The Ultimate Guide to BYOD

MobileIron®

www.mobileiron.com

CONTENTS

BYOD: Driving the mobile enterprise transformation

The rate at which enterprises are embracing mobile technology is more than an evolution — it's a global transformation. In fact, considering how fast users and businesses around the world are dropping PC dependency in favor of mobile devices, IDC predicted that PC sales would drop to record lows in 2013.

The explosive popularity of mobile devices and apps offers a tremendous opportunity for any enterprise to become a "Mobile First" organization — one that views mobility as the most important business enabling technology today. Mobile First organizations understand that the Bring Your Own Device (BYOD) trend is here to stay and is fueled by users who expect total flexibility in managing their professional and personal business wherever they are, on their device of choice. However, the ability to securely and cost-effectively enable BYOD presents a significant challenge for even the most forward-thinking companies.

Protecting corporate data and network resources while leveraging the benefits of mobility is a constant balancing act; one that requires IT to shift its focus from security lockdown to business enablement. While some companies (particularly in the tech sector) are "doing" BYOD well, most are still trying to devise a comprehensive, best-practice strategy for securing and enabling personal devices at work. Many organizations are simply figuring it out on the fly, leaving both IT and employees unclear about exact policies and expectations regarding personal device use and management.

For instance:

- How much control should the company have over the employee's device and content?
- Who should pay for the device and monthly service?
- What constitutes a reasonable end-user agreement?
- Which devices should the company support?
- What happens to company data on a personal device when the employee leaves the company?

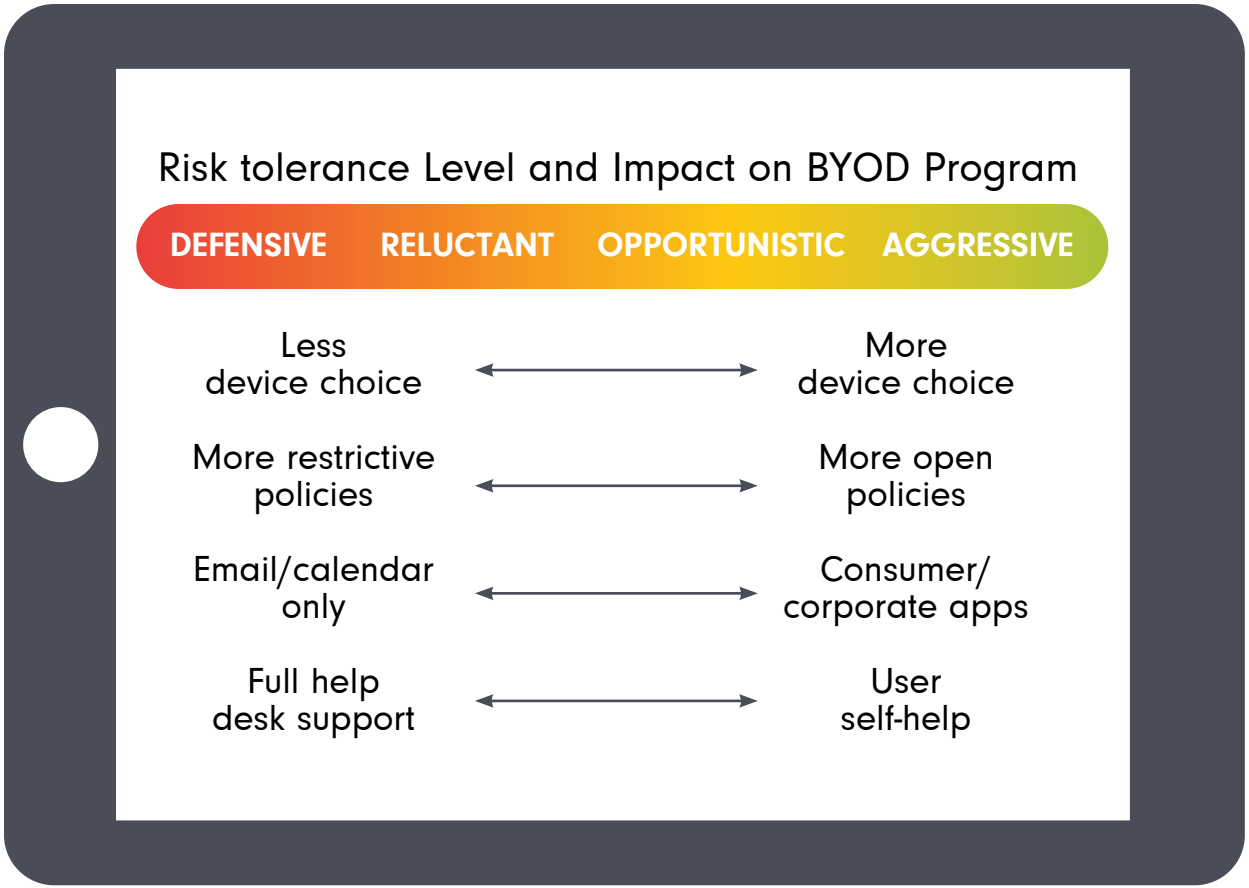
This eBook is designed to help your organization anticipate, understand and manage these and other questions regarding BYOD in the enterprise. In this four-part guide, we'll look at best practices for preparing, building, rolling out and sustaining a successful BYOD program over the long term.

