SAMSUNG

White Paper:

Planning a Choose Your Own Device (CYOD) Program: 8 Steps to Success

8 Steps to Success

Mobility is a key to growth and success for every industry in today's markets. Businesses of all types want to reach out to their customers: in person, online, whatever it takes to make the connection.

Having a workforce empowered to work anywhere and anytime they want is becoming a basic requirement as organizations move away from traditional work models.

As mobile devices move from "nice to have" to "strategic infrastructure," informal approaches to managing employee smartphones, tablets, laptops and wearables should be revisited. Organizational control doesn't have to be heavy-handed, but ensuring core device management, application interoperability and security of confidential information requires more than a "no policy" free-for-all.

Organizations seeking an empowered mobile workforce have many moving parts to coordinate: strategic planning, application development and security, policy creation, device procurement and deployment, user support, and operational management. It all seems complex — and, without the right plan, it can be. But, like all big tasks, breaking things down into manageable steps and attacking each step one at a time is critical for success.

So, what are the key steps to a successful mobile program? This white paper offers an eight-step model based on 20 years of working with enterprises around the world on their mobility and network security projects. Although every organization is different and will follow their own path, these eight core steps can make the process of designing and rolling out a mobility program more straightforward and help increase the benefits for your organization.

Acronym soup: BYOD, CYOD and COPE

Anyone researching enterprise mobility will quickly run into terms like BYOD, CYOD, COPE and many others. Unfortunately, there is little agreement on what each acronym exactly means in terms of important elements of mobile device deployment: device ownership and connectivity costs, device choice, control, security and support. In the long run, it doesn't matter what term you use to describe your program as long as you're clear what it means to you, your users and your organization.

The table on page 3 provides some common definitions, but feel free to adjust them to meet your own needs.

D	E	R	S	N	N	B	H	Y
T	U	M	I	A	I	G	U	R
G	A	N	K	T	H	D	C	I
O	B	Y	O	D	K	L	Y	W
N	P	S	F	H	O	E	O	D
A	N	O	I	U	J	E	D	T
R	O	U	Q	Z	B	S	A	R
S	P	T	C	O	P	E	Z	O
Z	C	B	R	K	X	N	B	S

	No Mobility Policy	Bring Your Own Device (BYOD)	Choose Your Own Device (CYOD)	Company Owned/ Personally Enabled (COPE)
Who pays for the device and service plan?	The user	The user, often with an Employee Purchase Program available for discounts	Often split between user and company	The company pays
Who gets to pick the device?	The user	Usually the user, within some limits	The company provides a short list of options; the user chooses	The company chooses or provides a short list of options
Who controls the device?	The user	Mostly the user, but some company requirements exist	Mostly the company via Mobile Device Management (MDM) tools	The company controls almost every aspect via MDM
Who is responsible for support?	The user	Mostly the user	Usually split between user and company	Company is responsible for most support
What corporate apps are available?	None officially	Common business collaboration tools, including Email, Calendar, Contacts and conferencing	Common collaboration tools, plus Line of Business apps and HR/Financial applications	Common collaboration tools, plus Line of Business apps and HR/Financial applications
Can the device connect to the corporate network internally?	No access (we hope)	Limited access	Usually yes	Usually yes
Can the user run personal applications?	Yes	Yes	Usually yes, but often in a separate profile/container	Usually yes, but often in a separate profile/container

Step 1: Get Executive Buy-In

Mobility usually falls to the IT group to implement, and IT may even handle the logistics of driving the development of policy and strategy — but the real direction has to come from the top of the organization.

No matter how aggressively IT approaches a CYOD mobility program, the buy-in has to start from the top of the organization with the C-suite and Line-of-Business (LoB) managers. Inevitably, any mobility program will have conflicts in timing and resource allocation, and the best way to resolve them is by having a clear agreement within the organization's management team on strategy, investments, priorities and metrics for measuring success.

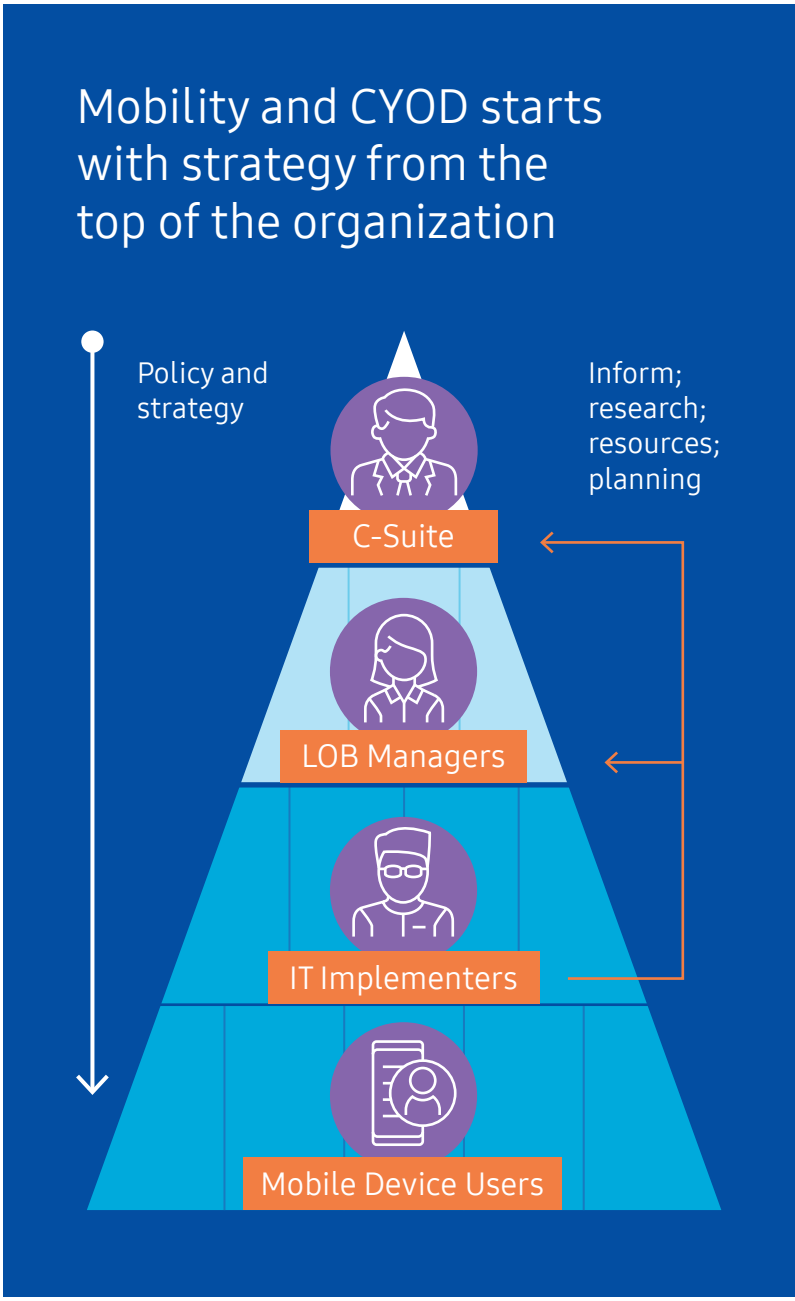
Mobility strategy may have to come from the top, but that doesn't mean that IT teams don't have a significant role. In fact, because of the level of technical knowledge needed, IT should be involved from the beginning. That can be as simple as making sure that the CIO is an integral part of the planning team, or you may want to have a dedicated IT mobility expert at the table to both provide a reality check — and to let the decision makers know about the latest developments in mobile technology. For many organizations, CYOD mobility starts with thinking "outside of the box," and having an idea of what is and is not possible helps frame the discussions clearly and ensures a usable and achievable strategy.

