Deloitte.

2015 Luxembourg Mobile Technology Survey on Corporate Usage & Security

Capturing insight

December 2015

Preface

We are delighted to present the 2015 Luxembourg Mobile Technology Survey on Corporate Usage & Security.

Recent mobile devices such as smartphones and tablets enable employees to work anytime, anywhere, and are powerful enough to handle most business activities and data, including e-mail, documents, contacts, and agendas. Mobile devices are a good example reflecting the new information security paradigm resulting from the deperimeterization of Information Technology, where IT assets, users and data are moved outside of the traditional Information System boundaries.

Today, in Luxembourg, numerous organizations across all industries are dealing with this type of project (either as a new service, or as migration from an obsolete system), and face the new security challenges brought by mobile technologies.

We hope you find the report both helpful and insightful in benchmarking your organization and that it assists you in reaching the most optimal balance between corporate mobile usage and greater organization's data security.

Stéphane Hurtaud
Partner
Information & Technology Risk

Laurent de la Vaissière
Directeur
Information & Technology Risk

Maxime Verac
Manager
Information & Technology Risk

© 2015 Deloitte Tax & Consulting

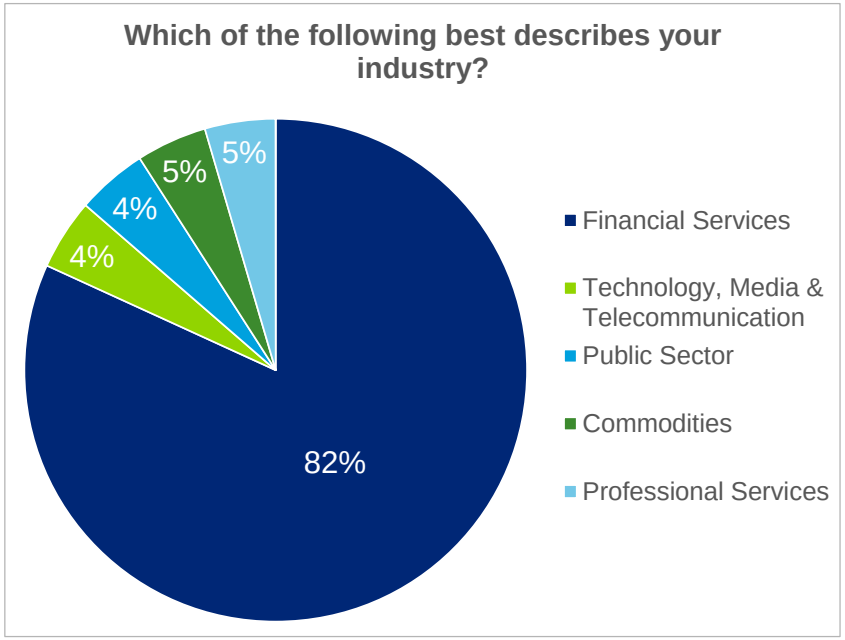
Content

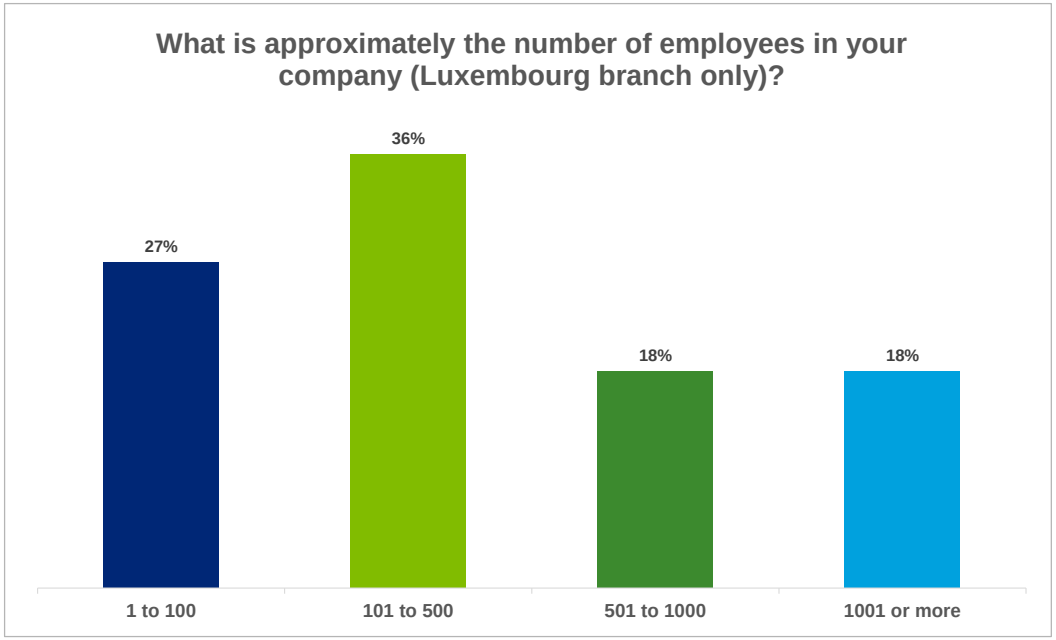
Scope and objectives	4
Mobile Strategy & Policies	5
Current and planned usage	7
Drivers & Inhibitors	14
Security controls	15
Infrastructure & Technology	21
Value & Perception	25
Key Definitions	26

© 2015 Deloitte Tax & Consulting

Scope and objectives

Deloitte Luxembourg launched the 2015 Luxembourg Mobile Technology Survey on Corporate Usage & Security in order to understand how organizations use or plan to use Mobile Technologies for their employees and what are the security controls they implement to secure their usage.