Determine Your BYOD risk tolerance

Mobility is opening up data and applications to an unprecedented number of users, on any device, almost anywhere in the world. But how can organizations fully exploit the business potential of mobile transformation without compromising security and productivity?

Understanding your company's tolerance for risk is the first step to understanding how BYOD can work in your organization. Your company's industry may be a primary indicator for risk tolerance. For instance, organizations in healthcare, financial services, government or security services will likely adopt a more defensive position toward BYOD than Internet-based tech companies.

Completing a BYOD Risk Tolerance Assessment will help identify special areas of concern or focus for your organization. It will also give you a good idea of your company's tolerance for employee flexibility, range of devices allowed, IT involvement and security policies. In a nutshell, identifying your risk tolerance is a good starting point to ensure your BYOD program supports your company culture and business goals without compromising security or employee satisfaction.



Engage stakeholders early to define program goals

One of the most important steps to developing a BYOD program is getting early buy-in from critical players across the company. While it can be difficult to align the interests of diverse company leaders from executive management, HR, legal, finance and IT, their support is critical for securing adequate program funding and momentum.

While the approval of executive-level stakeholders is essential, you also need to ensure the program will meet the needs and expectations of end users. In general, mobile users expect access to the data they need for both work and personal business, on their device of choice, wherever they are. Any BYOD program that fails to meet these requirements will likely be rejected by the majority of mobile users. To avoid this outcome, adding one or two employee representatives to the team can help you gain valuable input and feedback on end-user preferences, device requirements, support and communication needs and more.

Anticipating common objections to BYOD can also help you facilitate the planning phase. Some frequent concerns and responses that come up during this phase include:

EXECUTIVE SPONSORSHIP	HUMAN RESOURCES	FINANCE	IT OPERATIONS
We can't get executive support, but let's move the BYOD plan forward anyway.	**The company cannot be held responsible for compromised personal data on employee-owned devices.**	**We can't fund a program that doesn't offer demonstrated cost savings.**	**We cannot support the huge variety of apps that the business wants on personal devices.**
Simply put, a BYOD project can easily derail without executive sponsorship. Because BYOD projects require participation from diverse stakeholders, executive leadership is often necessary to ensure deadlines and responsibilities are met.	Working together, HR and IT should design clear boundaries between corporate and personal data. Also, your end user agreement should specify that the company may access personal data if the device is subject to forensic analysis. Also, upon separation from the company, all attempts will be made to preserve personal data on the employee's device, but a full data wipe may be issued if deemed necessary.	Actually, savings can be realized by reducing support and operational costs through an end-user self-service model that leverages self-help tools, user support communities, social networks and user forums.	For iOS deployments: New controls available with AppConnect allow moving, adding and changing app configurations and policies without having to deploy new versions of apps. Having the ability to dynamically modify or update security policies, user access and server configurations on already deployed mobile apps will reduce the operational overhead of managing mobile apps.

To help resolve these and other concerns right from the start, you should form a BYOD steering committee comprised of representatives from all stakeholder departments. A steering committee can help groups with different priorities build consensus and define program goals that all stakeholders agree upon. Documenting these goals will serve as a valuable resource to help all stakeholders stay focused on the overall objectives as the BYOD program evolves.

Survey and communicate with employees

Build it and they will come, right? Not necessarily. A BYOD program that is too restrictive, or lacks support for the right devices, will result in a lack of participation and wasted time and money. To avoid these pitfalls, you need to gather employee input early in the preparation phase.