Staffing and Resourcing for Mobility Programs

IT teams also need to be involved to properly estimate startup investment costs and continuing resource requirements. Many organizations run close to capacity, especially in areas such as IT staffing, which may mean that outside help will be needed for initial deployment or even ongoing support.

Mobility-as-a-Service (MaaS) providers, a new niche business, can help both at the strategic and operational levels. If you run into resource constraints during deployment, you can bring in MaaS providers to increase capacity quickly and flexibly.

For larger organizations, it's also helpful to get other implementing groups involved early on, including Purchasing, HR, and Legal. This is especially true in environments which are highly regulated or have strong compliance requirements (such as financial services or healthcare), or where there's an international component.



Step 2: Develop the Mobility Strategy

Moving from "no mobile policy" or a basic BYOD environment to CYOD or COPE usually means that mobility is important to the organization. And it means that the cross-functional team from Step 1 needs to develop an enterprise mobility strategy.

CYOD and COPE programs cost money: it's not just devices, but also the cellular connectivity, software, services, continuing support and replacement costs. No matter how large or small the organization is, an enterprise mobility strategy starts by answering one key question: "What do we want to accomplish by making this investment in mobility?"

From that answer — without going into too much detail — the strategy should also cover the major elements of the mobility program. Details come later, and from other groups. But implementers need to know what the strategy is before they can bring their expertise to bear on the problem and start to drive solutions into the organization.

A comprehensive strategy document doesn't have to be too long. Depending on the size and complexity of the organization, it could be anywhere from five to fifty pages in length. In some cases, it's appropriate to have little more than a sketch of the big picture. In that way, the details can be filled in by other groups or be left for refinement by implementers.

Mapping Your Mobility Strategy:

Here are some of the key questions to gain alignment on before handing over your mobility strategy to operational groups for implementation:

What are our goals?

A list of goals that specifically require mobility helps to frame everything else. Think about answering the question: "How is mobility going to change this organization in a way that generates a positive Return on Investment?"

Mobility Denial

Although mobile devices have been utilized in the workforce for nearly 20 years, there are still a small percentage of organizations in self-denial about mobility. These are the ones where there's no policy, no strategy and no resources allocated to mobility. In these organizations, employees are connecting their smartphones to enterprise collaboration applications like Exchange by taking an IT person to lunch and asking for the names of the various servers to fill in the email profile on their smartphone.

Mobility denial marches together with security problems and lost opportunity costs. For IT staff or internal advocates trying to advance a mobility agenda, bringing up security can be a two-edged sword. Yes, upper management can use the threat of lost devices, exposed confidential data and stolen directories as a spur to investigate the power and benefits of better integration of mobile devices. But they can just as easily demand that the limited mobility be shut off — and this threat is why some organizations float by, insecure and willfully ignorant of the risks.

Missed opportunity costs are a more difficult argument to make but are ultimately more effective. Even the most stalwart holdout on the benefits of mobility will have experienced the effects at some level recently. Mobility advocates trying to evangelize within their organization can use personal anecdotes and, even better, information about mobility-enabled competitors, to make the case for a structured mobility strategy.

What data access is needed? What processes must change?

Mobility usually means more than taking old applications and putting them onto smaller screens; it means re-visiting the way many business processes work and optimizing them for a more mobile workforce. This will require changes in process, obviously, but it may also drive changes in data access rules. To write this section, consider what do people — staff and non-staff — have to do differently than they do today? And what data do they need to do it?

What application development is going to be required?

Often, a comprehensive mobility project includes new apps or application harmonization. Strategy doesn't have to get into the details, but it's important to at least inventory the critical applications that need to be mobile-enabled or developed to meet the goals. In some cases, existing web-based applications may just need to be touched up or have new middleware inserted to make them mobile friendly. In others, starting from scratch with a new app or a new approach, such as migrating the app to a cloud/SaaS environment, will be the best way to gain traction. Laying these things out in broad strokes will get everyone on the same page regarding priorities and resource requirements.

What's the path to mobile enablement?

