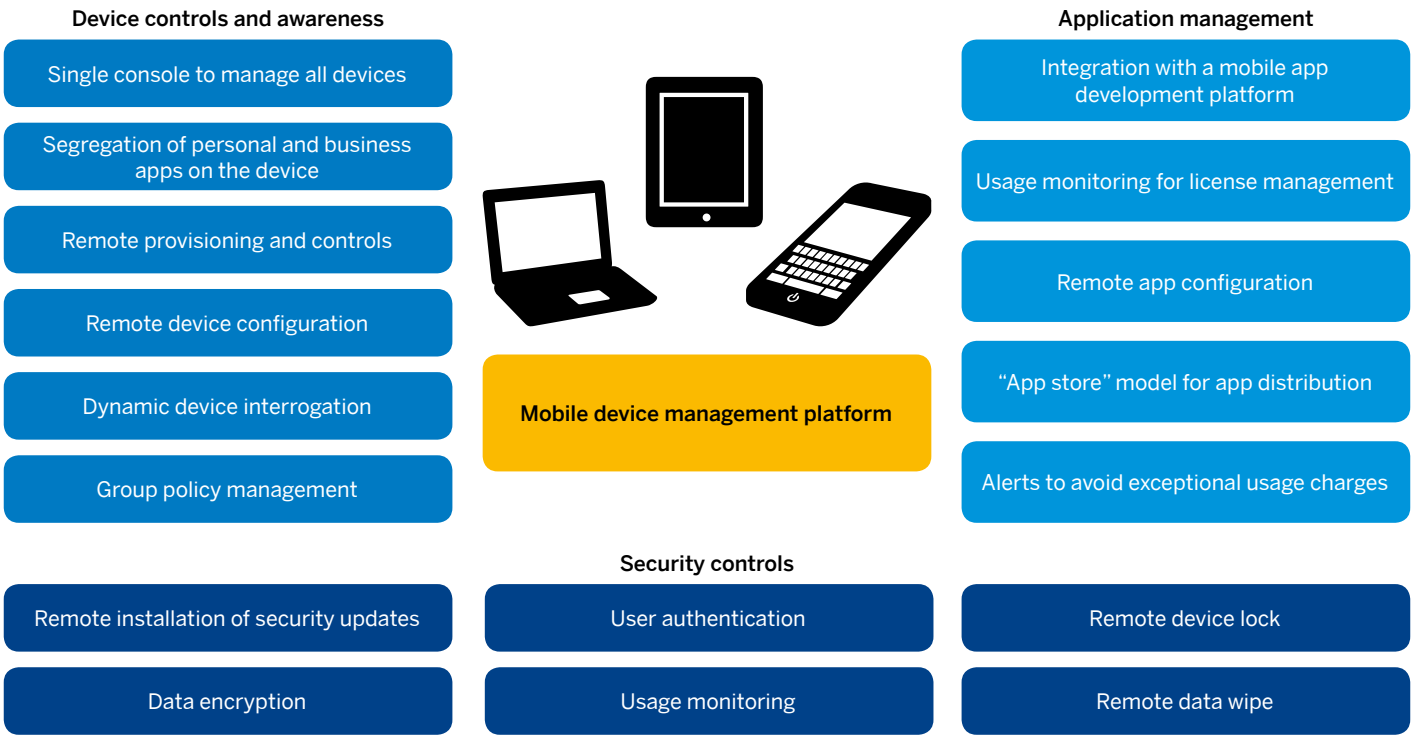
A platform provides essential controls that mobility managers need to enforce policy. It is the combination of mobile policy and a robust device management platform that enables an organization to build a mobile business strategy.

The figure shows essential capabilities of an enterprise-grade mobile device management platform. These include:

- **Compatibility with the widest selection of device types and mobile operating systems** – This is critical because it enables an organization to support the most up-to-date mobile devices. It also gives an organization greater flexibility when creating a BYOD policy for employees.
- **Remote provisioning and control** – This enables managers to remotely configure devices, and it provides remote and automated security controls used to secure data on lost, stolen, or decommissioned devices. It also enables companies to push applications to remote devices over the phone service network.
- **Dynamic device interrogation** – This gives real-time visibility into mobile systems, providing information like device types, version of operating system a device is running, software licenses in use, and other essential information about mobile systems.
- **Group policy management** – A mobile device management platform should support remote device control based on group policies. For instance, you might want to distribute three different versions of an application: one for all iPad users, one for all Android phone users, and one for all BlackBerry users. Or you might want to distribute a particular application or software update just to account managers.

Using these mobile device management platform capabilities to enforce mobile policies enables organizations to manage mobility in a strategic way, much like they already manage other IT assets. Let's see how policy and platform combine to produce an operational mobility management strategy.

Figure: Essential Mobile Device Management Capabilities



Service-Cycle Approach to Device Management

One approach to mobile management is to enforce policies in the context of a device's lifecycle or service cycle. A service cycle is the period of time when a device is in active service with the company.

A service-cycle approach to device management breaks down into three phases:

- **Provisioning phase** – This is the process of preparing a device for use in the business environment by installing essential security and business applications, segregating business and personal use functions if this is an employee-owned device, and performing initial security and user configuration.
- **Production phase** – During the production phase, a device is being actively used for work purposes. Applications will be installed or updated during this time, and companies will remotely monitor device activity to detect security breaches or violations of use policies. In addition to normal flows of business data to and from devices, workers may receive operational messages and alerts. For instance, a user might receive notification of data usage that exceeds the data plan for that device. IT managers will use group policies to automate some device management tasks.
- **Decommissioning phase** – When a device comes to the end of its service life (either naturally or by being lost or stolen), it will go through a decommissioning process that removes all business applications and data. A device management platform enables IT management to perform decommissioning functions over the air when they do not have physical possession of a device.

With a device management platform in place and a comprehensive set of mobile policies, it becomes possible to build and enforce a service-cycle management strategy.

Whether you are relying on a service provider to manage your corporate mobility or you are building in-house IT infrastructure to do this, effective mobile management depends on a mobile device management platform.

Preparing for a New Age of Mobile Device Management

For many organizations, mobility today means managing and enabling workers who use smartphones at work. However, mobile technology is moving very quickly.

It's widely accepted that most workforces will support tablets in the next few years. These workers will not be throwing away their smartphones. This means that in the near future, typical knowledge workers will be equipped with two mobile devices, each with its own device and application management requirements. Many organizations already support multiple mobile devices for their workers.

As mobile technology evolves and companies mobilize more of their operations, the greatest business advantage will go to organizations that most effectively manage their business mobility. This means:

- Establishing mobile policies that make business operations more efficient, make workers more productive, keep company information assets secure, and effectively control mobile IT costs
- Implementing a device and application management platform that is capable of managing and enforcing mobile policies for all devices in the organization

Companies that have the best mobile implementations will be the ones that win in a world of real-time business engagement.

LEARN MORE

For more information about developing and managing mobile applications that are core to your business operations, contact your local SAP partner.

As mobile technology evolves and companies mobilize more of their operations, the greatest business advantage will go to organizations that most effectively manage their business mobility.

The Best-Run Businesses Run SAP™

CMP25543 (13/03)