After you have determined your company's BYOD risk tolerance and stakeholder goals, the next step is to issue a short but specific employee survey across the company. The greater your risk tolerance, the more important it is to tailor the survey to capture user preferences for devices, apps, communication tools and tech support. To ensure you gather the information needed to design a successful BYOD program, your survey should include questions that identify:

- Which OS/devices employees currently own and plan to purchase in the future
- Which factors would encourage BYOD participation
- Which factors would discourage BYOD participation
- Which corporate apps they consider most valuable
- Their comfort level with self-service support
- The impact of BYOD on company perception, productivity and work/life balance

Identify your mobile IT capabilities

Now that you know your BYOD risk tolerance, program goals and user preferences, do you know if you have the right people and resources to build the program your company needs and users want? A capability assessment can help you determine if you have the right people, processes and technology to enable employees to use their preferred devices and apps and securely access business data on any network.

A capability assessment is actually a simple checklist of requirements, the status of completion or availability and where the capability or task is in the procurement process. For example, an IT staffing checklist would include all of the resources needed to implement the program, whether those resources are currently available or not, and who is responsible for bringing those people on board.

Here's a snapshot of just a few of the staffing requirements you would need to include in the BYOD capability assessment:

Sufficient Staffing	*Please place an 'X' in the appropriate column*				
	Ready	**Planned**	**None**	**N/A**	**Comments**
IT Resources					
Device exports					
Blackberry: <list name(s)>					
iOS: <list name(s)>					
Android: <list name(s)>					
Windows Phone: <list name(s)>					
Device testing					
Design process: <list name(s)>					

Upgrade your infrastructure to support BYOD

The technology skills needed to manage a mobile IT infrastructure differ dramatically from those needed to run a traditional desktop enterprise. Procuring the right expertise is critical to executing a successful BYOD program. Here are the recommended roles needed to build and sustain BYOD (keep in mind that one individual can wear many hats; you don't necessarily need one person for each role).

MOBILE SYSTEMS ENGINEER

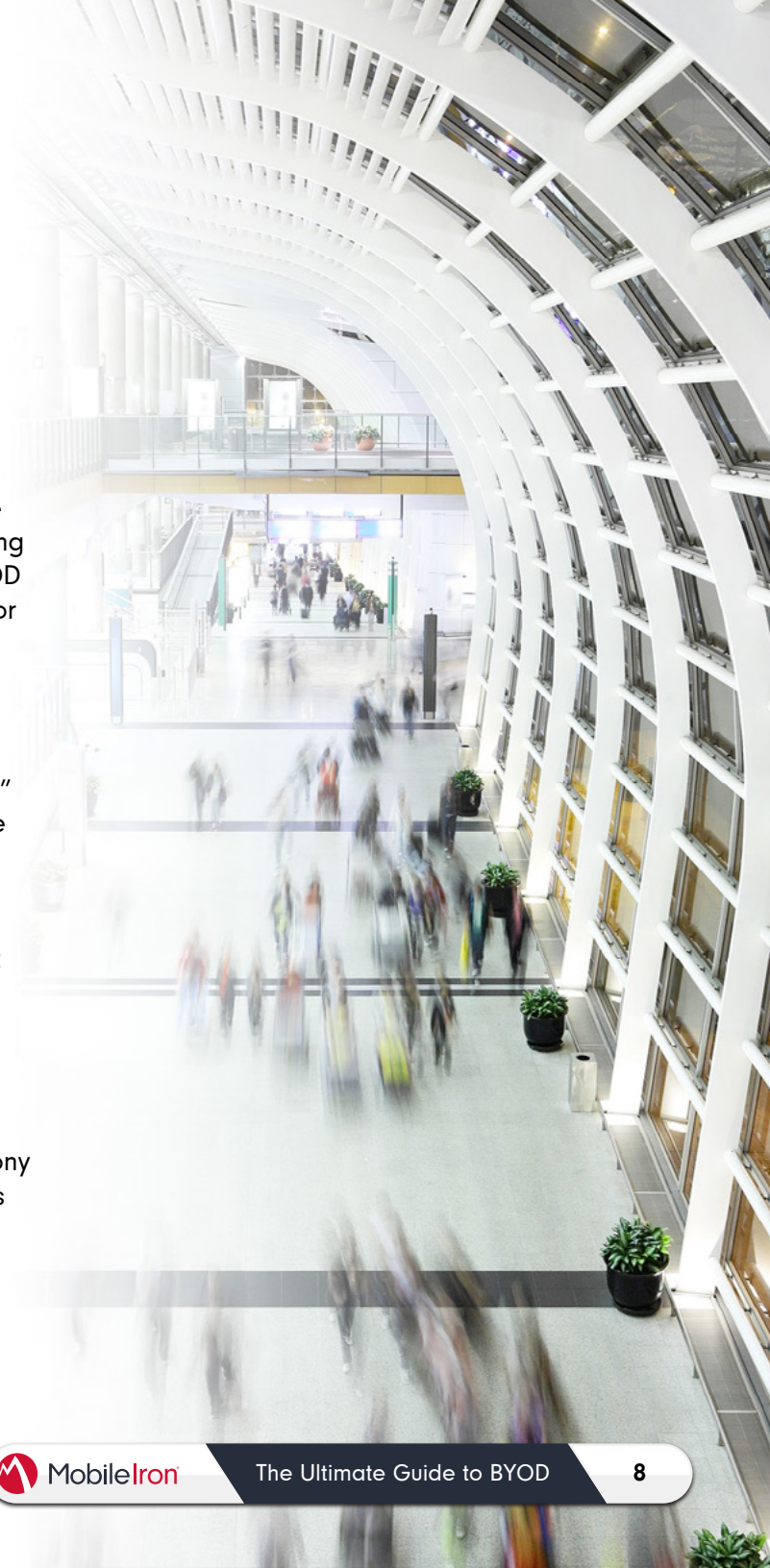
A mobile systems engineer is a subject matter expert for all aspects of mobile technology. This role encompasses all hardware, software and networking technologies required to implement a BYOD program. The mobile systems engineer also provides expertise in integrating mobile technologies with enterprise components such as identity, messaging, security, networking and database services. Their domain of expertise includes:

- Mobile operating systems, such as iOS, Android and Windows Phone 8
- Carrier networking technologies, such as GSM/CDMA/LTE and underlying protocols
- Mobile hardware, software, applications, application programming interfaces (APIs) and development toolkits

MOBILE DEVICE EXPERT

A mobile device expert is a "gadget hound" who stays on top of both existing and future devices and software releases that can impact the mobile infrastructure. By staying current on mobile technology trends, the device expert can prepare the environment to either support or restrict the use of new devices. The device expert is fully versed in popular platforms and manufacturers including:

- Android: Samsung, Motorola, HTC, LG, Sony Ericsson, Huawei, Dell, Lenovo, Acer, Asus
- Windows Phone 8: Nokia, HTC, Samsung
- iOS: All Apple devices
- Blackberry: All Blackberry devices



MOBILE SECURITY EXPERT

A mobile security expert is responsible for establishing mobile security policies and controls as well as determining their effectiveness and revising as necessary. The mobile security expert also educates users on social and behavioral security risks, sets appropriate use policy and helps develop strategies for:

- Mobile security and risk mitigation
- Mobile data protection
- Mobile OS platform review and positioning
- Mobile application threat management

MOBILE APPLICATIONS DEVELOPER

Regardless of whether your enterprise develops its own applications or outsources mobile app development, you may need onsite app developers with the following skills:

- Experience with application development lifecycles and methodologies
- Ability to design and develop iOS, Android and Windows Phone 8 apps
- Hands-on experience in Objective-C, Cocoa Touch, iOS SDK, XCode, Developer programs, Java, Android Market, Android SDK and device manufacturer APIs, .NET, Web Services, XML and HTML5
- Strong object-oriented programming and design skills

MOBILE SERVICE AND SUPPORT RESOURCES

The accelerated lifecycle of mobile devices and services requires an infrastructure than can quickly adapt to constantly evolving conditions. To respond effectively, your enterprise must customize the way services and support are delivered to mobile users, because they have much different needs and expectations than PC users. To be effective, mobile service and support resources must be able to:

- Provide self-service tools to help improve user satisfaction and reduce costs
- Establish a core mobile support group that manages all mobile escalations
- Develop and distribute knowledge base articles, support scripts and procedures to all users
- Share knowledge through social networking and mobile communities
- Establish clear and regular communication across multiple channels to keep users up to date on service status and changes

Include the Eight Components of a Successful BYOD Strategy

The ultimate challenge of any BYOD program is not just managing data security or optimizing end-user productivity. It's maintaining a constant balance between security, compliance, legal liability, cost concerns and a positive user experience. The Eight Components of a Successful BYOD Strategy are designed to help you build a sustainable program that meets the needs of your business and employees over the long term.

8 COMPONENTS OF A SUCCESSFUL BYOD STRATEGY

These components are the essential ingredients that ensure your BYOD strategy can meet the requirements for security, cost control, accountability, productivity and user satisfaction.