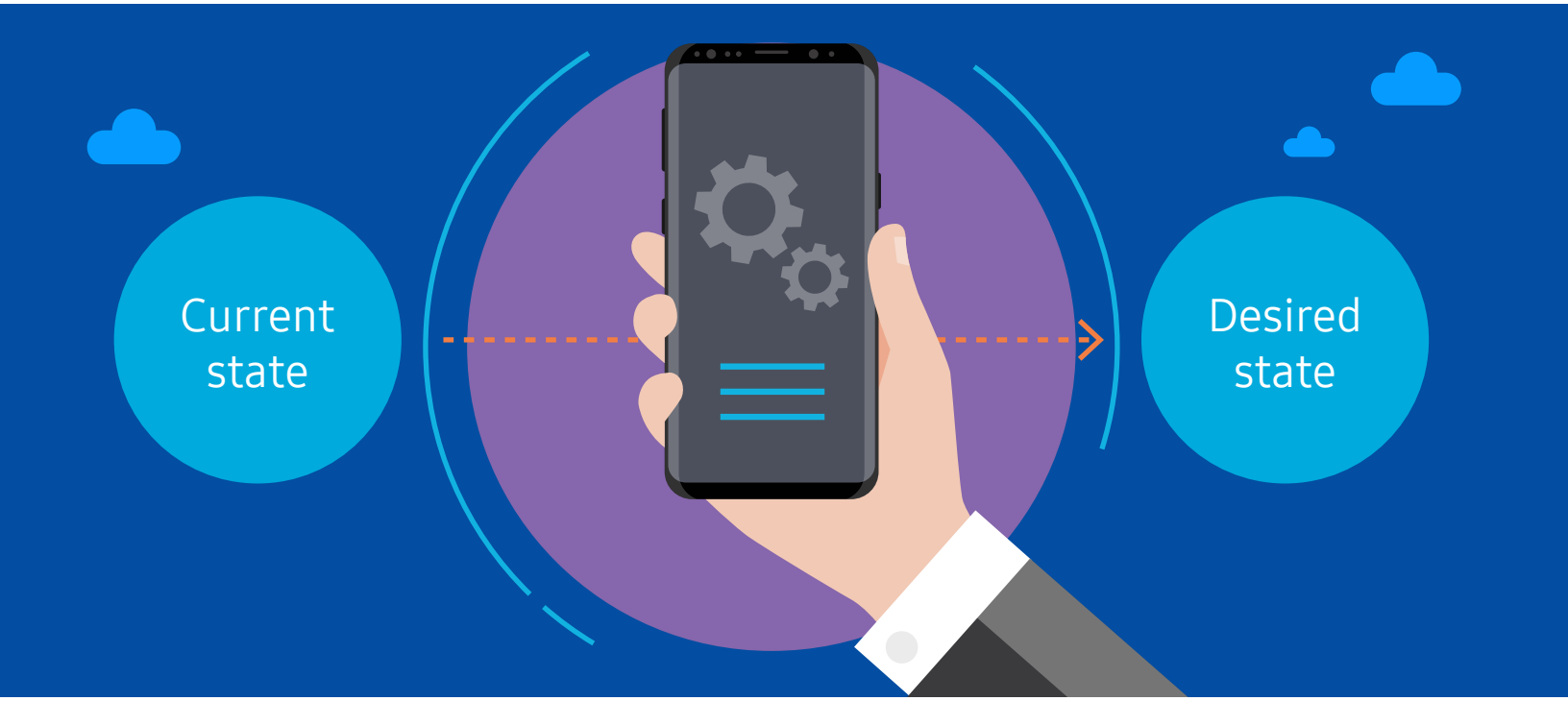
With goals, processes and apps all identified, a strategy document can set the tone and pace by showing the path from "current state" to "desired state." Again, details don't belong in a strategy document, but having agreement on what comes first and how applications infrastructure needs to change makes everything else clearer. Obviously, at some point, it all has to drive the procurement and deployment of devices, but that comes later.

How do we maintain security?

Mobility usually means operating out of the corporate campus, which brings security risks that must be mitigated. But even on campus, mobility may involve changes in application structures, data access rules and processes — all of which come with their own additional risks. A strategy document should lay out basic rules for maintaining security in the new mobile environment. Although this sounds more like an implementation detail, having an umbrella idea of how security will be maintained will reduce redundant layers, and help ensure that everyone knows where security will be implemented. This may sound too detailed for strategic thinkers, but experience shows that if it's not stated at this level, then it's not going to happen and security chaos can result.

How do we measure success?

With goals and a path already written, all that's left is to stand back and ask yourself: "How will we know if we have met our goals?" Since these strategy documents should be reviewed every year or so, development teams find it very valuable to have a way of measuring whether the organization is achieving its mobility goals. This helps in deciding what needs to be changed, if anything, and in identifying the greatest successes so they can be extended or replicated.



Step 3: Determine Your Device End State

With a mobility strategy in place, now is the time to structure the CYOD program by defining the end state: how do you want to end up six to 12 months from now?

At this stage, it's good to stop Googling what other organizations have done or what other pundits advise, because every organization is different. Instead, use the mobility strategy document as your roadmap, because this tells you everything you need to know about priorities, requirements and how you will measure success.

Start by saying what you want to accomplish: what is the "end state" for your organization? Be modest: we're not talking about something years in the future, but something you can realistically envision happening in a calendar year. The easiest way to define the end state is to look at four questions and write brief — one paragraph should be enough — answers to them.

What does your device end state look like?

1 Who are the users?

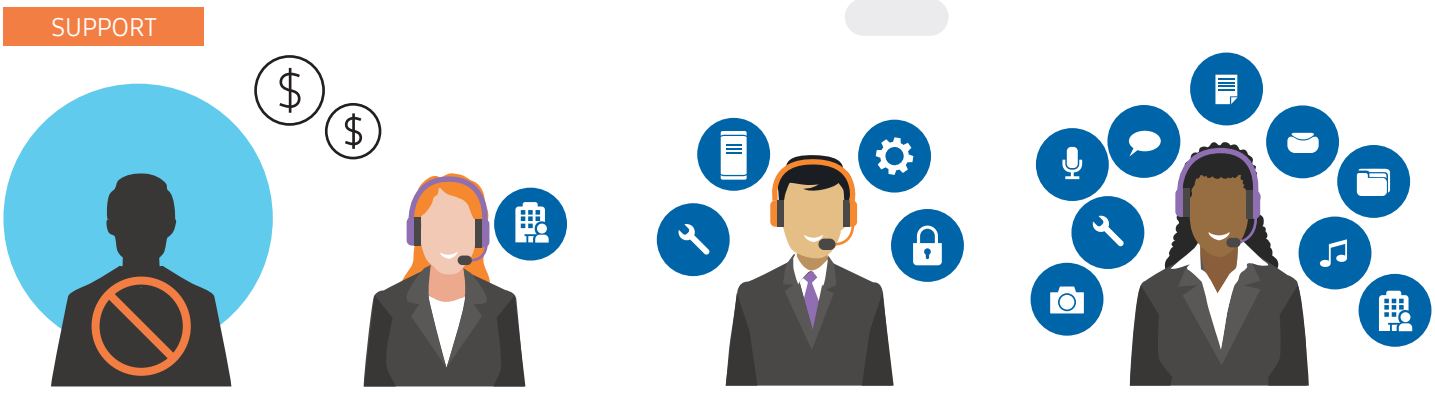
Is this CYOD program just for "mobile" staff who need a device to get their job done? Or is this for any worker who wants more connected access? Are we aiming at a special subset, such as executives, the sales or field service team? Or everyone associated to the organization, including consultants and part-time staff? Enumerate the specific groups of users who are going to be covered by the CYOD plan, and make sure you can map each group or answer back to a specific point in the strategy document. If you can't find a reason in the mobile strategy to include some group of users, either you've got to go back and fix your strategy document or you're not answering this question correctly.

