FUJITSU

White paper
BYOD – It's About Infrastructure and Policies

Consumerization of IT is inexorably moving forward. IT managers need to consider how they will introduce BYOD (Bring Your Own Device) programs. But what are the pros and cons? Which are the mandatory prerequisites? What should the supporting workplace infrastructure look like? And which other aspects should be considered? The purpose of this whitepaper is to give insight and guidance to technology leaders.

Content

The business world is changing

Historically, people have faced barriers and restrictions imposed on them by the physical world. Long distances and geographical borders between members of a team who need to collaborate and convenient access to information and systems often proved significant obstacles to the efficiency and effectiveness of business initiatives, at times causing them to fail. Today's digital world empowers users and removes such barriers enabling new opportunities and flexibility for everyone. Labor-intensive and time-consuming tasks which were feasible only with huge effort or which were considered almost impossible can be executed in moments.

Flexible working

Speed to market is priority and more important than ever before for an organization to remain competitive and as such businesses are increasingly focusing attention on the productivity of their workforce. Being able to perform work whenever and wherever is a key prerequisite and driver for success and leads to an increased significance in staff engagement and performance.

Today, many workers hold a changing mindset that work is more about what you do and not where you go. Due to this mindset change, organizations now support flexible working models and even encourage their employees to make use of flexibilities in the technical landscape which support such opportunities. The border between work and life is becoming blurred as employees "work-shift" to meet their personal and business commitments in the ever connected and online world. Working practices change constantly as we are faced with organizing work and private tasks irrespective of day or time. Device convergence enables the same device to be used for both tasks providing greater convenience for the user, and the desire to do so is obvious.

Proliferation of devices

At the same time, the number of mobile devices, such as notebooks, but in particular smartphones and tablet systems in various form factors, and with various operating systems platforms is exploding. The increasing majority of users choose to use diverse devices depending on the specific use case.

Analysts and other market experts speak of three devices being used by an individual user during a 24 hour day, e.g. a smartphone that you pack wherever you go for information consumption, a tablet for working while being on the move, and a device with a full keyboard for highly productive working and generating information in the office, at home or somewhere else. And this number is expected to increase in the future.

Digital natives

Every year, more digital natives enter working life. They have grown up in a digital world, constantly connected, and they are used to having access to great and latest technology for their personal life and expect the same from their work environment. But the reality often looks different. They are told to use technology which from their perspective is antiquated, not in the same league as the technology they use at home. These users are highly IT savvy and will naturally evolve towards the same applications, services and devices they use privately, ignoring draconian and outdated IT policies. These new users will find creative ways to do what they intend to do and constantly challenge the control and effectiveness of the IT department.

Consumerization of IT

So, consumer technology – be it devices, applications and even internet services, such as social media or storage services – is now part of enterprise IT. Consumer technology has overtaken business technology as the driver of innovation. That's why people now speak of consumerization of IT. With consumerization occurring beyond the control of the CIO, a shadow IT capability is being built by end users – in parallel to corporate IT.

So how does the CIO react? Should they embrace consumerization and the desires of their end users? Should they contain or perhaps even block them? Or should they simply ignore what is going on? They often come to the conclusion: no matter how they react, they won't be able stop consumerization. Therefore many of them follow the motto: If you can't beat them, join them.

BYOD – The way out?

For this reason, an increasing amount of IT managers try to design strategies to lead consumerization in the right direction by implementing BYOD programs. BYOD stands for "Bring Your Own Device", and actually means that the corporate-owned device is replaced by an employee-owned device of choice, which can be used for both private and business purposes. There are a lot of synonyms out there, such as:

- BYOC (Bring Your Own Computer) or
- BYOPC (Bring Your Own PC) if we are talking about computers,
- BYO-3 (Bring Your Own 3 Devices)
  to express that an individual users uses 3 devices per day,
- BYOA (Bring Your Own Application),
- BYOI (Bring Your Own Information)
  to indicate that we are not just talking about devices,
- BYOT (Bring Your Own Technology) and
- BYO (Bring Your Own) which are often used as umbrella terms including platforms, applications and data.
- And many more.

BYOD – What's in it for whom?

The next logical step after understand the meaning of BYOD is to ask the following questions:

- What are the benefits of
  officially introducing BYOD in an organization?
- What is in it for whom?

Let's take a closer look at three key stakeholders – the end user, the organization in general and the IT department in particular.

Benefits for the end user

Let us start with the end users. This is the group where the pressure for BYOD emanates from. Introducing BYOD means more flexibility for end users; they now have the choice and freedom to use devices for work which fit their preferences, their working styles and their values.

