FUJITSU

White paper
BYOD – It's About Infrastructure and Policies

Consumerization of IT is inexorably moving forward. This makes more and more IT managers think about introducing BYOD (Bring Your Own Device) programs. But what are the pros and cons? Which are the mandatory prerequisites? And how should the workplace infrastructure look like? And which other aspects should be considered? This whitepaper will give some guidance.

Content

The business world is changing

For ages, people had to accept barriers and restrictions imposed by the physical world. Long distances and geographical borders between members of a team, who had to collaborate, often proved as an obstacle which protracted projects enormously or even had them failed. The digital world, in which we live today, removes these barriers, thus providing innumerous new opportunities for everyone.

Especially regarding business efficiency the world changes dramatically. Labor-intensive and time-consuming tasks which were feasible with highest efforts only, or which were sometimes perceived as almost impossible, can be executed in the twinkling of an eye.

Flexible working

As time and speed are more important than ever before to be competitive, organizations set their strong focus on the productivity of their workforce. Being able to do your job anywhere and anytime is a key prerequisite for success and leads to an increased significance of mobility.

People understand that work is something what you do, and not where you go. Due to this mind change, organizations support flexible working models and even encourage their employees to make use of such opportunities. Therefore the borders between work and life blur, because people are faced with a mix of work and private tasks. Using the same device or both tasks for both tasks means more 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. More and more users even use diverse devices depending on the specific use case. Analysts and other market experts speak of 3 devices being used by an individual user during a 24 hours 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 even seems to increase in the future.

Digital natives

Every year, more digital natives enter working life. They have grown up in a digital world, 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 devices which from their perspective do not play in the same league as what they are used to have. Therefore they try everything to use the same applications and devices they are using privately also for business purposes. Often it makes no difference to them, if they are allowed to do so, or if they are not. Anyhow most of them will find a creative way to do what they intend to do, beyond the control of the IT department.

Consumerization of IT

In this way, consumer technology – be it devices, operating system platforms and even applications, such as social media or any open source – migrates into the enterprise. Consumer technology has overtaken business technology as the driver of innovation. That's why people speak of consumerization of IT.

If consumerization happens beyond the control of the IT department, a kind of shadow IT is built by the end users – in parallel to corporate IT.

The exciting question is now, how the corporate IT will react. Should they embrace the end user's desire? Should they contain or even block it? Or should they just 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, more and more IT managers try to design strategies to lead consumerization into 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 concurrently be used for private and business purposes. There are a lot of synonyms out there, as for instance:

- 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?

After having discussed the meaning of BYOD, we are turning towards the questions:

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

We are going to have a closer look at three 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 usually the pressure comes from. Introducing BYOD means more flexibility for them, they have now the choice and freedom to use devices for work which fit to their preferences, their working styles and their habits.

If they were not able to work location-independent in the past, because their corporate device was a stationary PC, flexible working becomes reality for them. Whether or not flexible working has a positive impact on the work / life balance, strongly depends on the individual user – there are many examples showing that work / life balance can be negatively impacted, especially if the employee is prone to be a workaholic. 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 and increases satisfaction.

Benefits for the business

It is not just the user, but also the organization in general that can take advantage from BYOD. Organizations see themselves often in a war for talents. Talents are rare, and in order to be successful in this war and get the talents you want, your organization has to be attractive for recruiting and retention. BYOD obviously contributes to an increased attractiveness. While in some countries one of the most frequently asked question in job interviews was related to a company car in the past, the working environment and the working equipment seems to have a much higher significance today.

From companies that have already introduced BYOD, we know that their staff is doing more work on weekends and after hours. As this additional work is not paid by the company, it is free hours that helps increase the overall productivity. This accelerates responses to your customers, opens up more business opportunities, drives innovation and adds to a creative company image and of course to competitive advantages.