1 SUSTAINABILITY:

Maintain a positive user experience

BYOD is a relatively new trend that is still establishing best practices. As a result, many companies rush to create policies and processes that are simply unsustainable over the long term. Understandably, enterprises are mainly concerned about implementation costs and security, and tend to focus on those issues in the beginning. But without respect for the user experience, the BYOD program may never even get off the ground.

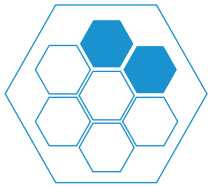
Here's why: If BYOD policies are overly restrictive, lack adequate support for employees' preferred devices or are simply too complex and confusing, employees will find a way to either circumvent the policies or end their participation altogether. In both instances, the needs of the company are not met – either security is compromised or business value is lost. So while cost and security concerns are important issues to manage, BYOD program sustainability depends completely on delivering a consistently positive user experience over the long haul.

2 TRUST MODEL:

Mitigate security risks

Once upon a time, corporate-owned desktops were among the few employee devices enterprises needed to manage. Today, the average employee uses several devices for work, including desktops, laptops, tablets and smartphones. Managing the sheer number and range of these devices — whether owned by the employee or company — has introduced extremely dynamic and complex security issues. Therefore, building a trust model that identifies how and when a device falls out of compliance, steps for remediation and the extent to which these actions are acceptable to users is absolutely essential. A trust model should:

- Assess the risk for common security issues on personal devices.
- Outline remediation options — such as notification, access control, quarantine or selective wipe —that will be issued depending on security concerns and whether the device is owned by the company or employee.
- Set tiered policies for security, privacy and app distribution based on device ownership.
- Clearly establish the identity of the user and device through certificates or other means.
- Ensure that security policies are sustainable and flexible enough to support a positive user experience without compromising data security.



3 DEVICE SELECTION:

It's a popularity contest

Based on feedback from your initial employee survey, you should have a good idea about which devices and platforms employees currently use and are intending to purchase. You should include as many of these devices as possible when the program launches to maximize employee participation. In addition, your device selection process should:

- Include all of the desired mobile platforms in the program as long as they meet your security and support requirements, such as asset management, encryption, password policy, remote lock/wipe, and email/Wi-Fi/VPN configuration. Without these basics, the mobile platform is not viable for the enterprise.
- Develop a certification plan to ensure that future devices can be quickly and efficiently evaluated for possible inclusion in your program.
- Clearly identify which devices are allowed (or not) and why, otherwise employees may purchase devices your program doesn't support.
- Ensure your IT team maintains expertise and knowledge about constantly evolving mobile devices and operating systems, otherwise your BYOD program can quickly become obsolete.

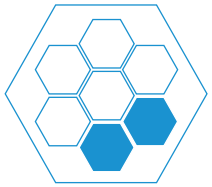
4 LIABILITY:

Protect your company from legal action

Introducing a BYOD program may also introduce new liability concerns to your business. As part of your BYOD program, you need clear policies and procedures that protect your company from threats ranging from the loss of intellectual property and confidential customer data to legal action, fines and reputation damage resulting from data leaks.

While every business needs to seek specific legal counsel on BYOD liability, your mobile device policy or end-user agreement should include, at minimum:

- Security policies for enterprise data on personal devices (especially since different types of security may be required on different devices. For example, more protection against over-privileged consumer apps might be required on Android vs. iOS).
- Policies for personal web and app usage (during and after business hours, onsite and offsite).
- Clear limitations for company liability due to the device owner's personal data loss.
- Understanding of how BYOD reimbursement (partial stipend vs. full payment of service costs) affects company liability.
- Extent of company's liability for personal data loss (for example, if IT accidentally administers a full wipe of data on a personal device).



5 USER EXPERIENCE AND PRIVACY:

Establish employee trust

Optimizing the user experience should be a top priority for your BYOD program. Clear communication over sensitive topics such as privacy is critical for establishing employee trust. Therefore, a social contract that clearly defines the BYOD relationship must be established between the company and your employees. The contract is a well-defined agreement that helps:

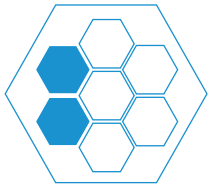
- Identify the activities and data IT will monitor on the device, such app inventory, to protect against rogue apps that could compromise enterprise data.
- Clarify which security actions IT will take in response to certain circumstances.
- Define granular controls such as activity monitoring, location tracking and application visibility.
- Critically assess security policies and restrictions to ensure they are not overly restrictive.
- Identify core services, such as email and mission-critical apps, the company can deploy to the employee's device.
- Preserve the native experience so employees can continue to use their preferred apps for everyday functions.
- Communicate when employee devices are out of compliance, the possible consequences and proactive notifications to help users remediate issues quickly.