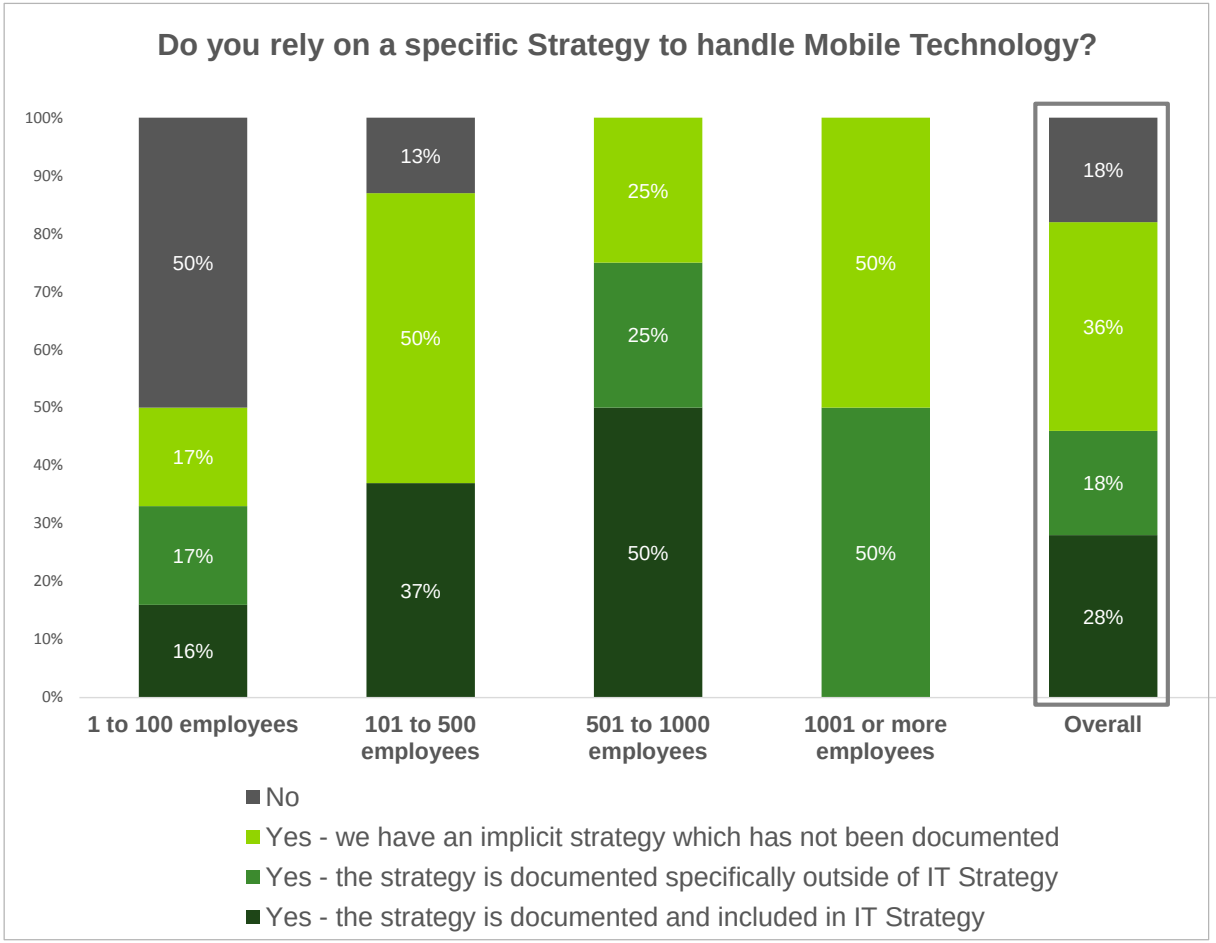


- This survey was performed between June and September 2015, and enabled to gather answers from a representative panel of **22 Luxembourg organizations**
- Respondents **are mostly CIOs and Information/IT Security Officers** from **Financial Services organizations**