In the past, end users were location dependent, tethered to the organization because their corporate device was a stationary PC, today flexible working are becoming a reality for them. Whether or not flexible working has a positive impact on the work / life balance strongly depends on the individual user. However, BYOD will definitely improve work / life integration. The fact that they can use a single device for both work and life reduces complexity for them, improves user experience, increases satisfaction and engagement.

Benefits for the business

It is not just the user, but also the organization that can take advantage from BYOD. Organizations see themselves in a war for talent. Talent is rare, and in order to be successful in this war and get the talent you need, your organization has to be positively perceived by potential and existing staff. BYOD can positively contribute to the attractiveness of your business and demonstrate that your organization is a great place to work. In the past, one of the most frequently asked questions during job interviews was related to a company car. Today, the working environment and workplace technologies play greater significance.

From companies that have already introduced BYOD, we know that their staff 'work-shift' spending more time working outside of core hours such on weekends and after hours. Overall productivity is improved which is significantly attributed to empowering workers with BYOD. This improves responsiveness to customers, accelerates speed to market, drives innovation, fosters a creative company image and of course delivers that critical competitive advantage.

There are also organizations that are quite happy to reduce their hardware assets and move costs from their balance sheets. Can BYOD deliver cost savings is a question which is rather difficult to answer. This will strongly depend on the policies and the agreements with your employees, discussed later in this whitepaper. The policies must be geared to the goals the organization wants to achieve. If cost reduction is the primary goal, there are ways to achieve this goal. Nevertheless, it might be questionable whether the end users will be happy and satisfied, which is an important prerequisite for highest levels of productivity. If high end user satisfaction is the primary goal, it is questionable whether there will be significant cost reductions.

When talking about costs, it also matters what you include. There are companies spending an enormous amount of money for the premises supporting their employees. If they take BYOD as an opportunity to let a significant percentage of their employees work from home, thus being able to reduce their office real estate, the cost savings can be huge.

And finally, as users care more about the devices they own, statistics show that fewer devices get lost or damaged.

Benefits for the IT department

And what is the benefit for the IT department? Due to ever shorter lifecycles, the proliferation of devices in a company the IT department has to look after is ever increasing, along with a proliferation of spare parts and drivers they have to deal with. This makes lifecycle management very complex and difficult. Considering the fact that devices are often seen as non-strategic assets, BYOD is an opportunity to relieve the IT department from the lifecycle management for these non-strategic assets.

With greater knowledge of their own devices, less user training is needed, and less support calls can be expected to the Service Desk. The IT department escapes the frequent complaints from the end users about the age and poor performance of corporate provided technology.

BYOD truly offers a highly effective vehicle for IT departments to focus on the really strategic projects that deliver innovation and a competitive advantage to the firm's marketplace.

Challenges for IT

So, BYOD can be a win-win-win situation for everyone - for the end user, the business and the IT department. But wait - there are also some challenges, especially related to manageability and security. Here are only some of the typical frequently questions asked:

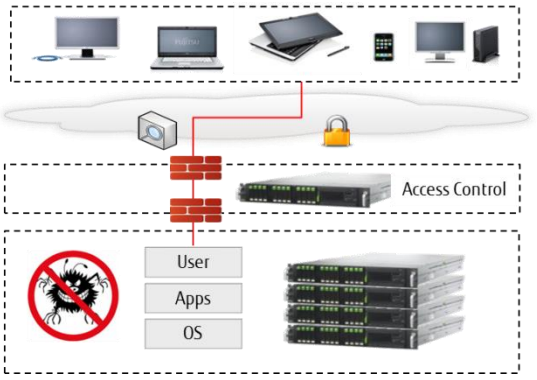
- How to install and use applications if the operating systems are different?
- How to deal with the proliferation of devices and configurations?
- Who takes care of hardware, software, data, and support?
- What if a device fails?
- How to keep control?
- How to protect corporate data from corruption, misuse or theft?
- How to enforce security policies without compromising ease of use?
- How to meet compliance demands of the business?

Because of these challenges, BYOD is often seen as complex, dangerous and expensive. End users may share similar concerns as well about how to protect their private data and activities from their employer.

How to mitigate the headaches caused by BYOD? As so often, there is no silver bullet. In the following sections, we are going to discuss what needs to be taken into consideration.

Virtualization and centralization

From an infrastructure perspective, it is obvious that a traditional workplace approach with a strong interdependency of hardware, operating system, applications and user environment is not suitable. Virtualization makes the individual components independent from each other and allows IT to move applications, data, and the client environment from the device into the data center. With everything in the data center, the user device will simply access services securely in the data center. The only thing you need on the device is a virtualization client or even just a browser. As virtualization clients and web browsers, from the major vendors, run on basically any device or platform, a centralization approach is device agnostic.