2 What devices are we talking about?

Smartphones | Tablets & Wearables | Laptops

Because the "D" in CYOD/BYOD stands for device, it's all pretty ambiguous. Now is the time to define precisely what that D means. Are we talking only smartphones? Tablets? Wearables? Laptops? Be as specific as you can about what classes of devices you are going to cover — mapping it all back to the strategy document.

3 How much is this going to cost?

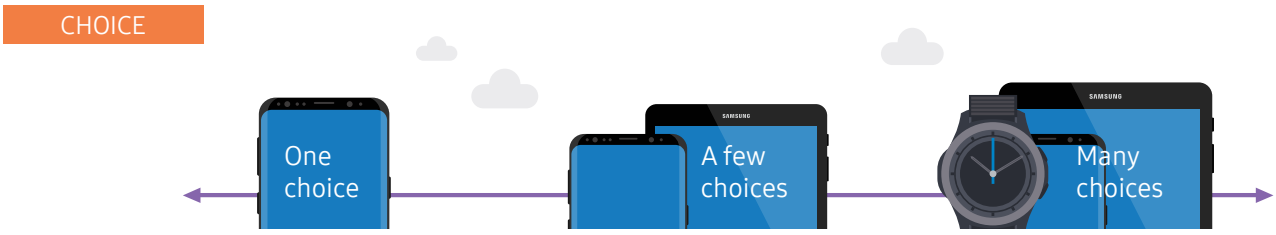


No Support | Support | Support ALL but apps | Lots of Choices

Budget discussions are always difficult, but as you structure your CYOD program, you need to start setting some limits so that costs can be clearly estimated. Many choices will affect total cost, with "buying devices" pretty far down on the list. These are less affected by the strategy document, but choices here will affect the penetration and overall ROI of the program. Be explicit about at least four aspects of CYOD design to set expectations for both users and decision-makers. We've listed them here in descending order of cost.

Support delivered to users is perhaps the biggest cost.

Setting limits on support are critical to keeping costs under control. At one end, organizations can decide to provide no support and run CYOD on an "as-is" basis. That's not recommended, but it is an option. Support can range from "nothing" to supporting only enterprise-specific applications all the way to a fully staffed call center offering support for both operating systems and applications, 24 hours a day.



Choice can also be expensive.

Trying to be all things to all people is usually an impossible task. CYOD usually means that users are presented with a menu of options. Be wary of making that menu too broad. Every device (and operating system) creates a maintenance liability: a requirement to keep things going for years, and everything on the CYOD list has its own liabilities and long-term costs. A single device isn't much choice, but two to four may be sufficient to meet most user needs. A super-broad list of more than five devices in each device class (e.g., smartphones, tablets, wearables) isn't sensible except in the largest of organizations.

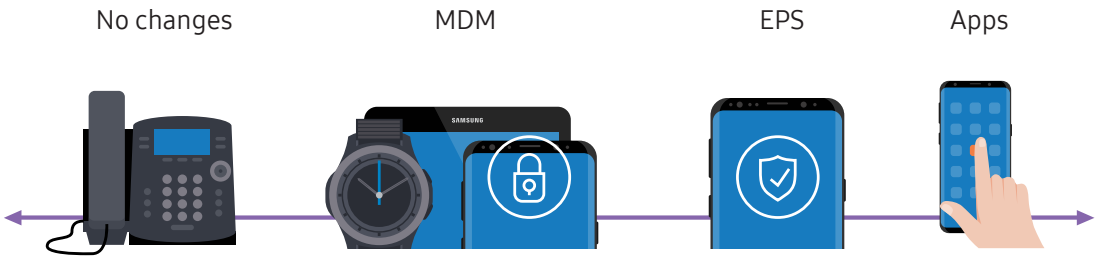
Monthly service charges add up.

Will the organization be paying for (and selecting) specific carriers? Or providing allowances to users who have their own carrier and monthly service plan? Or providing no budget or recommendation at all? Be aware the providing a stipend entails administration costs of its own.

Devices also cost.

You'll have to decide who is going to pay for the device and own the device. Will this fall 100% to the organization? Or 100% to the user? Or, something in between? Devices such as smartphones need to be replaced frequently, while laptops have a higher cost and longer life. Be sure to think about what happens to the device when the user leaves the company.

4 What changes to IT infrastructure are required to support this program?



Tools such as Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) and, to a lesser extent, Endpoint Security Suites (EPS) are almost always implemented within a CYOD mobility program. If these aren't part of your existing infrastructure, you'll need to acquire, install and assign administrative responsibility for these tools. Most organizations have existing EPS suites, but not all support mobile devices such as smartphones and tablets. This can mean either switching products or adding a second suite to your software portfolio. Application delivery can also require changes to infrastructure, especially when application developers need additional tools or application delivery controller hardware to meet security requirements. Identify any infrastructure changes that spill over from the application side towards IT operations, because these can be costly and take significant time to get fully into place.

Step 4: Get Your Policy Right

Your main inputs will be the mobility strategy and your well-defined device end-state, combined with a generous amount of discussion and debate from the mobility team you have assembled.

Whether you call it BYOD or CYOD or COPE, now is the time to put a policy in place that covers security and support issues. The CYOD policy is what defines the fine details of your deployment and is how you turn strategic thinking (in Step 2) into a more precise picture of how mobility will affect end users - and what end users need to know about as they participate.

The summary below includes major points that most mobility policies should include, based on your end-state. Remember that your defined end-state is always what provides the guidance for the policy, much more so than any template or online resource.

CYOD Mobility Policy Overview

Organizational Responsibilities

- **SCOPE** — WHO is participating and covered?
- **SUPPORT** — WHAT devices and carriers?
- **FINANCES** — HOW MUCH is paid by the company?

End User Responsibilities

- **AUP** — WHAT is the acceptable use for devices? WHAT are expectations for users?
- **Loss / Termination** — WHAT happens when a device is lost or a user leaves the organization?

Policy development is where the real interaction between IT and organizational management begins to touch the user community, and this can be a source of friction. Our experience is that aiming for total transparency during this process will reduce problems to the minimum. Try to keep all stakeholders in the loop about what is happening, including giving an opportunity to comment on draft documents. This can be a noisy process, and one that seems wasteful, but removing the element of surprise yields better alignment in the end.