© 2015 Deloitte Tax & Consulting

Mobile Strategy & Policies

Strategy to handle Mobile Technology

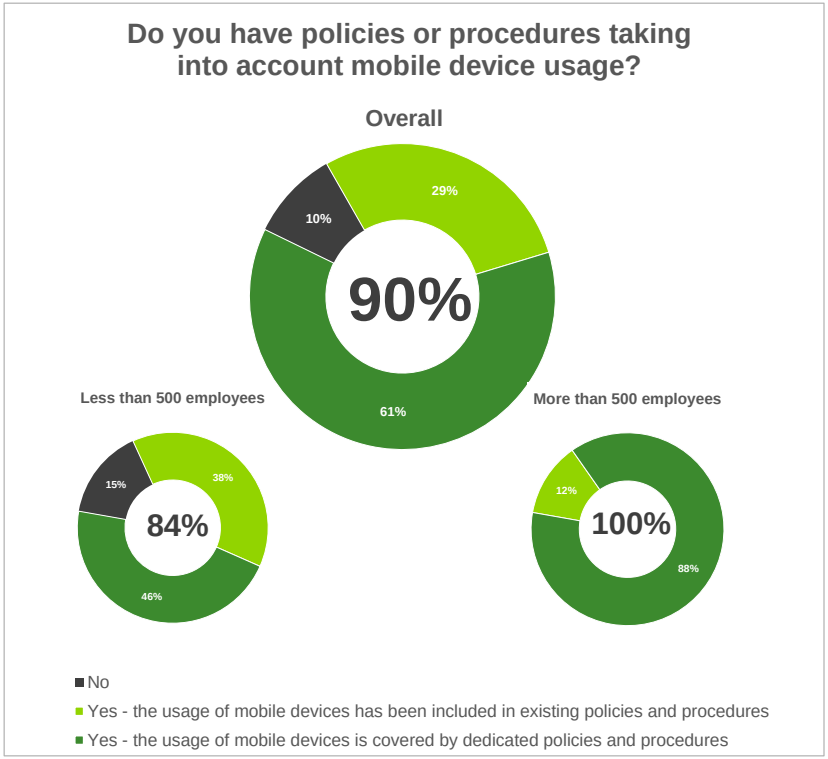


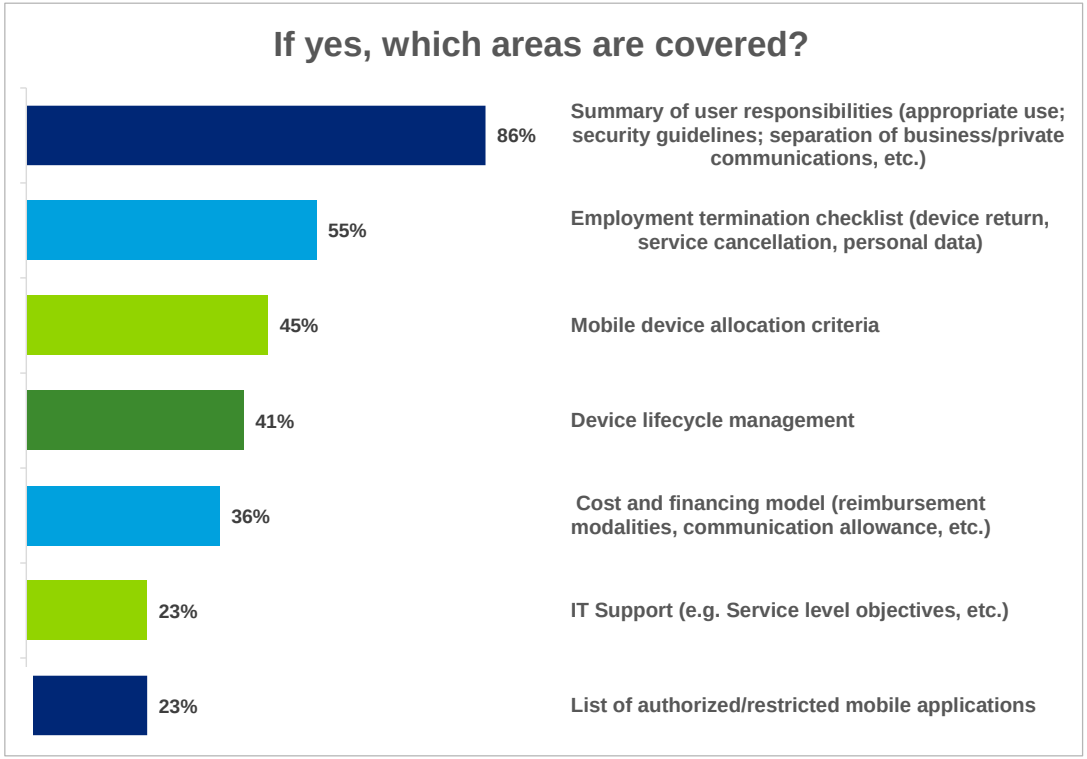
- Overall, **a vast majority of the respondents (82%) rely on a Mobile strategy** but this strategy is not systematically documented (only 46% of the respondents declared that they have a documented Mobile Strategy)
- **As expected, size does matter: 100% of largest surveyed organizations** (i.e. >500 employees) **rely on an implicit or documented mobile strategy** whereas **50% of smallest surveyed organizations** (i.e. <100 employees) **have an opportunistic approach** towards deployment and use of Mobile Technology

© 2015 Deloitte Tax & Consulting

Mobile Strategy & Policies

Areas covered by Mobile Policies



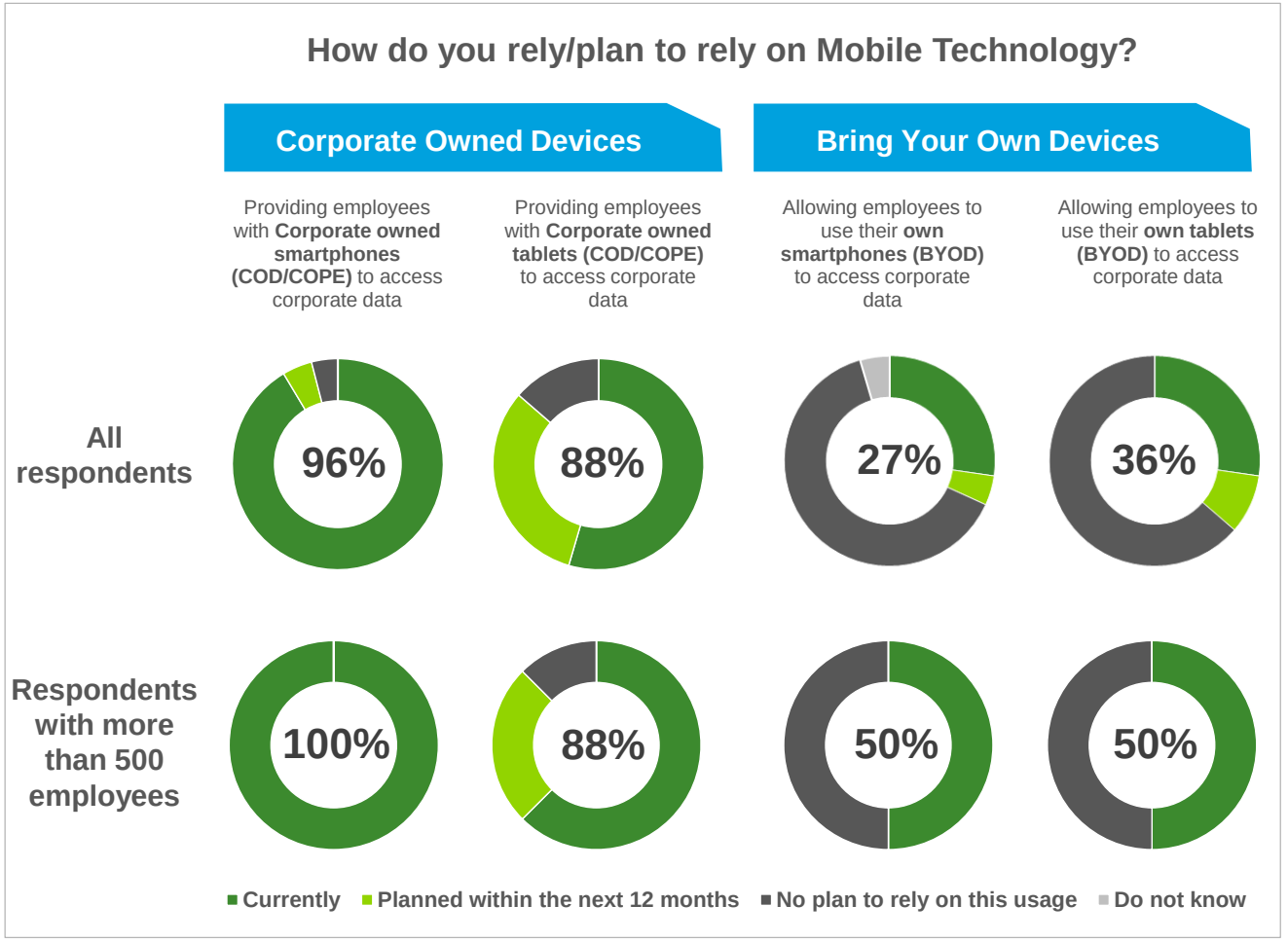


- Only 10% of the surveyed organizations have not formalized documentation to cover mobile device usage. **Most (88%) of the large surveyed organizations (>500 employees) rely on dedicated policies and procedures**
- The majority of the policies are used to define **user responsibilities towards the use of mobile devices**