By having corporate applications and data moved to the data center, we have achieved separation of business and personal services. Management is simplified, focus is no longer on the device but on the user and the corporate applications and data they consume. Applications can easily be deployed and updated, and patches become effective without touching thousands of end user devices and disrupting the business. The level of application, data and workplace availability is significantly increased; even disaster recovery concepts can be applied, enabling business continuity.

With all data hosted in the data center, the risk of data leakage is minimized. This is enabled through encrypted communication between the device and data center, firewalls and role-based access control to the client, applications and data in front of the data center, and anti-malware running in the data center. Data backup no longer depends on whether the device is turned on or whether it is connected, thus minimizing data security risks and simplifying compliance demands.

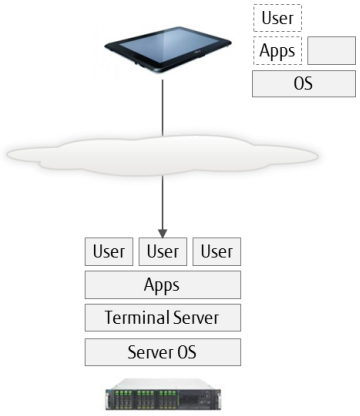
Centralization also enables end users to access their applications and data anywhere from any device, i.e. applications and data follow the user, while the user no longer has to follow the device. This allows adaptability to the trend of an ever increasing number of devices used by an individual.

Workplace delivery options

When it comes to centralization, again there are many answers. These depend largely on the role and work-practices of the different organization stakeholder groups.

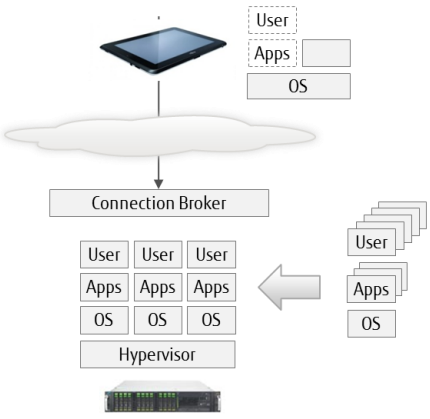
Hosted Shared Desktop

For the task workers who use only the same limited set of applications every day, the Hosted Shared Desktop with applications shared among several users running on a terminal server, is sufficient and provides a very low TCO (Total Cost of Ownership). But its restrictions – multi-user capable applications, limited individuality and separation from other users - don't make it applicable for real knowledge workers who need highest flexibility and individuality.



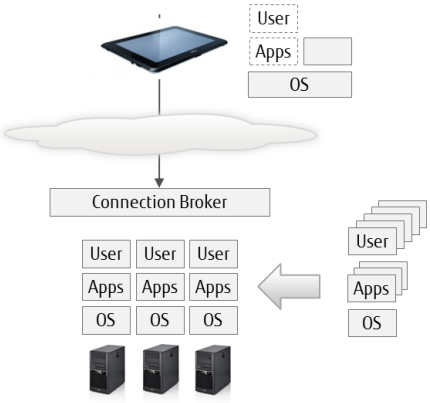
Hosted Virtual Desktop

For knowledge workers the Hosted Virtual Desktop (also known as VDI or Virtual Desktop Infrastructure) is the appropriate choice. Individual desktops with different types and versions of operating systems run as virtual machines on servers in the data center. They are isolated, and therefore fully protected from each other. They can be personalized to fit personal needs. And in contrast to "Hosted Shared Desktop", applications need not be adapted.



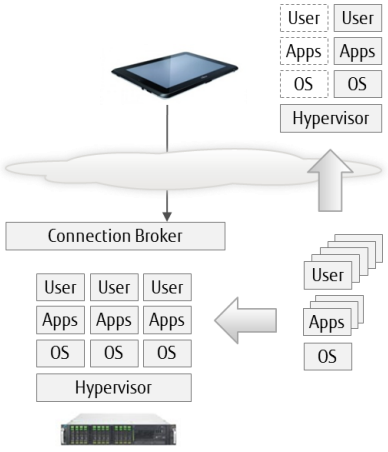
Central Hosted Desktop

If centralization is demanded for power users with extremely high demands in terms of graphics performance, the Central Hosted Desktop with graphics workstations in the data center may be an option.