6 ECONOMICS:

The cost of doing BYOD

BYOD programs are relatively new, so definitive studies of the economic benefits and impact are still on the horizon. But that doesn't mean it's too early to determine how to structure the financial aspects of your BYOD program. Key issues to consider include how to:

- Pay for devices and service: Determine if the employee will be 100 percent responsible for device and service costs, or if the company will pay a full or partial stipend.
- Leverage agreements with mobile operators to provide business, concierge and self-service options to users.
- Explore existing telecom services and processes and, where possible, offer corporate discounts to users, including waivers of termination fees and early upgrade allowances.
- Research new carrier services and plans that can improve and enhance the BYOD program.
- Save money on helpdesk resources by implementing self-help services



7 APP DESIGN AND GOVERNANCE:

Enforce security without becoming Big Brother

In a BYOD environment, apps involve sensitive enterprise data, which can easily be compromised if the device is accidentally lost or infected with malware. Your organization will therefore want some level of control to prevent data from falling into the wrong hands. And yet, employees don't want to feel that the company is tracking their every move, post and tweet, especially on their own devices. To gain employee trust and protect critical data, your BYOD program must implement app design and governance procedures that:

- Modify app availability based on security requirements.
- Communicate and justify the extent to which IT supports or restricts personal apps.
- Define app availability based on device ownership, because certain internal applications may not be appropriate on personal devices for security reasons.
- Define enforcement or remediation levels for app usage violations (such as notification, access control, quarantine or selective wipe).

8 INTERNAL MARKETING:

Build your IT "brand"

The process of implementing a BYOD program offers a great opportunity to nurture employee-company relations. You can promote your program as a corporate effort to support work/life balance through increased mobility and flexibility. The company can also foster the internal perception of IT as a champion of end users and supporter of technologies that employees want to use. In addition, a BYOD program can be used as an effective recruiting tool to show that the company values leading-edge technology and greater autonomy for its employees.

While internal marketing may seem like a low-priority activity, it can be a highly effective way to improve employee satisfaction, productivity and longevity, as well as enable IT to position itself as an ally to the mobile workforce.

"Soft launch" your BYOD program

After your program goals, policies, processes and technical infrastructure have been established, you can begin the phased rollout or "soft launch." By rolling out in phases, you allow a small subset of users to test the program and provide feedback on how to improve performance, support and other issues that you might not have discovered during the initial phases of building out the infrastructure. The BYOD program rollout typically follows three phases: Pilot, Deploy and Sustain. In some cases these phases may be combined or skipped altogether, but we'll describe them in detail for this guide.

INITIATE PILOT TESTS

Pilot tests help you troubleshoot and resolve problems before rolling out the BYOD program to the entire company. They provide an opportunity to safely test functionality from end to end and collect user feedback to identify what is working well and what needs fixing.

STEP 1:

Select the sample user group for the pilot

Choose a sample group of users to complete the device registration and configuration process. Your sample group should be a microcosm of the entire company and include a wide range of roles, business units and job functions so you can test the process of qualifying users by role and manager approval. You should also distribute the BYOD mobile device policy or end-user agreement at this stage to ensure users understand the terms of the program.

By including a large percentage of business and non-technical users in your sample group, you can get a better understanding of the average BYOD user experience. However, IT operations staff should also participate in the pilot to ensure any technical issues are discovered during the pilot phase.

"Soft launch" your BYOD program, continued...

STEP 2:

Survey employees to continually improve the user experience

It can't be emphasized enough: You need to survey users during every phase of the BYOD implementation to make sure the program is meeting employee needs and expectations. The three types of surveys include:

- **Pre-deployment survey,** which captures employee preferences for devices, operating systems, applications, data plans and support models.
- **Registration survey,** which captures the user's first experience with the BYOD program, and can identify any gaps in the device registration process. Because registration is essential to employee participation in the BYOD program, you want to make sure that the process is as fast, efficient and easy to understand as possible.

- **Follow-up or closing survey,** which provides both specific and open-ended questions to gather feedback about the overall user experience during the pilot test. It can capture metrics on performance and determine if the process has met employee expectations and program goals.