© 2015 Deloitte Tax & Consulting

Current and planned usage of Smartphones & Tablets

Level of adoption of Mobile Technologies

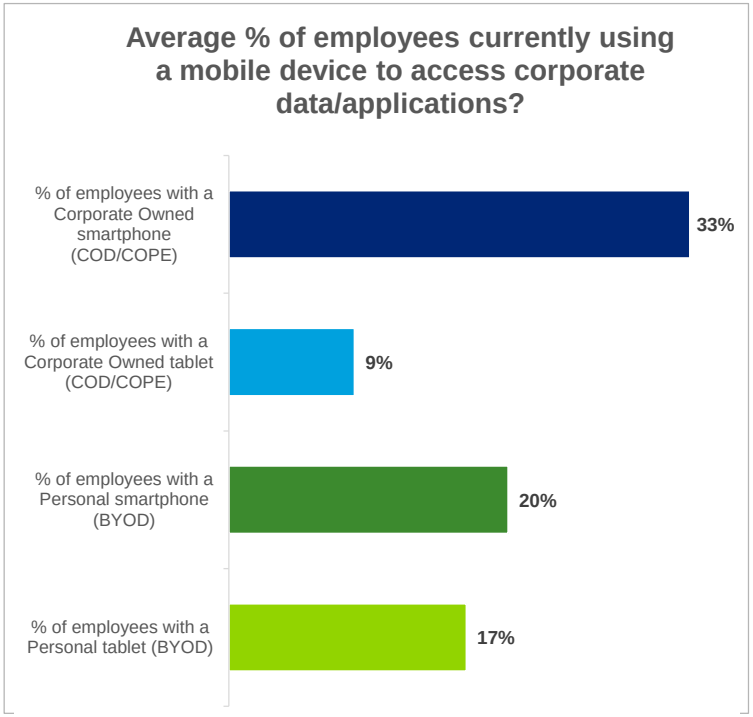


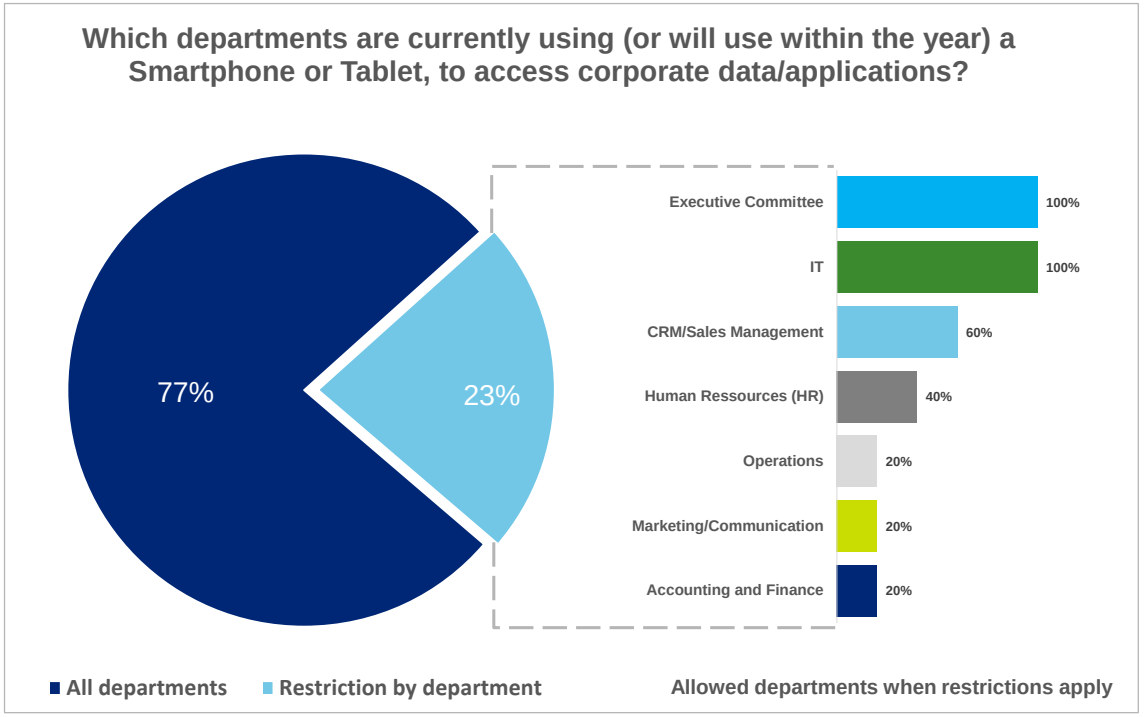
- **Massive adoption of Corporate Owned Devices** (COD/COPE) within organizations (96% for smartphones and 88% for tablets)
- Organizations are **still reluctant to adopt BYOD**, this is especially true for small and medium sized companies (i.e. <500 employees)