Local Virtual Desktop

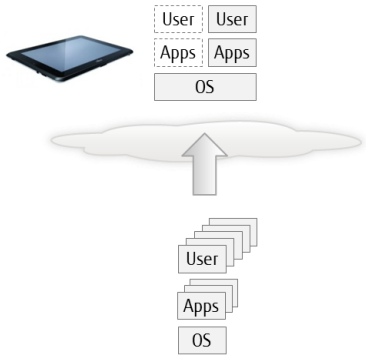
All delivery options discussed by now require a connection from the access device to the data center. By means of the Local Virtual Desktop even mobile users, can be accommodated, who occasionally have no network connection, but want to work offline. A hypervisor running on their local device enables them to use exactly the same virtual desktop locally which is centrally used in a Hosted Virtual Desktop scenario. For the IT department this means that they can manage these mobile users in exactly the same way as stationary workers. The virtual desktop is streamed from a central image to the mobile device. All work done offline will only have an impact on your local copy. As immediately when connected to the corporate network, your updates will automatically be synchronized with your virtual desktop environment in the data center, as are system updates and patches that affect your local virtual desktop. The synchronization eliminates the need to backup mobile devices, and the automatic update ensures that users always work with the latest software versions and security patches.



Virtual desktops are encrypted and fully isolated from each other and the private host environment. Additional security is provided by allowing policies to be put in place. For example, if a device hasn't re-connected to the corporate network for a certain period of time, the image will lock itself down. Likewise, data leakage can be prevented by disabling printing or access to local disk drives and USB storage. If the device gets lost or stolen, the corporate virtual desktop can be remotely wiped.

Local Streamed Applications

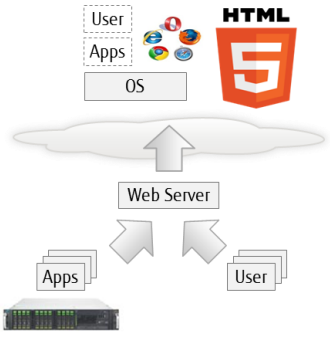
An alternative for offline usage is Local Streamed Applications. Business applications are streamed to the mobile device where they run in a "sandbox". Data used or generated by the applications can be totally isolated and separated from what else is on the device.



Web Desktop

In the last couple of years the Web has become the main workspace for many end users. More and more of the applications needed are web-based, or at least accessible through the web. The Web Desktop becomes the aggregator for these applications. For accessing web-based applications, an HTML5 compatible browser is sufficient, available on any device, no matter what operating system used.

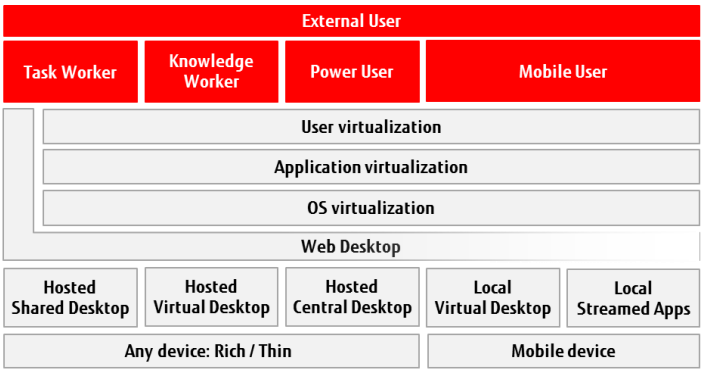
The degree of applicability of a web desktop is certainly the highest for task workers; however, knowledge workers and at a certain extent even power users can take advantage from a web desktop. This is true for stationary users and mobile users being online. Due to local caching features, minor disruptions to connectivity can be bypassed. Mobile users that are without network connection for long periods of time may be better seeking an alternative solution.



One size does not fit all

There are many types of end users each with different requirements in every organization. The optimum solution for the organization will mostly be a blended solution, i.e. it is rather a "mix and match" than a "one-size-fits-all" approach. With all concepts presented, it makes no difference whether a user is an employee of the organization or an external user, such as a guest or a contractor.

The figure below shows the user types, typical workplace delivery options including virtualization of user personality, applications and operating system images, and the typical devices used by the individual types of end users.



USB flash drive for business work

A supplementary option worth mentioning is the usage of a USB flash drive for business work, sometimes also denoted as "PC on a stick". Mobile users take a USB stick with encrypted content with them, which they can attach to an appropriate host device.

USB flash drive solutions can occur in various shapes. As soon as the client software is started, it is ready for the end user to login. Once logged on, a connection is established between the device and the user's Hosted Shared Desktop or Hosted Virtual Desktop. The secure client runs in an encrypted sandbox and does not leave any footprint on the host device. Due to its isolation from the host system the solution has inherent benefits such as reducing threats to the corporate network from viruses.