One almost inevitable problem with CYOD programs is device envy. Smartphones and tablets are coveted items and people can attach considerable status to them: who has them, who gets them, who pays for them, and how often they are replaced and upgraded. Even if the total dollar outlay is small, differences in status between staff members will inevitably cause some reaction. It's not possible to have a CYOD program in place without someone, somewhere, getting upset.

However, you can minimize the hurt feelings — which tend to impact productivity and cause active sabotage — by being as transparent as possible. This transparency should start early and be something that is promoted as part of the CYOD program.

Step 5: Dive into Procurement

CYOD programs come with two third-party partners, at least: hardware vendors for smartphones, tablets, and even wearables and laptops (if they're part of your program), and carriers, who provide data and voice services.

They may also include a reseller or mobility-as-a-service (MaaS) provider. Generally, except for very constrained environments (such as one or two cities and staff who rarely travel on business), you should separate out carrier negotiations from hardware negotiations. Carriers are happy to sell you smartphones and tablets at advantageous prices, but these generally come with a cost: contractual lock-in. Even if the carrier is happy to unlock devices for you, most Android smartphones will still be tied to the carrier's software update servers and may even lose the capability to update software.

Hardware Vendors

Depending on what you've put in your CYOD policy, you may need to start down a procurement path or, at the very least, a price negotiation with your selected hardware vendor or IT reseller. Even if the CYOD program doesn't come with a subsidy from the organization, it's a valuable perquisite for staff if you take the time to negotiate a bulk discount or set up an Employee Purchase Program to simplify purchasing and ensure that users get the appropriate devices.

Another reason to work directly with resellers, particularly for smartphones: pre-enrollment and configuration of devices. Some smartphone vendors allow you to capture device serial numbers at the point of sale and "push" a basic configuration to the device when it is first powered on, before it even downloads your MDM/EMM agent. When you're deploying hundreds or thousands of devices, saving 30 minutes on each one adds up very quickly. Plus, by linking your CYOD program to a smartphone vendor's pre-configuration tool, you ensure that everyone has a basic configuration with the appropriate applications and settings from Day One.

Carriers

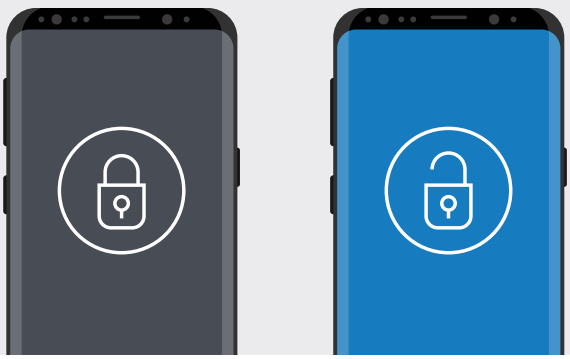
Carriers are needed for virtually every CYOD program if your organization plans on paying for part or all of the end users' monthly service plans. The market for carrier services in most metropolitan areas is usually quite competitive, so there are lots of opportunities for providing good value to end users — even if you choose not to pay for any of their monthly service plan.

One thing to keep in mind when negotiating carrier contracts is that some users will always need a "Plan B." No matter how good the coverage map is for a carrier, there are always blind and weak spots, and you don't want to be stuck with a user who can't use their smartphone because you've locked them into a carrier that doesn't cover their home. Carriers also vary from region-to-region, and will change their coverage over time with acquisitions and spin-outs, so some flexibility here is always a good thing. Hoping that a single carrier will solve all of your problems often leads to disappointment.

Locked or unlocked?

While the bottom line costs for simply buying unlocked phones directly from a reseller may look more expensive than taking the carrier discount, most organizations will find that unlocked phones give greater flexibility, better security (especially in Android devices), and allow you to customize your CYOD program based on your needs —not based on what devices the carrier decides to sell six months from now.

On the other hand, carriers selling smartphones and tablets may offer advanced consulting and deployment services for a CYOD project. Carriers have experience in large rollouts, and taking advantage of their services and logistics capabilities during project rollout may be worth the aggravation of dealing with locked phones in the future.



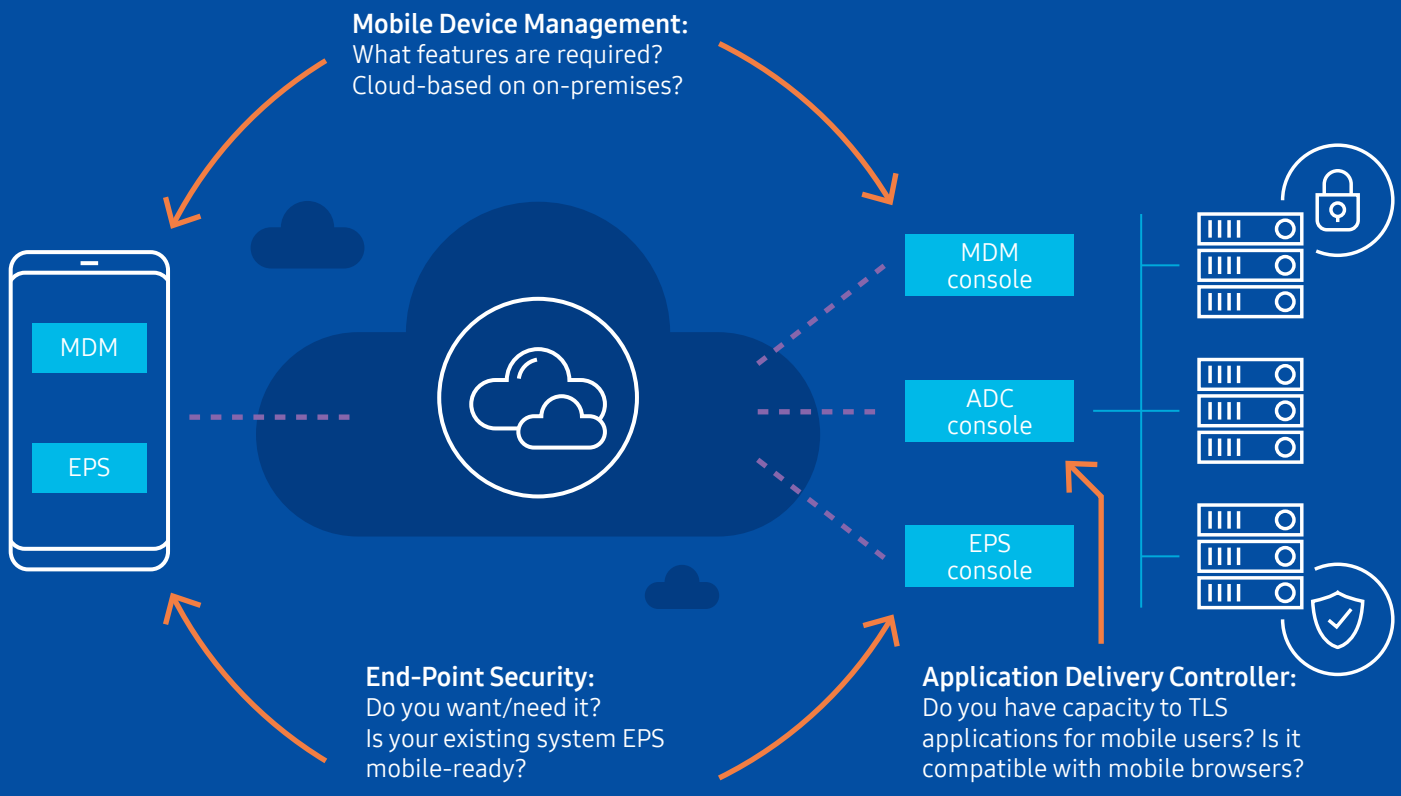
Step 6: Get Infrastructure Up and Running