Deploy the BYOD program and training services

Once you've ensured that all the registration and configuration processes are in working order, the next step is to fully deploy the program. However, instead of rolling out the program to the entire company, it's best to stage the deployment in phases to minimize potential impacts on performance and availability. By staging the rollout based on geography, department, job function or other criteria, you can ensure the right resources are available to mitigate any issues.

You will also need to set up effective training and self-service capabilities when you deploy the program. Comprehensive and easy-to-use instructions on device registration and troubleshooting can help streamline the process of bringing employees on board. You might consider conducting your training program in a variety of formats — online, in person and through written documentation — to support the different ways users access information.

The ultimate goal of user training is to minimize helpdesk calls and maintain uptime by anticipating and resolving problems before they lead to lost productivity, compromised data or more serious issues. And, by providing comprehensive training through self-service guides, online tools and a broad user community, you can increase employee satisfaction by giving them greater autonomy over how they work.

You've reached a comfortable cruising altitude. Now what?

Once your BYOD program has been fully deployed across your company, the work of sustaining the program begins. The first step is to transition BYOD services from the "Build" team to the "Sustain" team; that is, from engineering to operations staff. This transition includes knowledge transfer, documentation reviews, help desk services, support and escalation process design. Admittedly, the handoff process can be labor-intensive and challenging, especially when transitioning to outsourced or third-party support centers. To ensure the transition does not impact mobile service levels or security, you need to establish clear processes for escalation, incident, problem, configuration and availability management.

Enable self-reliance, self-service and self-resolution

In a BYOD program, the old-school model of helpdesk calls and tickets gives way to a new era of user-based self-service. Although the need for an IT helpdesk will never go away, a core component of BYOD is a comprehensive support service that allows users to resolve the majority of incidents without helpdesk intervention. The self-service model should allow users to:

- Self-register new devices, monitor and manage current devices and wipe or retire devices as needed.
- Self-remediate hardware, software, application and compliance issues through clear notifications and resolution instructions.
- Stay productive and efficient while maintaining security and compliance.

Incrementally add more devices, systems and apps

As mentioned earlier, the initial rollout of the program should include as many popular devices as possible to encourage employee participation. However, the market introduces new devices every 3-6 months, so your company will need a fast, efficient, light-touch certification plan for evaluating all future devices. The certification process must be ongoing and continually evolving. If the process is too heavy, it will become expensive and eventually fall behind the technology curve, so speed and efficiency are essential.

Ensure safe and effective device retirement

The lifecycle for mobile devices is significantly shorter than that for laptops and desktops — sometimes less than a year. Because users upgrade their devices more frequently, you will need to have a secure device retirement process in place to ensure that corporate data is not compromised once the device leaves your control. You typically need to retire devices when the user:

- Upgrades or purchases a new device
- Separates from the company

DEVICE UPGRADE OR PURCHASE

In the case of an upgrade or purchase, the user should notify the helpdesk once the new device has been received. The user should be reminded to back up data and apps on the old device and move this content to the new device. The helpdesk can then complete the security process by removing all network access, configurations, apps and data that had been granted to the old device.

To support your company's internal marketing efforts, you should already have recommendations for device recycling or donation centers where the employee can send the old device (assuming it won't be passed on to a friend or family member). Encouraging device recycling or donation offers a good public relations opportunity for the company and helps prevent usable devices, with hazardous components, from ending up in landfills.

Continued...

Device retirement, continued...

SEPARATION FROM THE COMPANY

The device retirement process for users who are separating from the company is slightly different from the device upgrade process. Instead of being initiated by the user, the separation process should notify the user when access to corporate resources will be revoked and the device retired. The timeline and type of notification may be different depending on whether the separation is due to a resignation, reduction in force or termination, and should be integrated with existing separation processes in consultation with human resources.

Measure and demonstrate BYOD value

Measuring the ROI of your BYOD program will be essential to guaranteeing long-term executive support. Because BYOD is a relatively new development, most organizations are still determining how to best measure ROI. It will typically include a combination of the following variables:

- Hardware savings on devices owned by employees, unless subsidized by the company.
- Overage charges due to excessive personal or business use.
- Cost of service plans, which will depend on your company's ability to leverage the benefits of consolidation with the carrier.
- Productivity gains, which, while hard to quantify, can be achieved through increased employee satisfaction and flexibility with the tools they use for work.
- Helpdesk costs: Although the complexity and variety of devices can potentially increase helpdesk costs, mobile employees are often willing to invest time in troubleshooting problems before calling IT. With the right self-service tools, the helpdesk may become a last resort for end-user problem resolution, which helps control IT costs.
- Liability costs that can vary depending on who owns the device: the employee or the company.
- Tax implications, which can vary based on whether the company or employee owns the device or what percentage of reimbursement must be reported for auditing purposes.