Administrators can also define whether access to printers and storage drives attached to the host device is allowed or restricted. In the same way, the transfer of clipboard data between virtual desktop and host system can be controlled. Most of the existing solutions are bound to a certain operating system on the private device, usually Microsoft Windows.

For offline usage, a full virtual desktop environment with an operating system and all corporate applications and data, can be stored on the USB stick. If there is a hypervisor on the host device, the virtual desktop from the USB stick can run on the hypervisor. Most currently available type-2 hypervisors require Microsoft Windows as operating system. Data is directly updated locally on the USB stick. A backup is conducted when there is a connection to the data center, either automatically or manually.

Alternatively, a complete standard operating systems image with corporate applications can be deposited on the USB stick and booted up from the start on the private device. This function (Windows To Go) is included in Microsoft Windows 8 Enterprise, and requires the respective hardware compatibility. The booted system runs fully isolated from what else might be on the host device, but can take full advantage of the host capabilities, e.g. Wi-Fi, video card, webcam, attached printers and other. Nothing needs to be installed on a host device, and the booted system will not leave any data footprint on the device. However, it is questionable if this approach makes end users really happy, because switching between private and business tasks would always require a system boot.

In both cases with offline usage option, corporate data is encapsulated and therefore separated from the host device.

The new formula: EMM = MDM + MAM + MIM + TEM

While directly accessing the web, devices can become infected by malware exploiting vulnerabilities, looking to exploit securities holes in other systems or business-related containers on the private device. It is true that in all of the delivery options discussed, there are solutions in place that protect corporate applications and data. However, it is likely that the attempted attacks will generate traffic and load on your network and use significant system resources of the device itself. This in turn could have a negative impact on end user productivity.

This can be significantly reduced by having anti-virus / anti-malware software installed on the device. By using a Mobile Device Management (MDM) solution, all necessary security software, but also other software such as the virtualization client, can be provisioned, monitored and regularly updated over the air without bothering the end user.

The MDM can be used to enforce device passwords, application black or white lists, jailbreak and rooting detection and remote wiping of all critical contents in the event of device theft or loss. MDM helps IT organizations efficiently manage mobile devices on a level which is needed to meet regulatory compliance, without impacting end user productivity.

Certainly more important than having a defined level of control over the end user's devices is the control over corporate applications and data. This is what experts denote as Mobile Application Management (MAM) and Mobile Information Management (MIM). By the separation of business-related content from private content on the device, business content can be secured and controlled without having to interact or interfere with private content. For instance, business emails and attachments can be restricted from being emailed via personal email accounts.

MAM and MIM include automated enforcement of usage policies based on factors such as device type, type of network and user. If needed, a selective lock and wipe can be performed without impacting the user's personal data. Enforcing a password for the container could - from a company perspective - even make the device password superfluous. This might improve the user experience and acceptance in many cases, as not every user is happy, if the smartphone needs to be unlocked every the user wants to take a picture.

Together with Telecom Expenses Management (TEM) used for managing connectivity, data volumes and time in order to optimize communication costs, MDM, MAM and MIM are important building blocks of a comprehensive Enterprise Mobile Management (EMM) solution which today's modern enterprises need to implement.

BYOD requires well-defined policies

We have seen that BYOD requires an appropriate foundation which minimizes business risks. However, BYOD is not just about infrastructure. There are various aspects which must be considered, decided upon and included in business policies.

The first aspect is scope and eligibility. It should be clear to employees what options are available to them, is the organization moving towards employee-owned devices being the only option, or is the company-owned device option to be maintained? – If BYOD is to be embraced, is it subsidized and will all employees be encouraged to adopt it in some form. Bear in mind that not all employees will want to BYOD. If the user has the choice: will there be a revocation option, once he has taken a decision? Is every user allowed to join the program? Or do you make a difference between users depending on their role, title, seniority, geography or the sensitiveness of the data they produce or consume? Will employee-owned devices replace corporate devices, or is it just a supplement? How does the approval process look like? How to deal with new employees?

To be able to run corporate applications at a sufficient performance, minimum configurations in terms of hardware, software, network capabilities, accessories and other technical prerequisites should be defined. It is quite likely that this will have to be updated frequently. You will also need to provide clarity whether you allow any device, any form factor and operating systems platform, or if you limit them.

An important topic is license implications. Can corporate licenses be used on a private asset? Does it make a difference, if you use the software on-premise or off-premise? How many devices may be used? Is there a need to change the license model? Is the parallel use of a software product for private and business purposes allowed? Is everything procured by the organization and what has to be self-procured by the user? Unfortunately, these questions will always depend on the individual software and the respective vendor.