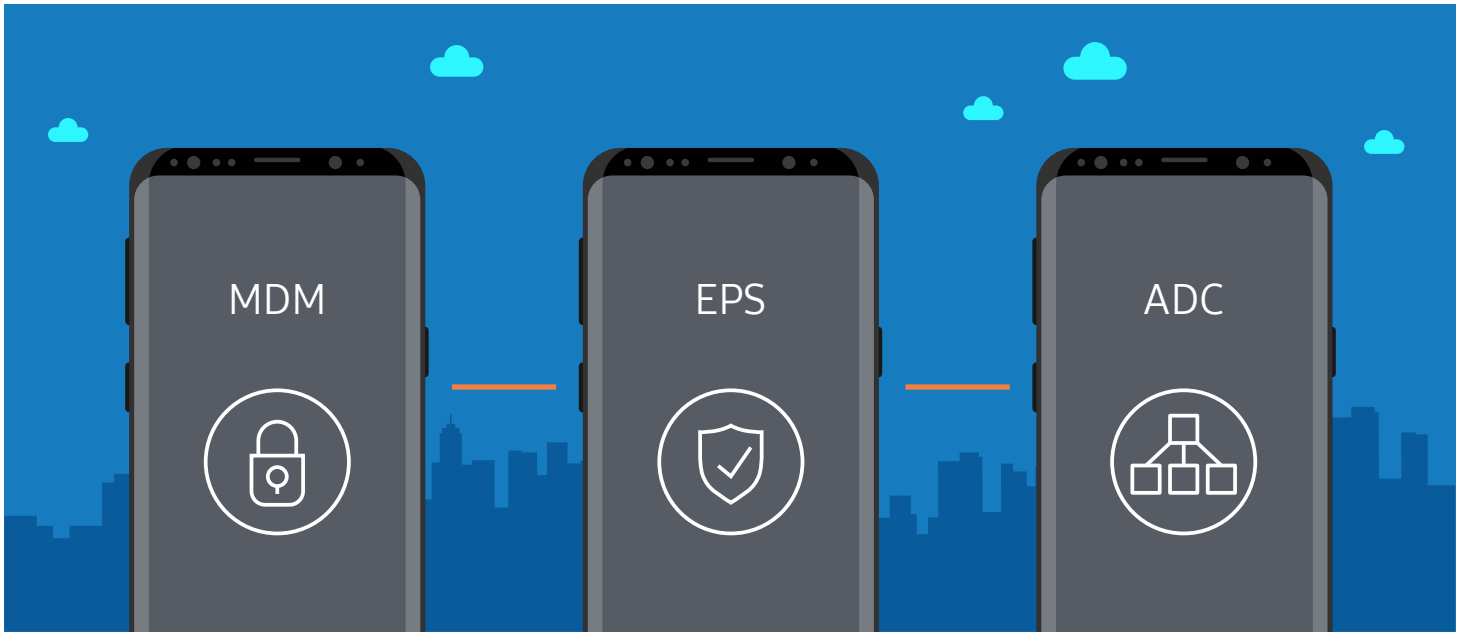
Before starting a large-scale deployment of devices, it's wise to put security and management infrastructure in place.

This minimizes disruptions down the line and also lets you identify possible show-stoppers or major issues early on. By knowing what things will look like when the first smartphone is deployed to a real end-user, you can build confidence in the support team and user community that things will go smoothly and predictably.

We've separated out "infrastructure" from "applications" because applications can take a long time to re-develop and re-deploy, while the infrastructure for a CYOD program usually is a much smaller intrusion. You don't need to have every application running on Day One, but it's nice to have at least some new apps to show users and managers the benefits of the CYOD program. In addition to the topics below, human infrastructure should be ready: Train support teams or identify third-party support resources and develop documentation for both end-users and help desk teams.

Infrastructure: End-Point Security (EPS), Mobile Device Management (MDM), and Application Delivery Controller (ADC)





There are three infrastructure areas that need attention: mobile device management, end-point security, and application delivery controllers (ADCs, sometimes called "load balancers").

Mobile Device Management (MDM)

MDM is the most critical piece of the infrastructure. For organizations that have not had a strong mobile policy in the past, this is often a new installation. MDM — sometimes referred to as Enterprise Mobility Management (EMM) — suites range from the very simple to amazingly complex.

Samsung offers an affordable, cloud-based EMM solution called Knox Manage that allows you to manage Android, iOS and Windows 10 devices. It provides a robust feature set including all the core policies such as whitelisting and blacklisting apps, event-based management, and device location tracking.

The market for MDM/EMM suites is broad and deep, with both on-premises and cloud-based solutions. Selecting the right MDM/EMM tool should not be difficult, since the requirements for what it can do have already been laid out as part of your mobility policy. Key options to look for, outside of device security and configuration controls, include ease of agent deployment and end-user self-service features.

End-Point Security

End-Point Security should be discussed and decided early on. As we discuss in whether or not you need an end-point security (EPS) suite for smartphones and tablets is still an open question, and will depend on a number of factors. However, once you decide whether having EPS is required or not, you'll want to make sure that it is part of the initial deployment along with MDM/EMM. Normally, if the existing organization EPS suite for laptops and desktops also is supported on smartphones and tablets, it's best to continue to use that same suite and the existing enterprise console. If the EPS suite is not supported, making a wholesale change will require further discussion and an evaluation of pros and cons. With CYOD deployments barreling full speed ahead, though, a swap-out of the EPS suite may be a major pothole in the way of success.