© 2015 Deloitte Tax & Consulting

Current and planned usage of Smartphones & Tablets

Deployment of Mobile Devices



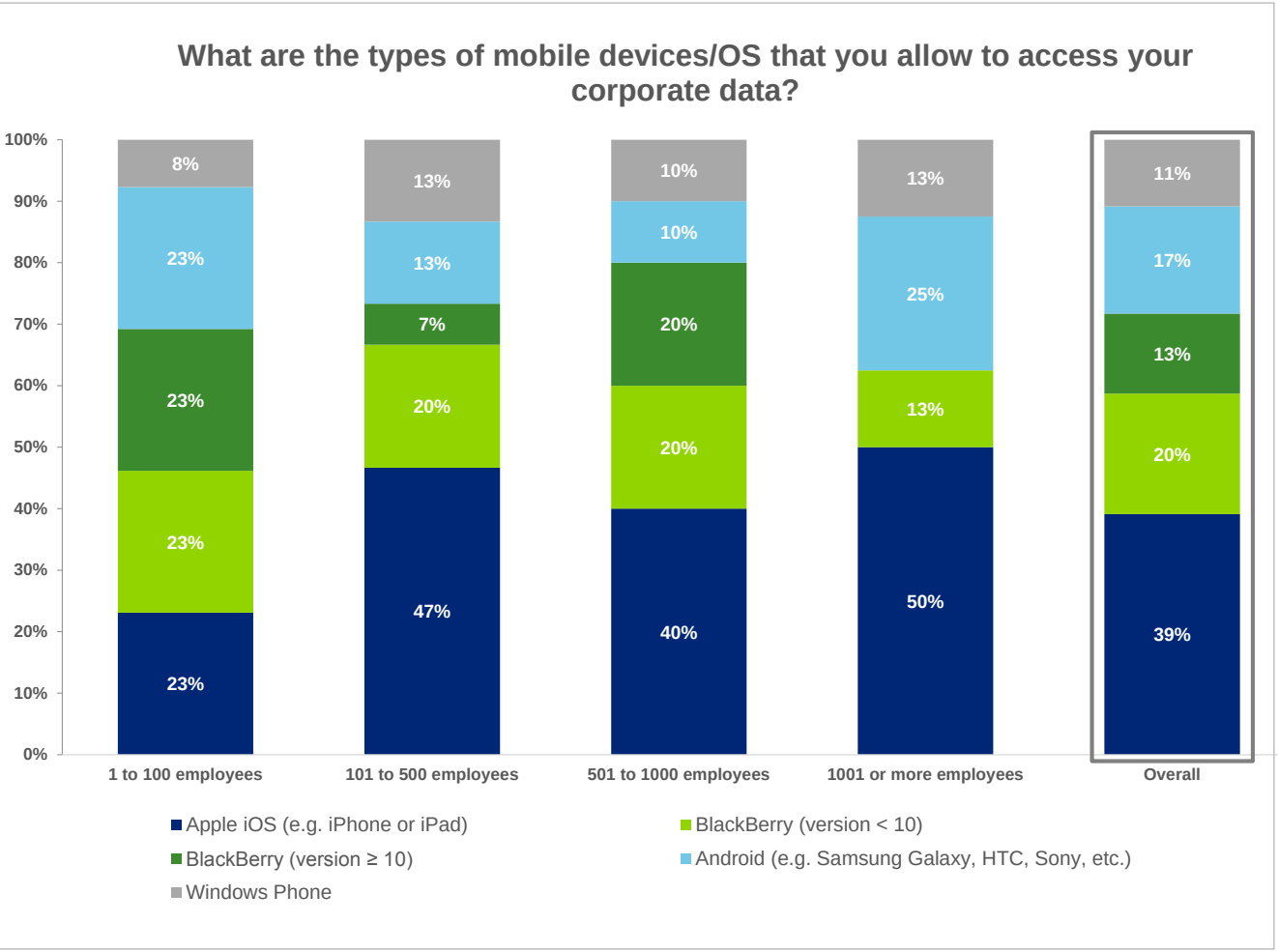


- In average, **33% of employees are currently using a Corporate smartphone to access corporate data/applications** (minimum 2% and maximum 63%)
- Most surveyed organizations (77%) do not restrict use of mobile devices to specific departments but **promote a "horizontal deployment" while focusing restriction on a hierarchical basis**. Executive Committee and IT department are systematically allowed to use mobile devices to access corporate data

© 2015 Deloitte Tax & Consulting

Current and planned usage of Smartphones & Tablets

Types of mobile devices/OS



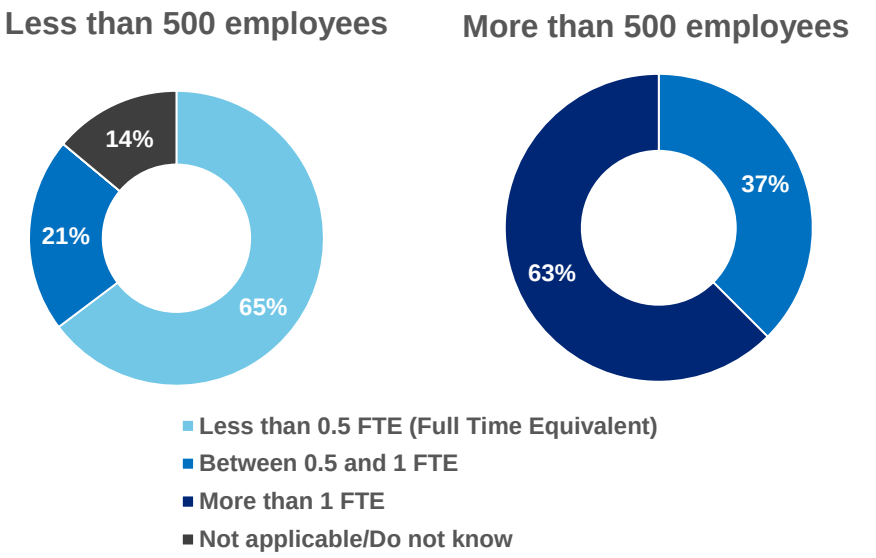
- 85% of surveyed organizations allow access to their corporate data through multiple types of mobile devices/OS
- **Prevalence of Apple iOS devices for accessing corporate data**, especially in largest surveyed organizations (50% allow access to iOS devices)
- **Windows Phone with 11% and BlackBerry** (version ≥10) **with 13% are lagging behind**
- **Old versions of BlackBerry devices (i.e. version <10) are still largely allowed** to access corporate data and are more deployed than latest releases

© 2015 Deloitte Tax & Consulting

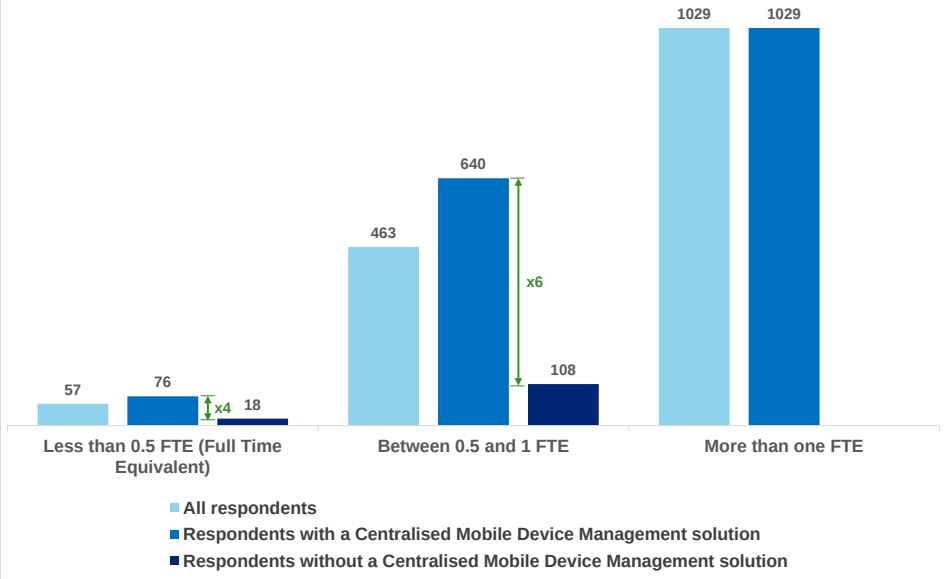
Current and planned usage of Smartphones & Tablets

Required workload to manage Mobile Technology

What is the required workload to manage Mobile Technology?



