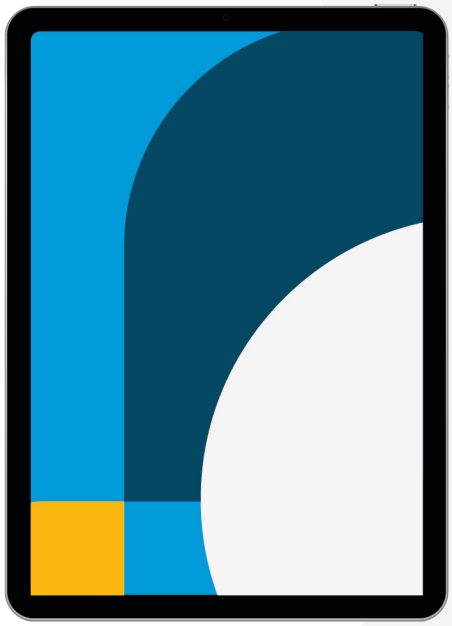
pro warehouse

Choose Your Own Device strategy



26 questions & tips

Consultants Network

Introduction

Implementing a Choose Your Own Device strategy can be a daunting task. Where do you start, what choices will you give your employees and how do you manage all these devices and systems without losing the overview and without endangering the security of your ICT infrastructure?

This white paper presents a step-by-step plan to support you in rolling out a Choose Your Own Device strategy. The orientation process, choosing the right hardware, connecting software and Mobile Device Management systems, and the final implementation of Choose Your Own Device in your organisation are discussed in detail and summarised in a handy overview.

Table of contents

Introduction 2

1. Choose Your Own Device 4

1.1 From Bring Your Own Device to Choose Your Own Device 4

1.2 Good IT management is the success factor 4

2. The orientation process 5

2.1 Choose Your Own Device in your organisation 5

2.2 Internal stakeholders 6

2.3 Compile a list of desired software 6

2.4 Get advice from suppliers 7

3. The purchasing process 8

3.1 Freedom of choice for employees 8

3.2 Mobile Device Management tools 9

3.3 Security 9

3.4 Quantity of new hardware 10

3.5 Define the implementation strategy 10

4. The implementation process 11

4.1 Set up a pilot group 11

4.2 Implement the MDM tools 11

4.3 Test all software and apps 12

4.4 Inform colleagues 12

4.5 Roll out the strategy company-wide 13

4.6 Reflect, streamline and automate CYOD processes 13

5. Choose Your Own Device strategy checklist: all the questions at a glance 14

5.1 Orientation 14

5.2 Purchasing process 15

5.3 The implementation process 15

Our PROs can always help you 16

1. Choose Your Own Device

With a Choose Your Own Device strategy, you let your employees choose what operating system and hardware to work with. The term originated around the year 2000 and stems from the Bring Your Own Device strategy that was originally initiated bottom-up within companies in the 1990s.

1.1 From Bring Your Own Device to Choose Your Own Device

As private hardware became more accessible, employees started using their own laptops and phones at work. Organisations allowed employees to use their own electronics and Bring Your Own Device (BYOD) strategies were rolled out.

However, BYOD also has many disadvantages. The company has no control over data exchange and cyber security. Work-related files, programmes and apps remain in the ex-employee's possession after the termination of the contract, and there can be administrative ambiguity about ownership of the devices and the files and programmes on them. Despite these drawbacks, employers also saw the benefits of working on their own familiar devices. Choose Your Own Device strategies were introduced to maintain employee satisfaction and efficiency but manage corporate information, files, programmes and security in-house.

1.2 Good IT management is the success factor

Not the choice of a device itself, but the proper management, control and security of these devices is the basis for a successful Choose Your Own Device strategy. In order to achieve the desired result, different operating systems must be able to communicate with each other. Good software implementation and the right security programmes are also important. You can let employees choose their own devices, but if the operating systems cannot communicate with each other and the software does not work, your strategy fails.

In this white paper, we provide a step-by-step plan for implementing a Choose Your Own Device strategy. In this, we focus on CYOD strategies in which employees can choose between Apple and Microsoft operating systems for their computer, laptop, phone and/or tablet.

2. The orientation process

Good orientation is an important first step towards a successful Choose Your Own Device strategy. Therefore, the first part of this step-by-step plan is dominated by the orientation process. In doing so, ask yourself and/or your employees the following questions and reflect on them:

2.1 Choose Your Own Device in your organisation

A logical first step in the orientation process is to ask yourself why you want to implement a Choose Your Own Device strategy in your business. After all, the point of running multiple operating systems is that it helps your organisation move forward, instead of working against it. It is advisable to evaluate important software for your organisation: can this software run on both systems or is there a suitable alternative? Also make an inventory of whether the software is specifically important for one department, or if it applies to several.