There are organizations that are quite happy if they can reduce their hardware assets and get them off their balance sheets. If BYOD can lead to cost reduction, is a question which is rather difficult to answer. This will strongly depend on the policies and the agreements with your employees, which will be discussed later in this whitepaper. The policies in turn will be geared to the goal the organization wants to achieve. If cost reduction is the primary goal, there will be 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 productivity. If highest end user satisfaction is the primary goal, it is questionable whether there will be a significant cost reduction.

When talking about costs, it also matters what you add to the equation. There are companies paying an enormous amount of money for the office area of many thousands of 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 evidently better care about 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, and along with that also the 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.

As the end users know their own devices, less end user training is needed, and less support calls can be expected. Besides this, the IT department escapes the frequent complaints from the end users about age and poor performance. They can even observe how latest technology is adopted at the speed of the consumer market.

All the reliefs mentioned will enable the IT department to focus on the really strategic projects that bring the company hopefully ahead.

Challenges for IT

At the first glance it might look as if BYOD can be a win-win situation for everyone - for the end user, the IT department and the business. But there are also some challenges, especially related to manageability and security. Here are only some of the typical frequently questions asked:

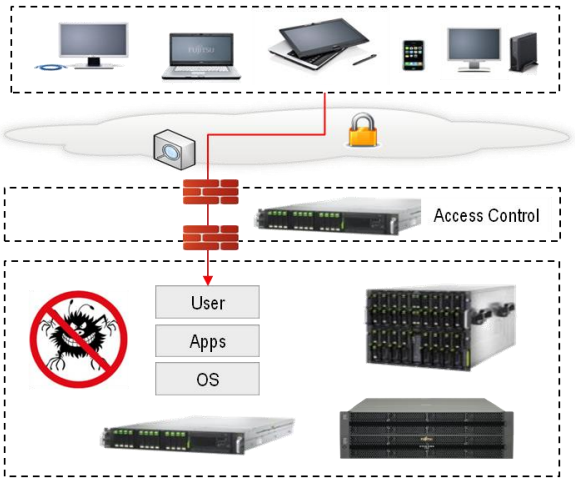
- How to install and use applications, if the operating system or operating system versions are different?
- How to deal with the proliferation of devices and configurations?
- Who takes care of hardware, software, data, and support?
- What if a device fails?
- How to keep control?
- How to protect corporate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

Due to all these challenges, BYOD is often seen as complex, dangerous and expensive. And by the way, the end users might have similar concerns as well, how to protect their private sphere and activities from their employer.

How to mitigate the headaches caused by BYOD? As so often, there is not just a single answer. 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. However, virtualization makes the individual components independent from each other and gives IT all the options to move applications, data, the user environment or even entire workplace environments from the device into the data center. If everything else is in the data center, the user device will just serve for the access to the data center. The only thing you need on the device is a virtualization client or just a browser. As the virtualization clients from the major vendors and also web browsers run on basically any device platform, a centralization approach is device-agnostic.



By having corporate applications and data in the data center, we have already achieved a separation of the business from the private environment. Management is simplified for the IT department, as their focus is no longer on the device, but just on the corporate applications and data over which they have full control, Software can easily be deployed and updated, and patches become effective without touching end user devices and disrupting the end user. The level of application and workplace availability is significantly increased; even disaster recovery concepts can be applied.

The fact that all data is hosted in the data center minimizes the risk of data theft. This is ensured by an encrypted communication through a virtual private network tunnel between device and data center, firewalls and a granular role-based access control to desktops, 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 the risk of data loss. This helps fully meet compliance demands.

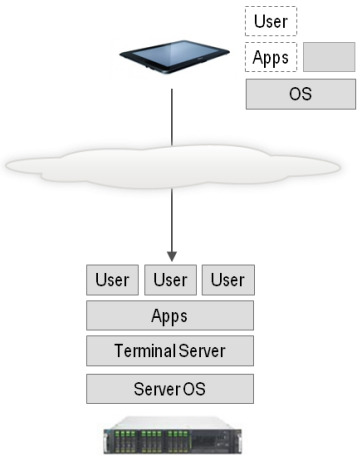
Centralization enables end users to access their applications and data anywhere from any device, i.e. applications and data follow the user, while the user no longer has to follow the device. This plays to the trend of an ever increasing number of devices used by an individual.