Average number of managed Corporate Owned Devices (COD) and Bring Your Own Devices (BYOD) vs. required workload (internal & external) to manage Mobile Technology



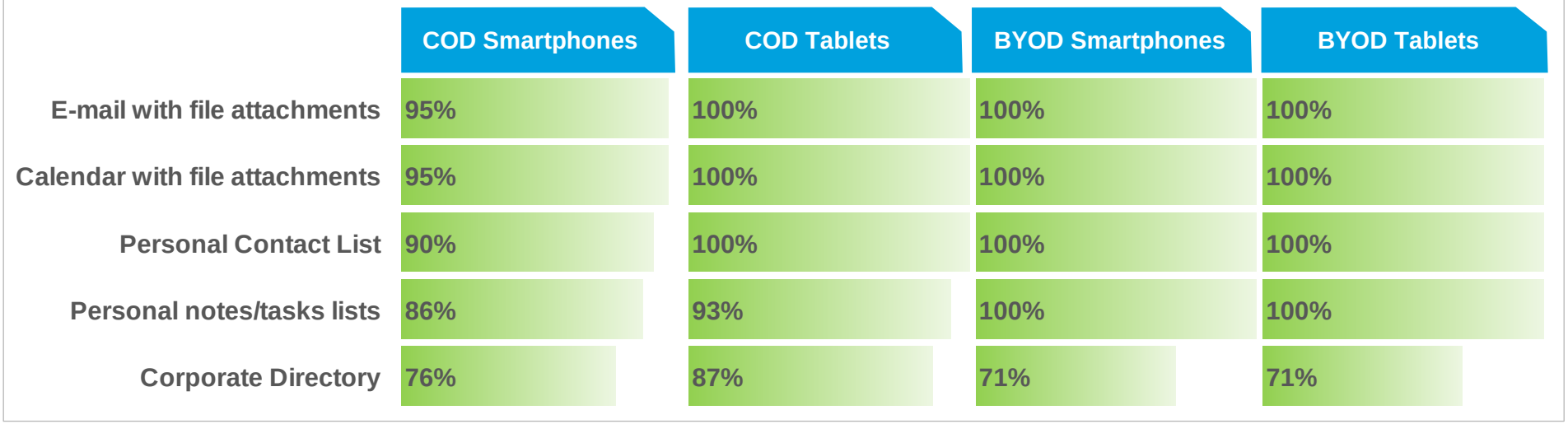
- Large surveyed organizations (>500 employees) require at least 0.5 FTE to manage mobile devices and most of them require more than 1 FTE (63%)
- For the same required workload, **surveyed organizations with a Centralized Mobile Device Management solution manage between 4 and 6 times more devices** (COD and BYOD) than organizations without such a centralized solution

© 2015 Deloitte Tax & Consulting

Current and planned usage of Smartphones & Tablets

Types of corporate PIM data accessible

What types of corporate Personal Information Manager (PIM) data can be used or will be accessible within the year?



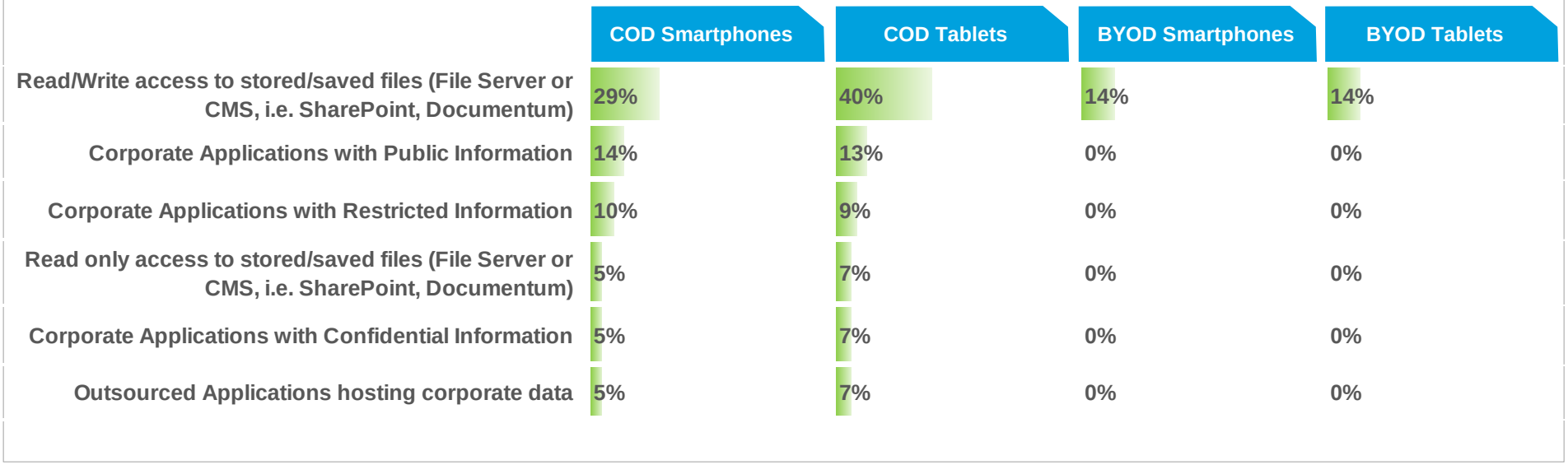
- Personal Information Manager (**PIM**) **is the most common use case for mobile technology deployment** projects (i.e. use of e-mail, calendar, personal contact list, personal notes and corporate directory)
- COD and BYOD have a similar level of access to PIM data
- **No surveyed organization restricts access to file attachments contained in e-mails or calendar events**

© 2015 Deloitte Tax & Consulting

Current and planned usage of Smartphones & Tablets

Types of corporate data/applications accessible

What types of corporate data/applications can be used or will be accessible within the year?