Application Delivery Controllers

Finally, any changes to Application Delivery Controllers (ADCs, sometimes called Load Balancers or Reverse Proxies) should be in place. ADCs are key to CYOD deployment for two reasons. First, they easily add a mandatory encryption layer to applications that are being pushed out as Internet-accessible. When the pre-mobile strategy called for remote access VPN, most mobile deployments prefer to avoid bringing up VPN tunnels and simply slide in a TLS encryption and security layer between the application and the network—an ideal job for an ADC. Secondly, ADCs often do image resizing and content rewrite to speed application access, especially when applications have a large client-side JavaScript component. Testing critical Line-of-Business applications and the ADC's rewrite capabilities against popular mobile browsers is a major step prior to deployment. If any ADC application optimization don't function properly on mobile clients, the ADC may need to have a software upgrade or may need to be configured to omit certain types of optimizations for mobile clients.

Step 7: Finalizing the Deployment Plan

With strategy, policy, infrastructure, and vendors all in place, now is the time to begin deployment and operations of your CYOD program — which begins with some planning.

Deployment often requires a lot of staff being very busy, but only for a short period of time, as devices arrive, are configured, and delivered to users. A mobility project usually includes ordering and staging devices so that users can dive in quickly with the right device and the right software at deployment time. Once the device is in (and inventoried), a basic software load with configuration settings has to be pushed onto the device so that it is ready for the user.

Planning at this stage is equal parts preparation for the actual deployment, and preparation for long-term operations. The table below identifies some of the questions you will want to address. If the burden of deployment and operations will strain existing IT resources, Mobility-as-a-Service providers can be brought in to help run the entire deployment and operations side of the CYOD program.

Establish a Reporting Plan

During initial deployment stages, reporting is also an important part of the process. Any change in mobile devices or mobility policy will bring out some squeaky wheels. Acknowledging issues, dealing with them, and also showing that they are a small part of the whole program is part of keeping things on track and moving forward. Be prepared to report laterally within the CYOD team so that everyone knows about progress and issues. Think about how you want to summarize deployment status, operations issues, end-user satisfaction and issues, as well as any security or interoperability problems encountered.

Because CYOD is high visibility, also be prepared to have simple reports ready for consumption both upstream, in the organization's management team, and for general user education. As part of "extreme transparency," letting people know how things are going is a great idea. By preparing these reporting templates ahead of time, you can minimize the time lost generating reports, yet still offer a professional and complete picture of what is happening.

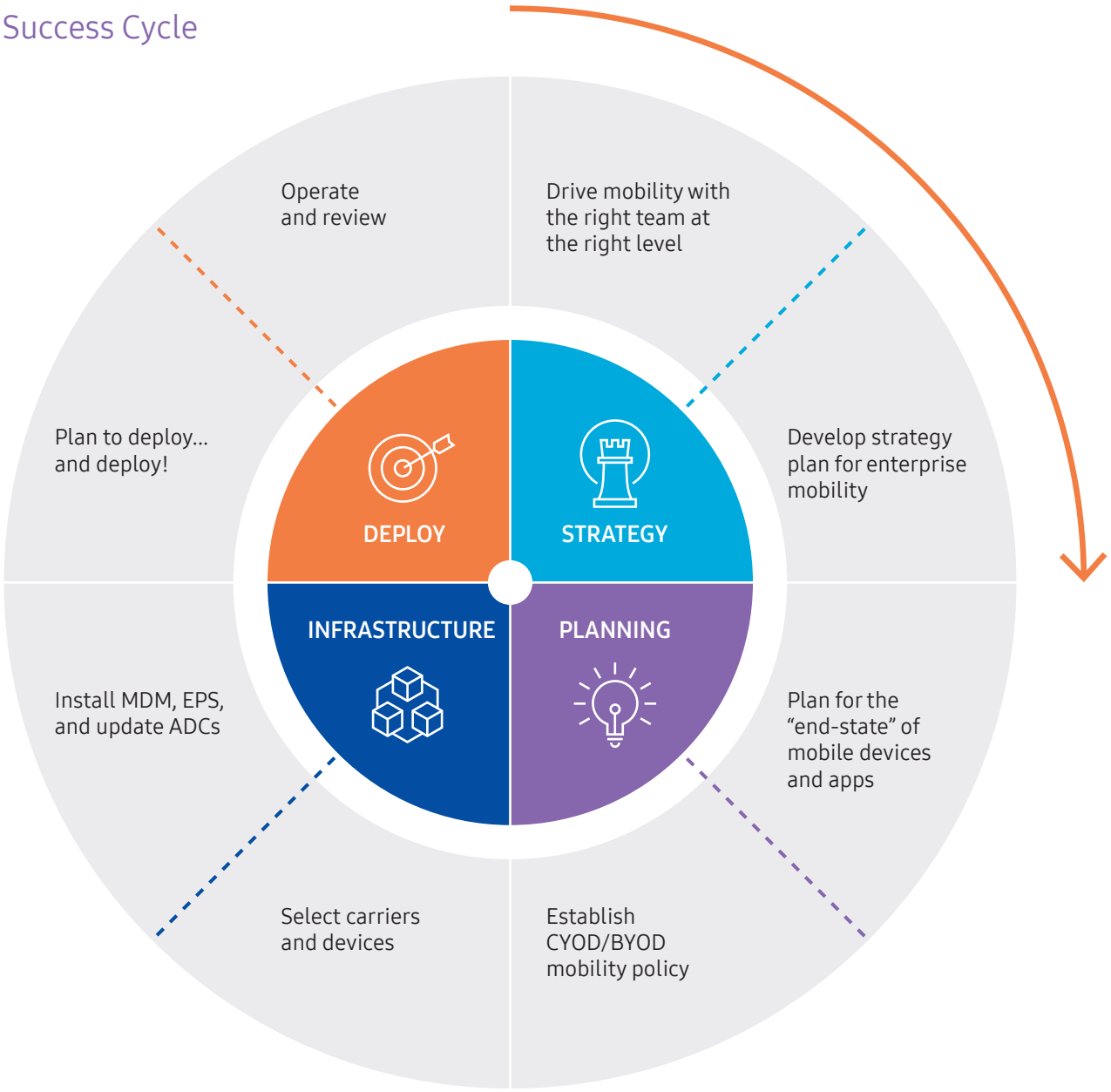
Deployment and long-term operations go hand-in-hand. Once the initial rush of new devices is over, things should settle down to a steady state of daily operations, occasional exceptions (such as device loss, failure or theft), and basic support. This will take continuing time, and you should allocate resources in your work plan to make sure that CYOD operations has the staff, training, and support needed.