Workplace delivery options

When it comes to centralization, there is not just one optimum concept for every situation. User types, their requirements and economic aspects matter.

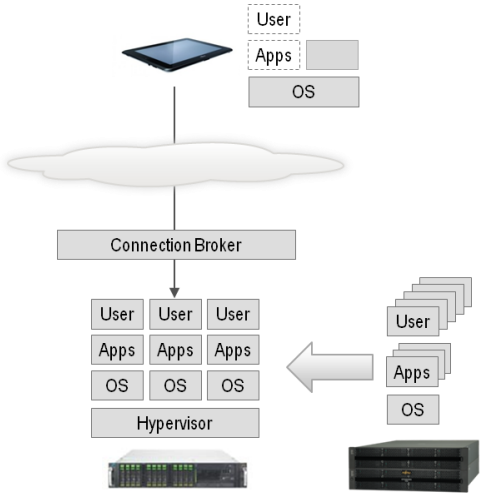
Hosted Shared Desktop

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 absolutely 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.



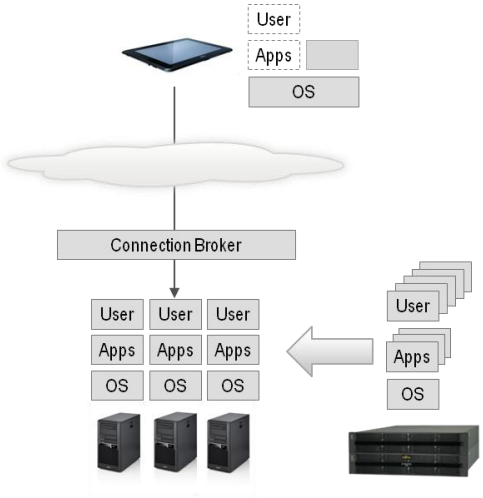
Hosted Virtual Desktop

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.



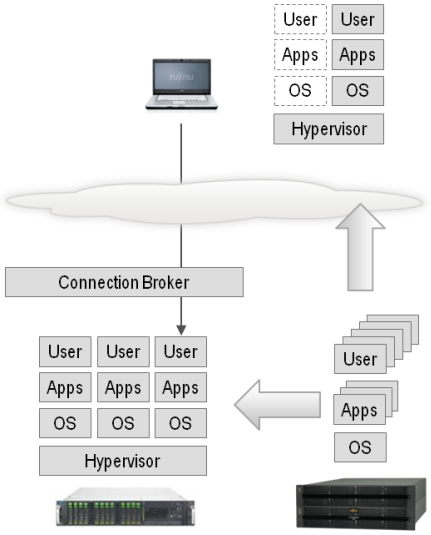
Central Hosted Desktop

If centralization is demanded for power users with extremely high demands in terms of graphics performance, it is mostly the Central Hosted Desktop with graphics workstations in the data center that represents the only useful alternative.



Local Virtual Desktop

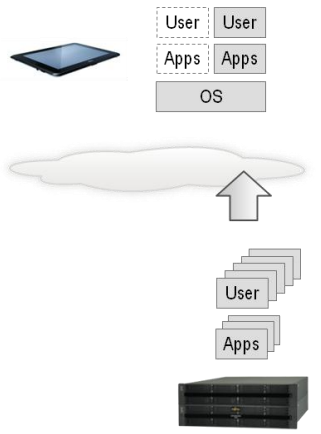
All delivery options discussed by now require a connection from the access device to the data center. By means of the Local Virtual Desktop even mobile users can be involved who occasionally have no network connection, but want to work offline. A hypervisor running on their local device enables them 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 the stationary workers. The virtual desktop is once delivered from a central image to the mobile device. All work done offline will only have an impact on your local copy. As soon as you get connected to the corporate network, your updates will automatically be synchronized with your virtual desktop environment in the data center, as system updates and patches will 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.