If the use of exclusive software is limited to a few departments, a Choose Your Own Device strategy need not be discarded. It is likely that employees in these departments already have a preference for the operating system on which the software works best and/or are easier to convince them to choose the operating system that best supports their work. Also, employee satisfaction in other departments will not suffer from the software restrictions of a small part of the company.

Is it really only possible to use Apple or Windows in your own company? Then you might consider letting employees choose from different flavours with the same operating system. Consider, for example, the choice between a 13" versus a 16" laptop, or between phones with better cameras or just more memory.

1. How will a Choose Your Own Device strategy move our organisation forward?
2. Can important software run on multiple operating systems?
    A. If not? Is there a good (or better) alternative?
    B. If not? Which departments does it apply to?

2.2 Internal stakeholders

Which employees from which departments will you involve from the start? From whom do you collect wishes and feedback first, and who do you use as a sparring partner? Although it depends on each company who you involve in the orientation process, you can consider a number of departments and individuals. For example, involve those who would like to have a Choose Your Own Device strategy and who would benefit most from it. Nine times out of 10, these are your employees from the HR department, but it can also come from a group of employees from other departments. Also ask them about their reasons for a CYOD strategy.

Other departments that are advisable to involve from the start are Finance and Security. This gives you a guideline for a budget and all the safety requirements are listed. It may be useful to involve someone from the board of directors to test whether a CYOD strategy fits in with the company's vision and progress. This information also helps later on when implementing the strategy.

3. Who will I involve from the start?
   A. What advantages do I gain from a Choose Your Own Device strategy?
   B. What requirements do I set for a Choose Your Own Device strategy?

2.3 Compile a list of desired software

It is advisable to draw up a list of desired software. There is software that only works well on Windows or Apple. Fortunately, this number is steadily decreasing and lots of software runs on all operating systems, or there are good alternatives, such as working in the cloud.

List all software, online tools and apps used within your organisation, indicating how important the programmes are and how much they are used (this can be done on a scale of 1 to 5, for example). Check whether the tools work on several operating systems, but if in doubt, ask the supplier if there are alternatives. Are exclusive tools not used or hardly used, or are they not essential? Then finding an alternative or terminating the licence is an easier step than when tools are used daily.

4. What software, online tools and apps are used within the organisation?
   A. How important is the tool? How much is the tool used?
   B. Does the tool work on multiple operating systems?

2.4 Get advice from suppliers

With the goal and vision in mind, the wishes and requirements of internal stakeholders listed and the desired software in a list, you can start planning talks with suppliers. Every organisation has different requirements when selecting a partner and often it is also a question of "having a good feeling with the partner".

To make the decision-making process easier, it is useful to ask the same questions to each supplier so that you can compare the answers properly. Also, ask how they would approach implementing the Choose Your Own Device strategy and what hardware, software and Mobile Device Management tools they have available to make the Choose Your Own Device strategy successful from start to finish.

5. Which suppliers do I talk to?
6. What am I going to ask them?
7. What am I basing my judgment on?

3. The purchasing process

After the orientation process and discussions with suppliers, it is time to procure hardware, associated software and a Mobile Device Management system. Here, it is important to think about the choices you will give employees, the tools you will use, security and the implementation strategy.

3.1 Freedom of choice for employees

To illustrate the freedom of choice for certain hardware and operating systems in a Choose Your Own Device strategy, it is useful to first look at their minimum and maximum versions, and then determine a good middle ground that suits your organisation. The minimum implementation of a Choose Your Own Device strategy is purely about providing choice. For example, the choice between two types of laptops, phones or tablets with the same operating system, but with a different look. For example, one employee may prefer to work on a 16-inch laptop, while another may prefer a lightweight laptop.

The maximum implementation of a Choose Your Own Device strategy gives the user the choice of all devices. Brands, models, versions and operating systems can all be mixed to suit the user's needs. The minimum and maximum versions are both often undesirable. With the minimum version, the choice is nevertheless limited, while the maximum version is often not easy and safe to manage.

In addition, it is not cost-effective to let all employees choose "just like that". Also, which devices and corresponding choices are needed may vary from department to department. For example, there will be departments that need large, heavy machines to do their work properly, versus those that can do their work just fine with simpler devices. A desk clerk will not need a heavy computer to perform well, while a designer will not be able to edit videos optimally on a small laptop because the device does not have enough capacity. The accessibility to certain (niche) software, described in chapter 2, is also a determining factor for the choices you give per department or part of the company. Discuss these issues and choices with the various departments.