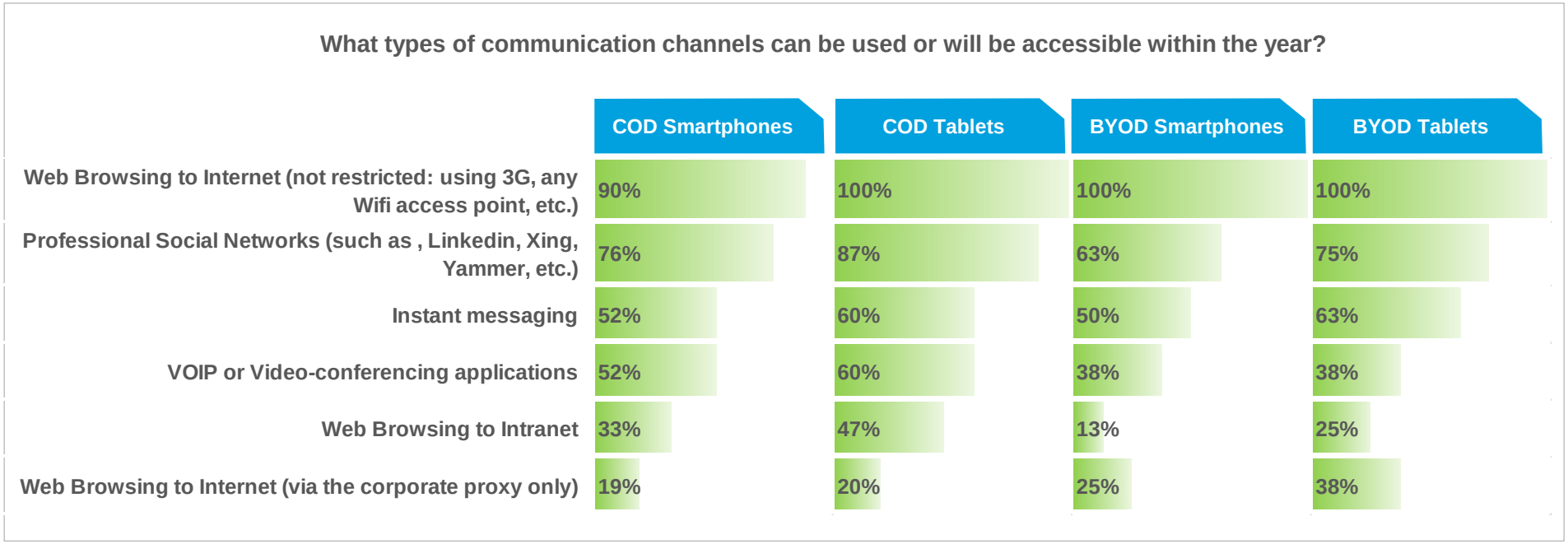


- **Besides e-mail and calendar**, **very few other ways to access corporate data are used on mobile devices**
- Only 1 respondent (Financial Services organization) allows the usage of corporate applications dealing with confidential information on corporate mobile devices
- BYOD devices of the surveyed organizations **do not have access to corporate applications**

© 2015 Deloitte Tax & Consulting

Current and planned usage of Smartphones & Tablets

Types of communication channels used

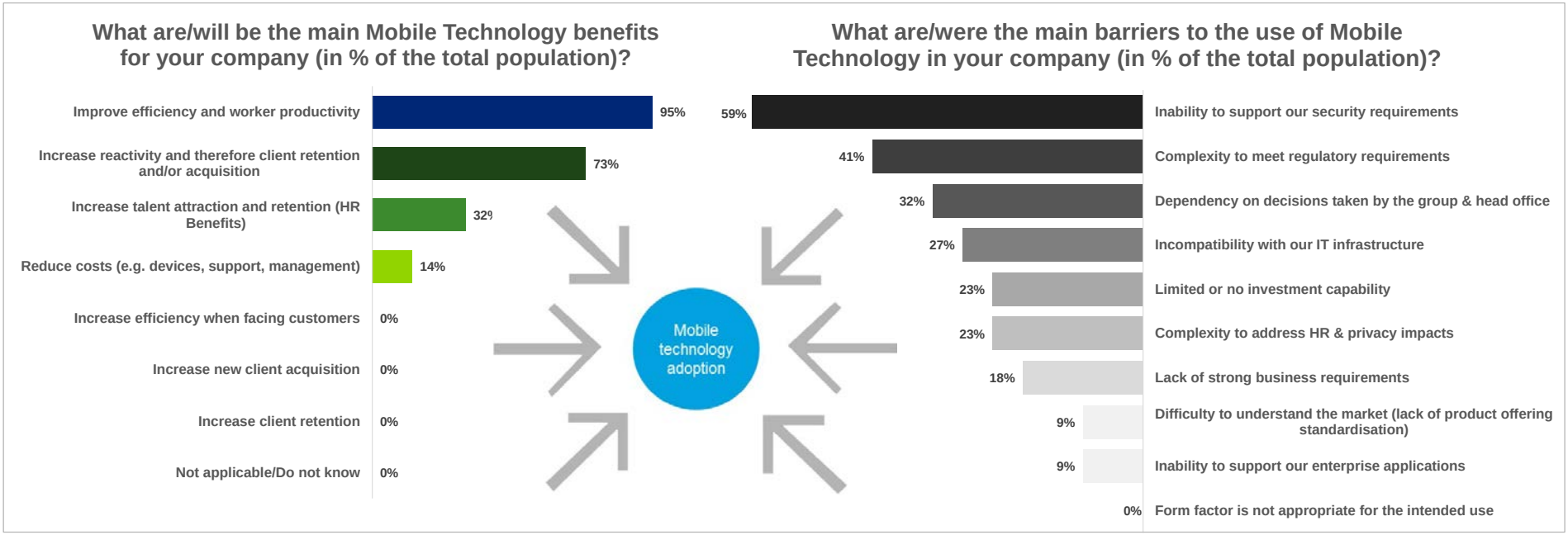


- **Access to Internet** on smartphones **is massively allowed**
- Web browsing to Intranet is rarely allowed