Is also recommended that you specify whether you will allow private applications to be used for business purposes, or whether using applications from the corporate virtual environment is mandatory for business purposes, even if from a functional point of view, applications in the private environment can deliver the same result.

And what about using private applications in the corporate network? Do you allow, do you limit or even forbid it? Allowing it can cause an increased network traffic which in turn could cause extra investments. And besides, you would quasi act as an internet service provider for your employees, with all duties an internet service provider is subject to, as for instance keeping all connection data for a certain period of time.

Although the previously discussed infrastructure options in combination with Mobile Application Management, Mobile Information Management and Mobile Device Management ensure a high level of security and minimize business risks, security demands are an essential part of the BYOD policy work. Amongst others, you will define which anti-malware to use on the device, if the malware scan should be executed automatically in certain time intervals, or if it needs to be initiated manually by the end user. You will define the rules for the device password or container password. You will decide whether and how private devices have to be registered, before they can be used for work. You will decide on possible access limitations to applications and data depending on devices, users, network, location and time. And it should be clear who has to do what, when a device is infected, when it is lost or stolen, when the users change their role, when they replace their device, or when their carrier contract is terminated. At the same time, you should not lose track of the privacy of the user's private data and applications.

The challenge when defining the security policy is to find the right balance between security and ease of use. Too many restrictions compromise user experience, limit user productivity, decrease the attractiveness of BYOD, and will increasingly burden the IT department because creative users will always find workarounds.

Support guidelines should sort out who is in charge of supporting what. The focus of the IT department will certainly be the user profile, corporate applications and data, but not the device. Will users get device support? Will you insist on a support contract with any 3rd party service provider? Will you even nominate one? Or is device support up to the employee? Do you want to promote community support by establishing a platform for sharing experiences and information? What if a device is damaged or stolen? What is the maximum disruption time you will tolerate? Is there a loan pool in the organization where users can procure a spare device? Or will they have to work in the office using tethered devices?

If you want to encourage your employees to use BYOD or if it is the one and only option, your employees may expect reimbursement. But here again, several questions have to be clarified. Which users may join the stipend program? May they join the program any time, or only when their corporate device has reached end-of-life? Which employee-owned devices are subsidized, in which frequency? Is it a fixed amount for all members of the stipend program, or from which parameters does the amount depend? Is the stipend paid as a one-time allowance or per month? Will there be a prorated payback, if an employee quits the company after he has got the one-time allowance before? Which services are covered? If communication costs are covered: will they be covered fully or partially? Will you cap the amount you will pay?

Depending on your country, there may be tax implications, such as depreciation, income-related expenses or other monetary benefits you should be familiar with. It will make no sense if you pay a considerable amount of money to the employee but they will be required to forward a major component of this to the tax authorities.

One of the most difficult dimensions of BYOD is the legal aspect. Imagine there is an internal security investigation or discovery for a lawsuit, for which you need to access the employee-owned device. An agreement with the employee that you can request the surrender of the device to IT in such a situation should be a prerequisite for the participation in a BYOD program. Similar to this, there should be a claim for getting a copy of business-related data if this data is exclusively stored on the device, and the employee is on annual leave or sick, or his contract is terminated. But be aware that you always have to ensure the privacy of the user's non-corporate data, applications and activities.

Another legal aspect is liability. To demonstrate the broad scope of what needs to be considered and correspondingly agreed, we are going to demonstrate some of the questions that may require intensive discussion:

- Who is liable for the device in case of damage or theft?
- In which situation can the employee claim for compensation?
- Is there a difference, if the device is stolen or damaged at home, on company premises, or during a business trip?
- Will there be an individual lump-sum, or will the value of damage or loss be exactly evaluated?
- What if culpable negligence by the end user can be proved?
- Is it a duty of care violation, if e.g. the device is left in car?

Defining the answers beforehand can help avoid potential litigation. If possible, you should disclaim the company's liability for the loss of private applications and data, and advise the employee of his responsibility for the backup of personal content.

BYOD should be implemented with clear rules and policies covering all of these varying aspects. But what if it comes to a policy violation, because employees do not stick to the rules?

- Will the employee be counseled?
- Will you stop the payment for the employee?
- Will you claim for compensation?
- Will you terminate employment?
- Will you remove the employee from the BYOD program?

When prosecuting misuse, it is important and necessary to consider civil law and criminal law related problems.

Some of the policies require the agreement by the workers council, which is of course also different from country to country.

While defining the BYOD policies, it is recommendable to take existing policies and compliance demands into consideration. In addition, you should not neglect to undergo a risk and insurance assessment. Going for BYOD will create new risks and require changes to insurance policies. Ensure that the company insurer is aware of the change in working practices.