Preparation for Deployment	Preparation for Operations
How will you get devices to staff? In-person? Remotely? Will you use third-party resources for this?	How will you deal with devices that need to be upgraded or repaired? What is the process?
How will you maintain device inventory? As part of existing tools? A separate tool linked to MDM/EMM? Within MDM/EMM itself?	How will you handle lost or stolen devices? What do users and help desk teams need to know?
How will enrollment into MDM/EMM occur? Will you be using vendor pre-enrollment tools (such as Samsung's Knox Mobile Enrollment or Knox Configure)?	How will end users get support? Are teams ready and trained for this?

Step 8: Review and Revisit Mobility Plan

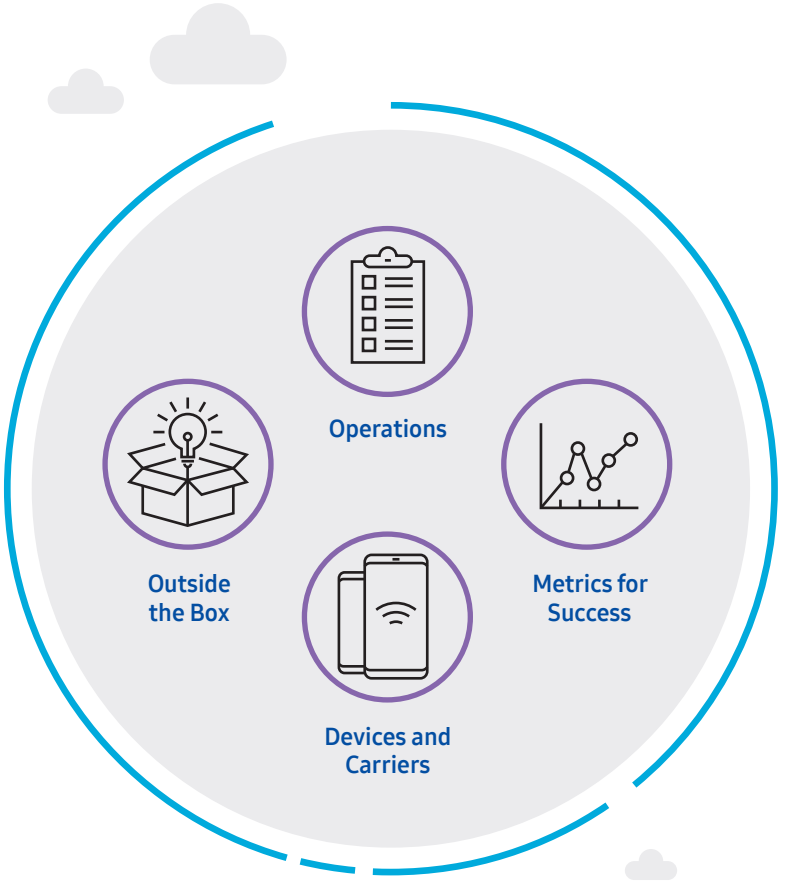
Mobile devices are fast-moving technology. New smartphones are launched frequently, but it's more than that — new ideas sweep through the mobile device community very quickly. Biometric authentication, Near-Field Communications, secure containers: These are examples of things that didn't exist one day, and were common in devices within 18 months.

Mobility Success Cycle



A good CYOD mobility program has built-in checkpoints to pause, zoom out, and evaluate successes, failures, and needed changes. You don't need to allocate time to re-do all of the steps we've outlined in this white paper, but you should plan to talk to application developers, line-of-business managers, end users, and IT teams every 12 to 24 months. The goal is a conscious and documented effort to review that the mobility program is optimized for your enterprise.

You don't need to start over each step 2 through 7, but you should make a conscious and documented effort to review that every step was done correctly and is aligned with the rest of the enterprise. Start by looking at four main areas:



Operations

Operational reporting can give you a feel for the day-to-day experience in areas such as deployment, support, and user experience.

- How is the infrastructure running?
- Are there changes in particular applications (e.g., MDM tool choice or options) that will help to smooth things out and optimize the program?

Metrics for Success

Because metrics for measurement of success were built into the strategic plan, this is also a good opportunity to review the numbers.

- Are you meeting the success metrics you laid out?
- What should change about the program to increase its chances of success?

Devices and Carriers

- How are your devices and carriers operating?
- Were the choices well-accepted by users?
- Should the list be lengthened or shortened?
- How many exceptions were required and is there a trend that needs to be addressed?
- Are carriers performing as expected and within budget?

Outside the Box

Now that you've got at least a yearlong experience with a well-developed mobility program, take a few moments to think outside the box.

- How can mobility help the organization?
- Look at what your competitors are doing; get some blue-sky thinking and outside help in to lead discussions.
- What changes are appropriate?

Enterprise mobility may seem a daunting project, but the eight steps in this white paper break things down into simple and manageable tasks. Follow as much of the cycle as you need to, and gain the benefits that mobility can bring to modern organizations.

How Samsung Can Help

Samsung understands the challenges of enterprise mobility. Beyond our portfolio of smartphones, tablets, wearables, 2-in-1s, and laptops, we offer a broad range of device management solutions, as well as the expertise to help plan and execute any mobility initiative.

The Samsung Knox Platform and Solutions

Learn more about the defense-grade Samsung Knox security platform and device management solutions, such as Knox Configure, a tool for remotely provisioning and configuring a fleet of mobile devices, and Knox Workspace, for secure containerization of work and personal data.
samsung.com/knox

Samsung Business Services

Learn about how Samsung Business Services can help with device deployment and technical support. Get easy access to expert advice and assistance, including EMM assessments, deployment planning and execution, and tech-to-site senior engineers.
samsung.com/SBS

The Enterprise Edition

Learn about how Samsung's Enterprise Edition unlocked devices can help drive your business. Combining Knox Configure, Samsung E-FOTA, regular security updates, these combine powerful and simple device management, customization capabilities, and defense-grade security.
samsung.com/enterprise

Get a Consultation Today

Get an enterprise mobility consultation from Samsung's mobile solutions experts to address your biggest business challenges. Click here to learn more.