CONCLUSION

Achieving the Mobile First transformation

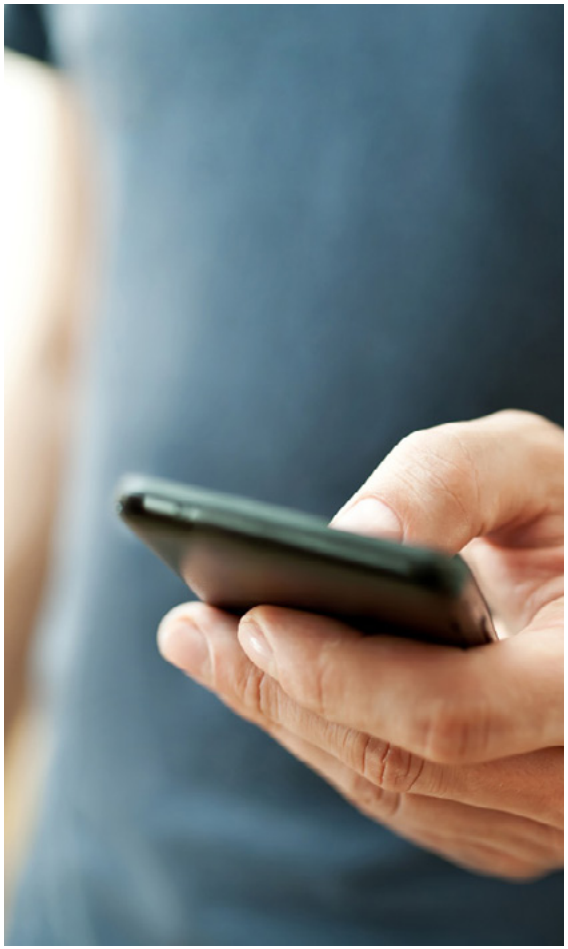
If you're reading this, you probably know that BYOD is already a question of how, not when or if. By the end of 2014, BYOD could reach as much as 80 percent of your workforce and transform your business in ways you may never have imagined. Preparing for this transformation is more than just a matter of security. It's a matter of leveraging the people, processes and tools needed to become a Mobile First organization that's ready to explore a whole new opportunity landscape.

This BYOD guide is a great first step toward achieving your mobile transformation by implementing a successful BYOD program. By following the recommendations in this guide, you can deliver a program that meets the needs and preferences of mobile workers, while upholding corporate security and budget requirements. But the true success of any BYOD program depends on its long-term sustainability, which means you must ensure the security of your corporate data, drive user adoption by supporting employees' device preferences and maintain a flexible technology portfolio that enables business innovation.

BYOD sustainability also depends on effective, ongoing communication with stakeholders and users. Stakeholders have to see that the program supports their goals and users must receive continuous updates about security and device policies to encourage their continued participation.

In short, your BYOD program requires continuous care and feeding to be successful. You need to invest in skilled resources to refine support and maintenance and continually improve self-service and helpdesk guidelines and processes. And you have to be willing and able to adjust policies and processes to adapt to user needs, business growth and changing technologies.

One thing everyone agrees on: BYOD is here to stay. Using the best practices and recommendations outlined in this guide, you can meet even the toughest IT security and management requirements while giving end users a consistently outstanding and productive mobile experience.



FOR MORE INFORMATION

Find out how MobileIron provides the foundation organizations need to achieve the Mobile First transformation by driving innovation, productivity and cost savings across the enterprise. Please visit us at **www.mobileiron.com**.

ABOUT MOBILEIRON

The leader in security and management for mobile apps, content, and devices, MobileIron's mission is to enable organizations around the world to embrace mobility as their primary IT platform in order to transform their businesses and increase their competitiveness. Leading global companies rely on MobileIron's scalable architecture, rapid innovation, and best practices as the foundation for their Mobile First initiatives, including 8 of the top 10 automotive manufacturers, 7 of the top 10 pharmaceutical companies, 5 of the top 10 banks, 5 of the top 10 law firms, and 4 of the top 10 retailers. For more information, please visit

www.mobileiron.com

415 East Middlefield Road
Mountain View, CA 94043 USA
Tel. +1.650.919.8100
Fax +1.650.919.8006
info@mobileiron.com

MobileIron®