BYOD involves all parts of the business

Having all policies in place, communication to the employees is essential. Your staff has to be aware of all the options and restrictions, responsibilities, duties and consequences. To help users understand the risks and benefits, and to underline the importance of data protection, training sessions can be helpful.

This means, that BYOD involves basically all parts of the business: the IT organization, Human Resources, the Legal department, finance, corporate communications, training and the worker's council. Without the contribution of all stakeholder groups, BYOD may not realize the full benefits intended by the organization.

Company-owned devices and private use

There are IT managers who understand the advantage of dual-use devices for work and life, but their organization wants to keep on owning the devices, giving them exclusive control over the devices. Due to better control, it is easier for the organization to ensure protection from attacks, espionage and malware, and to enforce security policies.

This brings an alternative model into the game: CYOD (Choose Your Own Device). Company-owned devices which may be used privately are an alternative and viable way, if the basic conditions are fulfilled. Meeting the requirements of the end users is certainly most important. In essence, you should offer support for a broad selection of innovative devices and form factors which enables them not only to run the latest versions of the software they need for the business, but also enable them to run private applications.

By CYOD, similar objectives can be achieved as with BYOD. And if the basic conditions suit, company-owned devices which may officially be used for private purposes will also contribute to making your organization more attractive and competitive in the war for talent. In addition, the organization can take advantage from the same discounts for communication services as in the past. At the end of the day, much less policy work needs to be done, because there is more safety and clarity regarding laws, the ownership structure and the authority to give directives to the employees.

However, a few challenges remain. When going for CYOD, you will also be bound to have policies in place determining what software is usable for which purpose, especially whether you allow private applications to be used within the corporate network and how personal data is to be treated.

How Fujitsu can help

Transforming the workplace into a shape that supports BYOD considering all accompanying current and future trends which add value is for sure an exciting journey for the customer. However, such a journey can be extremely long, costly and full of risks and traps.

Fujitsu's approach to BYOD is to accompany you on this journey and optimize the duration and risks by avoiding the potential traps and overcoming the hurdles you may be faced with.

No matter how the customer's workplace strategy will look like, no matter which concepts, workplace delivery options and technologies are ideally suited for the customer's specific objectives, Fujitsu will provide a complete and optimum desktop virtualization solution from a single source, usually as a mix of various concepts.

Global partnerships with prominent market leaders, such as Citrix, Microsoft and VMware enable us to use best in class virtualization software and other technologies to optimize the overall solution. Fujitsu provides the respective licenses, the subscription advantage and the support.

Fujitsu's infrastructure products for the data center, such as Fujitsu PRIMERGY servers and Fujitsu ETERNUS storage systems, are certified for all market-leading virtualization products, have proven success in innumerable virtualization projects, and therefore represent an excellent basis for this purpose. A number of PRIMEFLEX integrated systems including hyper-converged systems especially designed for virtualization simplify and accelerate deployment, minimize risk, reduce costs and increase operational efficiency.

Through all our activities in real-life projects and globally significant end user transformation programs, we have gained experience as to what is required to successfully introduce desktop virtualization and mobility solutions. This broad knowledge of optimizing solutions for specific customer requirements is reflected in our services, comprising consulting, the design and the implementation of the new infrastructure, along with the integration services and the migration from the current environment into the new world. Likewise, Fujitsu provides maintenance and support, end-to-end with a single point of contact for the entire infrastructure solution, helping avoid the typical finger-pointing when ingredients originate from different vendors. For international or global companies, these services can even be delivered consistently across borders.

Not every customer has budget available to invest in a desktop virtualization project upfront, despite wanting to take advantage of the benefits it provides. Fujitsu Financial Services, the IT leasing and financing arm of our business, provides a multitude of solutions that can help overcome initial capital expenditure blocking points. By shifting fixed costs into variable costs, we allow our customers to maximize their operating budgets. This increases their flexibility, and allows them to maneuver within their budgets.

If IT organizations want to be free to concentrate on their core business and strategic projects rather than daily routine tasks, Fujitsu will manage the customer's workplace infrastructure, based on standardized and optimized processes. Customers can take advantage of Fujitsu's economies of scale, the simple opportunity to alleviate shortages in resources and skills, flexible customer-specific and business-related service levels, and cost reductions. "Price-per-user" cloud based charging models eliminates investment risks and ensures highest cost transparency. At the same time, customers keep their IT infrastructure fully under control.