8. Which operating systems do I make available to my employees?
9. What types of devices do I make available to my employees?
10. Are there differences between the required hardware/operating systems in each department? If so? How will I facilitate these differences?

3.2 Mobile Device Management tools

Your organisation probably already uses a Mobile Device Management (MDM) tool for the operating system it already works with. This means that an MDM tool only needs to be implemented for the operating system that may be added. If it is up and running and the IT department knows how it works, it hardly needs looking after. When choosing a new MDM tool, it is advisable to first take stock of what your existing tool looks like. Determine the advantages (and any disadvantages) and look for a tool that meets the needs of your organisation and department. Often suppliers offer MDM tools that fit your organisation and IT management. Make sure the systems can run seamlessly side by side. The less they differ, the easier it is to manage them.

11. How does my existing MDM tool work?
12. How do I successfully run my new MDM tool alongside my existing one?

3.3 Security

Security of all operating systems is a must, as cybercrime is lurking everywhere. The requirements for securing different operating systems are the same, although the software may differ. Go through these requirements again with the company lawyer and purchase the software licences that meet them. The supplier can also advise on this.

Do you work in the cloud? Then good general protection and encryption of sensitive data are important. Of course, the security of the ICT infrastructure, (Wi-Fi) networks and passwords also plays a role. However, this makes no difference to the type of operating system.

13. What are my organisation's security requirements?
14. How are my current devices protected?
15. Are special software licences needed to protect the new operating systems?

3.4 Quantity of new hardware

The amount of hardware you purchase at once depends on your budget and your organisation's wishes and vision. Are you going to let all your employees choose and change all your devices at once? Will you only let employees who have been in service for a number of years choose? Do you start with all the new employees who have just arrived? Are you going to roll out the strategy per department? Do you start with phones first and only move on to desktops and PCs after a few years? Or do you apply a mix?

16. How much new hardware am I going to purchase?
    A. What is the budget?
    B. What is the strategy?
    C. How will I justify this choice to internal stakeholders?

3.5 Define the implementation strategy

How you implement the Choose Your Own Device strategy depends partly on the choices you made earlier in the process, but also relies heavily on a successful pilot strategy and the company-wide roll-out after the pilot. Indeed, running a pilot is an important step for further implementation. By testing the strategy, you tackle teething problems on a small scale, without hindering the work process of the entire organisation.

Determine the scope of the pilot, the points that the pilot must meet to be successful and the company-wide roll-out of the CYOD strategy. This process can also be discussed and taken up with the supplier.

17. How will I implement the Choose Your Own Device strategy?
    A. What will be the scope of the pilot period?
    B. When will the pilot period be successful?
    C. How will I implement the strategy company-wide?

4. The implementation process

After proper preparation, the implementation process of the Choose Your Own Device strategy follows. Before it is rolled out company-wide, in most cases, a pilot is run to test whether all systems work. Training and instruction are also given to those employees who need it.

4.1 Set up a pilot group

There are many ways to compose a pilot group. You can take one department, assemble a handful of employees from all layers of the organisation, or have the most important internal stakeholders test the new strategy. One way that often works well is to choose one person from each department to test. It is helpful to choose employees who are open to new things, tech-savvy and have time for testing.

Especially when rolling out the strategy, earlier testing is a benefit across different departments. In fact, there is one employee per department who knows how the strategy works and who can act as an ambassador for the strategy in his/her own department. This also allows questions to be put to the ambassador and lowers the threshold for sharing any concerns. This puts less pressure on the IT department and makes it easier for employees to ask these questions or share possible concerns.

4.2 Implement the MDM tools

For testing, the MDM tools must be implemented. Make a checklist of which functionalities of the MDM tool should be tested. This includes security operations such as remotely blocking devices and remotely installing and removing software and apps.

19. Do all the functionalities in my MDM tool work?

4.3 Test all software and apps

You may have purchased new software and apps for the new operating system. They must be tested to ensure safety and user-friendliness. The connections to the cloud, external database, (Wi-Fi) network and printers also need to be assessed. Functionality and user-friendliness are important factors here.

20. Do the (new) software and apps work on the operating systems?

4.4 Inform colleagues

Once the pilot period has been successfully completed, it is time to roll out the Choose Your Own Device strategy across the company. In addition to the ambassadors of the different departments, it is advisable to involve the communications department and the internal helpdesk. The communications department has all the tools to inform employees properly and fully. The helpdesk provides support in helping employees with their new devices.