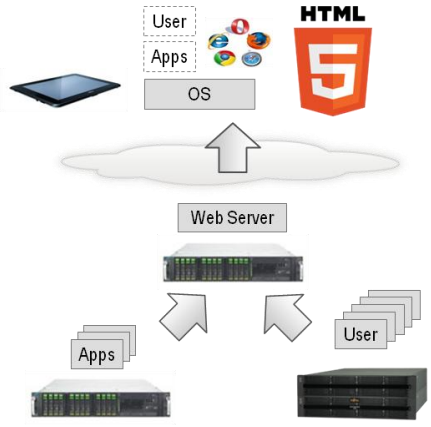
Local Streamed Applications

An alternative for offline usage is Local Streamed Applications. Business applications are once downloaded to the mobile device where they will run in a sandbox. Data used or generated by the applications can be totally isolated and separated from what else is on the device. For the rest, all security mechanisms known from the Local Virtual Desktop, such as data encryption, enforcement of policies and remote wipe are also available.



Web Desktop

In the last couple of years the Web has become the main workspace for many users. More and more of the applications needed to do their job 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, which will be available on any device, no matter which operating system is deployed.

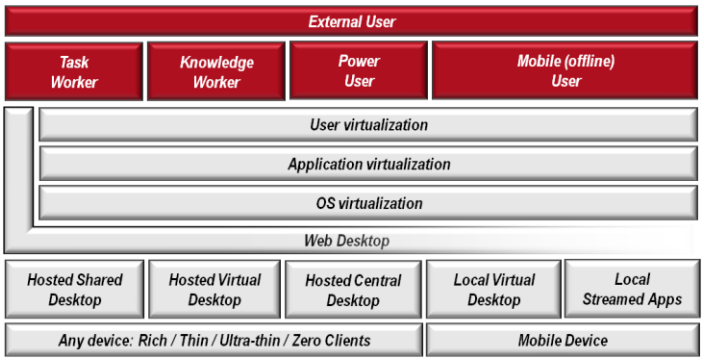


The degree of applicability of a web desktop is certainly the highest for task workers; however, knowledge workers and at a certain extent even power users can take advantage from a web desktop. This is true for stationary users and mobile users being online. Due to the local caching feature, minor disruptions of the connection can be bypassed. Just in case the mobile users have no network connection for any length of time, this might not be the optimum approach for them, yet.

One size does not fit all

As there are usually various types of end users with different requirements in every organization, the optimum solution for the organization will mostly be a mix of various concepts, i.e. it is rather a "mix and match" approach 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 contract worker.

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.

Such USB flash drive solutions can occur in various shapes. In a first variation, the USB stick contains a **secure client for remote connection**. As soon as the client software is started, it is waiting for an end user login. After login, a connection will be established between the private 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, it will not infect the corporate network with viruses, no matter how much infected the host system might be.

Administrators can 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 operating system and all corporate applications and data needed, can be stored on the USB stick. If there is the respective hypervisor on the host device, the virtual desktop from the USB stick can run on the hypervisor. Most currently available type-2 hypervisors require again Microsoft Windows as operating system underneath. 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 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 get infected by malware exploiting vulnerabilities, then looking for further securities holes in other systems or the business-related containers on the private device. It is true, that for all delivery options discussed before, there are solutions in place that protect corporate applications and data. However, it is rather likely that the attempted attacks 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 significantly be reduced by having an anti-virus / anti-malware and always the latest security patches installed on the device. By using a **Mobile Device Management (MDM)**, 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.

MDM can be used to enforce device passwords, application black lists or white lists, jailbreak and rooting detection or remote wiping of all critical contents in the event of device theft or loss. Thus, 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. Thus, for instance, business emails and attachments can be restricted from being emailed via personal email accounts.

MAM and MIM include the automated enforcement of usage policies based on factors such as type of device, type of network and user, and a selective lock and wipe of the isolated, secured environment, without touching the private sphere of the user. 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)**, which today's modern enterprises need to incorporate – sooner or later.