Furthermore, Fujitsu's Virtual Workplace Services can be delivered via true cloud based delivery models, as easily as electricity from the socket or water from the tap, allowing you to scale services up and down as your business and market conditions dictate. A "pay-as-you-use" model is the basis for billing, turning CAPEX to OPEX, and delivering an optimized TCO.

Fujitsu's Managed Mobile is a complete service for managing and supporting mobile devices, applications and data across multiple platforms. It is designed to increase personal productivity, collaboration and overall efficiency, whilst minimizing security risks.

However, we should not forget the devices, although in the context of BYOD they might play a minor role for businesses. Fujitsu is in a position of strength when it comes to workplace and mobile end user technologies as our current hardware portfolio includes all device form factors required for the evolving needs of the workplace. For the access to centralized virtual desktops, Fujitsu FUTRO Thin Clients are the products of choice. Mobile users will of course go for Fujitsu LIFEBOOK notebooks, Fujitsu STYLISTIC slate PCs and smartphones. And if for certain use cases desktops or powerful workstations are needed, Fujitsu can also assist with its Fujitsu ESPRIMO PCs and Fujitsu CELSIUS workstations.

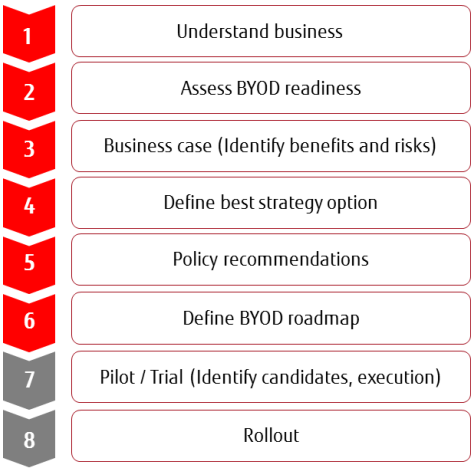
Fujitsu's client computing devices are perfectly suited for business and private purposes, i.e. for work and private life. BYOD-optimized frame agreements between your organization and Fujitsu let your employees benefit from our leading edge workplace systems and technologies at attractive rates. With or without such frame agreements, ordering by your employees happens through an easy-to-use online portal. To add value for your employees, the devices offered can be bundled with accessories, software, and services.

If you decide to go for CYOD, expanding your devices portfolio by client computing devices from Fujitsu will certainly attract many of your employees.

In a nutshell: Fujitsu is a one-stop shop that provides everything you need for BYOD from a single source. This helps reduce complexity, implementation time and risk. Moreover, Fujitsu gives its customers all the flexibility they need to select the most appropriate sourcing option or combination.

The first step: BYOD Assessment

To simplify the first step of the journey to BYOD, Fujitsu has developed a standardized service called BYOD Assessment. The approach is a cross-organizational engagement. Through tool-based interviews with business leaders, a broad mix of users, and business unit representatives, Human Resources, IT, Finance and the legal department, Fujitsu's consultants get a deeper understanding of the business, enabling them to assess the BYOD readiness in terms of company structure, management culture and technology.



Based on this information, benefits and risks can be identified, and the business case can be developed, considering the associated infrastructure changes. Together with the customer, the best strategy option is defined. Based on Fujitsu's experience, policy recommendations are given, and the BYOD roadmap is jointly defined.

The benefits for the customer are evident: He will be guided to an optimal solution which is specific to his needs; he will have a clear understanding of the business value and get the business justification. As depending on the stakeholder's availability, the BYOD Assessment can be completed within 3 to 4 weeks, you will shorten time to BYOD tremendously while reducing risk.

After the BYOD assessment, Fujitsu will provide on-demand support during the pilot phase with selected early adopters. The pilot program serves for determining the effects on productivity, working practices and whether the perceived security risks and manageability concerns are real.

Of course, Fujitsu will support end users during the rollout. Ideal candidates in the initial phase include business partners, external consultants, new hires, mobile workers and home-based workers.

Summary

The consumerization of enterprise IT is a serious issue for CIOs that cannot be ignored and will not stop. BYOD can be the solution, but it brings its own challenges around security and manageability. Desktop virtualization helps separate corporate applications and data from the device, thus mitigating many of the challenges facing CIO's.

But BYOD is not just about infrastructure; it is also about policies whose definition requires the involvement of all parts of the organization. Fujitsu offers a broad range of End User Services designed to enable your users effectively work in a world where our business and personal lives are increasingly blurred, thus making BYOD a success.

Contact
FUJITSU Technology Solutions GmbH
Address: Mies-van-der-Rohe-Strasse 8
80807 Munich, Germany
Website: www.fujitsu.com/global/vdi
2018-03-09 WW/EN