It is important to inform your employees about:

- Why the organisation has opted for CYOD and how it will contribute to the progress of the organisation (vision).
- The course of the entire process.
- The measures taken to ensure safety, continuity and employee satisfaction.
- The "rules" of CYOD implementation.
- The people to whom questions can be asked.

You can do this by sending an informative e-mail, providing a training course or giving a presentation on the new Choose Your Own Device strategy.

21. How will I inform my colleagues about the upcoming changes?
22. What am I going to tell my employees?
23. Which internal stakeholders do I involve in this process?

4.5 Roll out the strategy company-wide

Your employees have been informed, the right hardware has been sourced, MDM tools are working and software packages have been compiled: it's time to roll out the Choose Your Own Device strategy company-wide.

No matter how big or small the roll-out, the continuity of the organisation must be maintained as far as possible. Installation processes should not take too long, and it is not desirable for the entire company to be out of action for several hours, a day or several days .

It is, therefore, advisable to roll out the strategy in small groups. Is everything working? Then you can move on to the next group. In large companies, this can make the process take up to a week, but it does little or no harm to business continuity and allows employees to return to work quickly after implementation.

24. How do I roll out the strategy without harming business continuity?

4.6 Reflect, streamline and automate CYOD processes

Your organisation has probably learned a lot from this whole process. This feedback is important for continuing to perfect the strategy. List your own learnings, ask for feedback from employees via a survey and reflect on the strategy with your ambassadors. What are they up against? Do they or the employees they represent have any questions, comments or (positive) feedback?

Installing hardware and making it ready for use is also becoming quicker and quicker with the right MDM tools and practices. In order to save time, the preparation of software packages, apps and online tools is a must. This allows new hardware to go to the user quickly, and sometimes even without intervention from the IT manager.

25. What are the learnings from the process?
26. How can I continue to improve the processes of the CYOD strategy?

5. Choose Your Own Device strategy checklist: all the questions at a glance

The overview below lists all the questions that will help you orientate, procure and implement a Choose Your Own Device strategy.

5.1 Orientation

1. How will a Choose Your Own Device strategy move our organisation forward?
2. Can important software run on multiple operating systems?
    - If not? Is there a good (or better) alternative?
    - If not? Which departments does it apply to?
3. Who will I involve from the start?
    - What advantages do I gain from a Choose Your Own Device strategy?
    - What requirements do I set for a Choose Your Own Device strategy?
4. What software, online tools and apps are used within the organisation?
    - How important is the tool and how often is it used?
    - Does the tool work on multiple operating systems?
5. With which (B2B) suppliers will I enter into discussion?
6. What am I going to ask them?
7. What am I basing my judgment on?

5.2 Purchasing process

8. Which operating systems do I make available to my employees?
9. What types of devices do I make available to my employees?
10. Are there differences between the required hardware/operating systems in each department?
    - If so? How will I facilitate these differences?
11. How does my existing MDM tool work?
12. How do I successfully run my new MDM tool alongside my existing one?
13. What are my organisation's security requirements?
14. How are my current devices protected?
15. Are special software licences needed to protect the new operating systems?
16. How much new hardware am I going to purchase?
    - What is the budget?
    - What is the strategy?
    - How will I justify this choice to internal stakeholders?
17. How will I implement the Choose Your Own Device strategy?
    - What will be the scope of the pilot period?
    - When will the pilot period be successful?
    - How will I implement the strategy company-wide?

5.3 The implementation process

18. Who will be part of the pilot group?
19. Do all the functionalities in my MDM tool work?
20. Do the (new) software and apps work on the operating systems?
21. How will I inform my colleagues about the upcoming changes?
22. What am I going to tell my colleagues?
23. Which internal stakeholders do I involve in this process?
24. How do I roll out the strategy without harming business continuity?
25. What are the learnings from the process?
26. How can I continue to improve the processes of the CYOD strategy?

Our PROs can always help you

After reading this white paper, would you also like to introduce a Choose Your Own Device program within your organisation? Or do you want more substantive information? We will be happy to help.

Your business is not standing still and information technology is developing at lightning speed. That is why we at Pro Warehouse are constantly working extremely hard to keep innovating and improving our services. Pro Warehouse's PROs are happy to deliver solutions to help your organisation grow. Solutions that are also immediately deployable on the shop floor. From purchasing and deploying hardware, to assisting users with management and support.

We will be happy to help you with honest advice and clear insights on Apple devices in the workplace.

pro warehouse

Tel: +31 20 423 16 37
Mail: sales@prowarehouse.nl

Address: Paasheuvelweg 34 c
1105 BJ Amsterdam
Nederland

Web: www.prowarehouse.nl