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 should be considered, decided upon and included in policies to be defined. We are going to have a closer look at these aspects now, showing what an organization should look after and which questions to ask to itself, when introducing BYOD. Which answers to these questions are right and optimum ones can of course not be answered in general, because this will depend strongly on the organization's strategy, its goals and other views. Let us just take two examples of high priority goals: cost reduction and end user satisfaction. Some policies will probably look totally different when going for one or the other goal.

The first aspect is **scope and eligibility.** It should be clear, if BYOD is just allowed, if employees are encouraged to go for it, or if BYOD will even be subsidized. Are employee-owned devices the only option, or is the company-owned device option maintained? Bear in mind that not all employees will want bring their own devices. 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 data they get in touch with? 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? And what if they do not endure the probation period?

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 part will have to be updated frequently. Make also clear, if you allow any device, any form factor and operating systems platform, or if you limit them.

An important topic is **license implications**. May 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 different 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? Or is anything left that has to be self-procured by the user? Unfortunately, these are questions to which there is no general answer, because this will always depend on the individual software and the respective vendor.

Is also recommendable to specify whether you 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 of the private environment could lead to 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 user changes his role, when he replaces his device, or when his 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. What is done by the IT department? The focus of the IT department will certainly be the corporate applications and data, and not the device. But maybe at a certain extent, users can get device support, too? 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 loaner pool in the organization, from where users can procure a spare device? Or will they have to work in the office using stationary devices?

If you want to encourage your employees to go for BYOD or if it is even the one and only option, your employees certainly expect a **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 might be **tax implications**, such as depreciation, income-related expenses or monetary benefits that you should get familiar with. By all means, it will not make too much sense, if you pay a considerable amount of money to the employee, but at the end of the day, he will have to forward a major share to the tax authorities, because it is subject to tax.

The most difficult part is the **legal aspects**. Imagine there is an internal security investigation or a discovery for a lawsuit, for which you need the employee-owned device. An agreement with the employee that you can **claim for surrendering 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 private data. Besides, you should think about the certainly rare situation that corporate data is on the user's device, and the user has forgotten his password.

Another legal aspect is **liability**. To demonstrate the broad scope of what needs to be considered and correspondingly agreed, we are going to show some of the questions that sometimes 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, in the company, or during a business trip?
- Which adjustment can be expected?
- Will it 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 hearings at the labor court. 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.

Hence, BYOD should come along with clear rules and policies covering all these various aspects. But what if it comes to a **policy violation**, because employees do not stick to the rules? Think also about this:

- Will the employee get a written warning or call to order?
- Will you stop the payment for the employee?
- Will you claim for compensation?
- Will you terminate the labor contract?
- 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 the already existing policies and compliance demands into consideration. In addition, you should not neglect to undergo a risk and insurance assessment. Going for BYOD can lead to a new insurance situation which may result in new fees. Therefore, ensure that company insurers are aware of the change in working practices.

BYOD involves all parts of the business

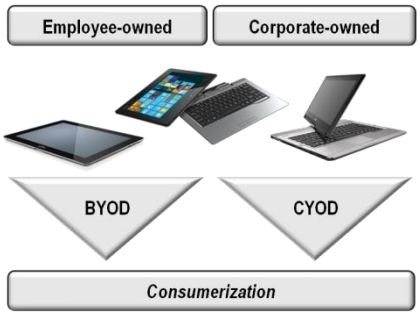
Having all policies in place, communication to the employees is essential. Your staff has to be aware of all the options and restrictions, responsibilities, duties and consequences. To make user understand what can happen, and to underline the importance of data protection, training sessions can be helpful.

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, BYOD will fail.

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, no matter which private data is locally stored. 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 them a broad selection of innovative IT-supported devices which enables them not only to run the latest versions of the software they need for the business, but of course also their 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 talents. 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 labor 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 showing which software is usable for which purpose, especially whether private applications may be used from inside the corporate network.

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 is to accompany the customer on this journey, optimize the duration by avoiding all the potential traps, overcoming the many hurdles you are faced with, thus reducing risks and costs.

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 virtual client computing solution** from a single source, usually as a mix of various concepts.

Close partnerships with all prominent market leaders, such as Citrix, Microsoft and VMware enable us to use best in class virtualization software and additional 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.

Through all our activities in real-life projects, we have gained experience as to what is required to successfully introduce virtual client computing 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, the integration and the migration from the current into the new world. Likewise, Fujitsu provides **maintenance** and support, end-to-end 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 virtual client computing upfront, despite wanting to take advantage from the benefits it provides. Fujitsu **Financial Services**, the IT leasing and financing arm of our business, has 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 rather want to concentrate on their core business and strategic projects than daily routine tasks, Fujitsu will operate the customer's workplace infrastructure, based on standardized and optimized processes. Customers take advantage from scale effects, the simple opportunity to alleviate shortages in resources and skills, flexible customer-specific and business-related service levels, and cost reductions. The "price-per-seat" charging model eliminates investment risks and ensures highest cost transparency. At the same time, customers keep their IT infrastructure fully under control.

By Fujitsu's **Virtual Client Services**, the largest virtual client computing infrastructures in the world with 10,000s of users are operated.

Alternatively, applications and standardized IT workplaces can be delivered as a service from the cloud, with a standardized service level agreement, as easily as electricity from the socket or water from the tap. A "pay-as-you-use" model is the basis for billing, turning CAPEX to OPEX, and minimizing costs in total.

Especially for smartphones and tablet PCs, no matter whether corporate- or employee owned, **Fujitsu Managed Mobile** is worth mentioning, which 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 an extraordinary position, that already today its portfolio includes all relevant device types. For the access to centralized virtual client computing infrastructures, Fujitsu FUTRO Thin Clients and Smart Zero 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 help out with its Fujitsu ESPRIMO PCs and Fujitsu CELSIUS workstations.

Fujitsu's workplace systems 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 technologies at attractive conditions. 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 workplace systems from Fujitsu will certainly attract many of your employees.

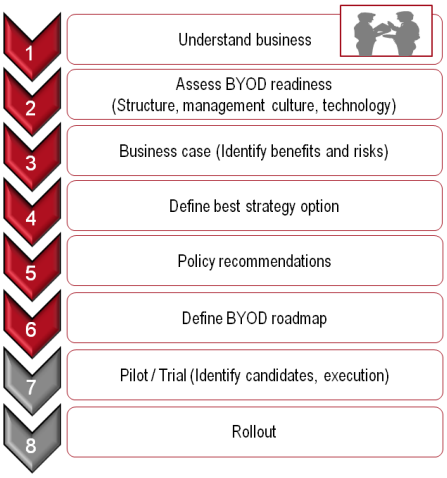
In a nutshell: Fujitsu is a one-stop shop that provides everything you need for BYOD from a single source. This helps reduce complexity, implementation time and risk. Moreover, Fujitsu gives the customer all the flexibility he needs to select the most appropriate sourcing option or even a mix of them.

The first step: BYOD Assessment

To simplify the first step of the journey to BYOD, Fujitsu developed a standardized service called BYOD Assessment. The approach is a cross-organizational engagement. By tool-based interviews with the management, with knowledge workers, and business unit leads, with Human Resources, the IT department, with 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 support the customer on demand 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. Use the pilots to put in place appropriate support mechanisms.

Of course, Fujitsu will support its customers also 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 potentially can be the solution, but it brings its own challenges around security and manageability. Virtual client computing solutions help separate corporate applications and data from the device, thus mitigating the CIO's headaches. But BYOD is not just about infrastructure; it is also about policies whose definition requires the involvement of various parts of the organization. Fujitsu is a one-stop shop, able to support customers in terms of virtual client computing, from products to solutions and services, making BYOD a success.

Contact
FUJITSU Technology Solutions GmbH
Address: Mies-van-der-Rohe-Strasse 8,
80807 Munich, Germany
Phone: +49-7203-922078
Fax : +49-821-804-88429
E-mail: gernot.fels@ts.fujitsu.com
Website:www.fujitsu.com/fts