© 2015 Deloitte Tax & Consulting

Drivers & Inhibitors of Mobile Technology adoption

Benefits & Barriers

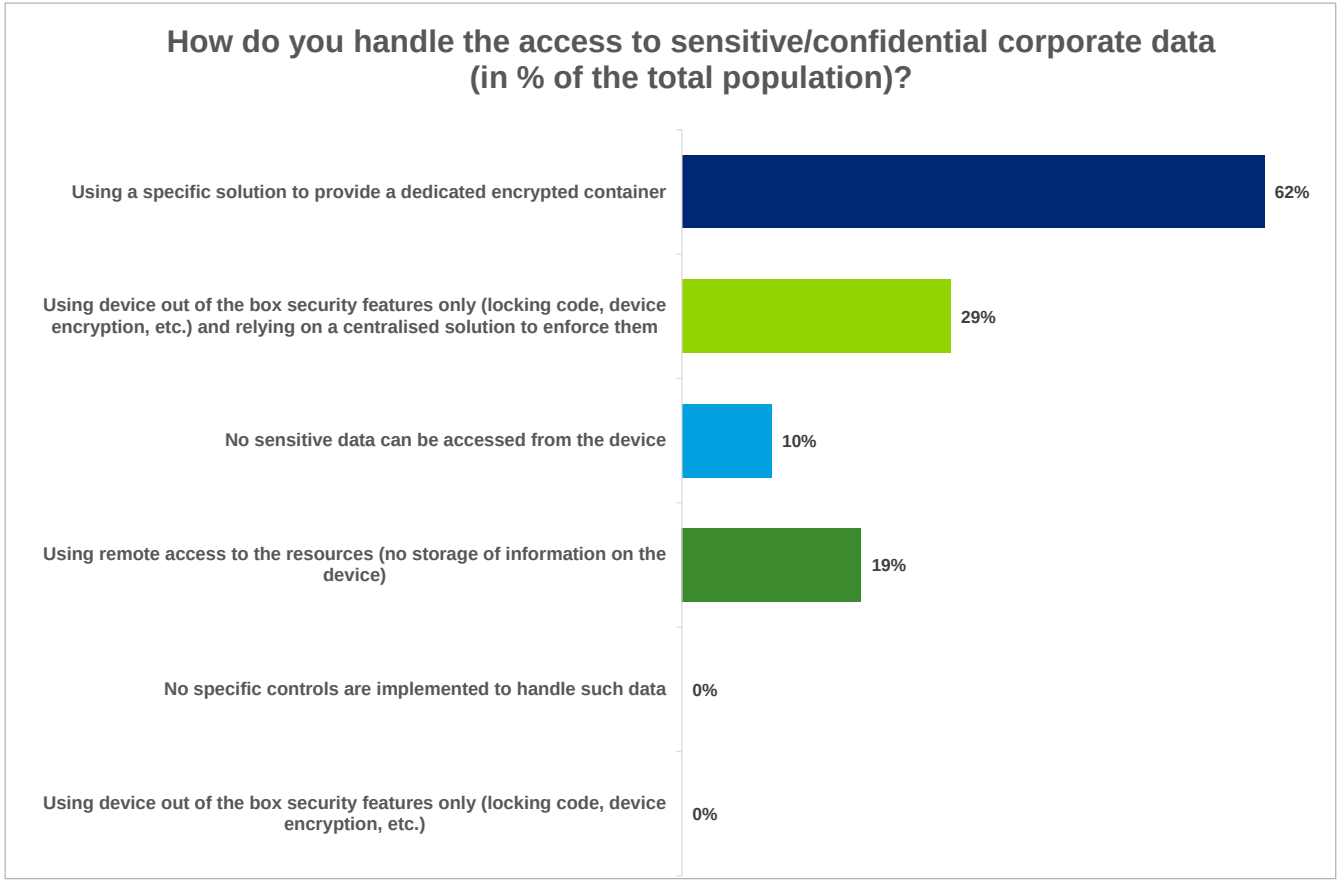


- **Inability to support security requirement is seen as the main barrier. Two potential explanations:**
  - Current mobile technologies security features are not perceived as mature enough to cope with information security requirements
  - Information security requirements are not adapted to deal with mobile technologies
- **Half of financial services organizations surveyed perceive complexity in regulatory requirements**

© 2015 Deloitte Tax & Consulting

Security & Controls

Access to sensitive/confidential corporate data



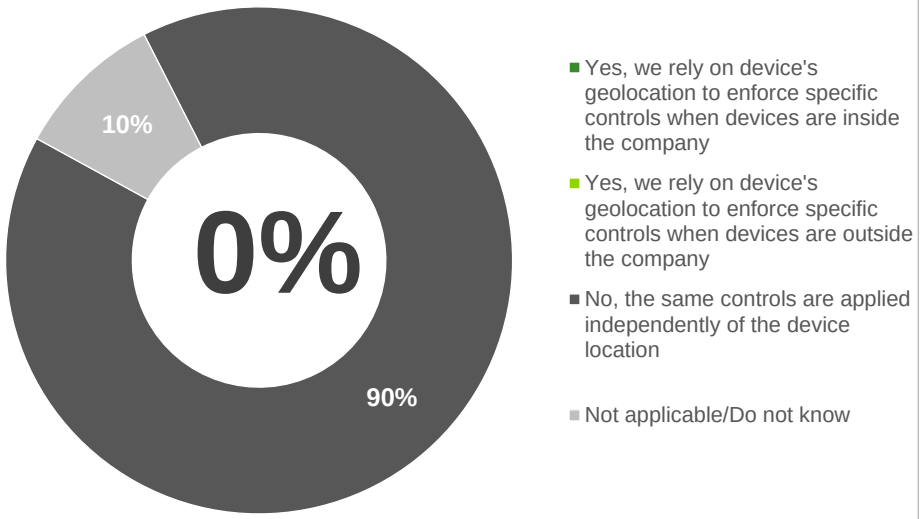
- **Most of the respondents rely on a dedicated encrypted container** to protect access to sensitive/ confidential corporate data
- **Still 29% of respondents rely on native device security features only** (among them, 80% use iOS devices)

© 2015 Deloitte Tax & Consulting

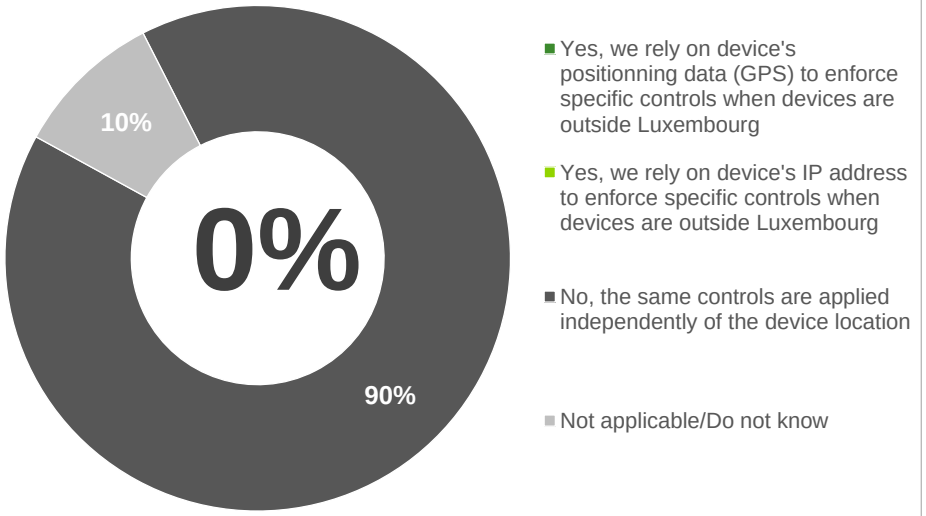
Security & Controls

Controls based on device location

Do you apply specific controls/restrictions when devices are inside or outside the premises of the company?



Do you apply specific controls/restrictions when devices are outside the Luxembourgish borders?

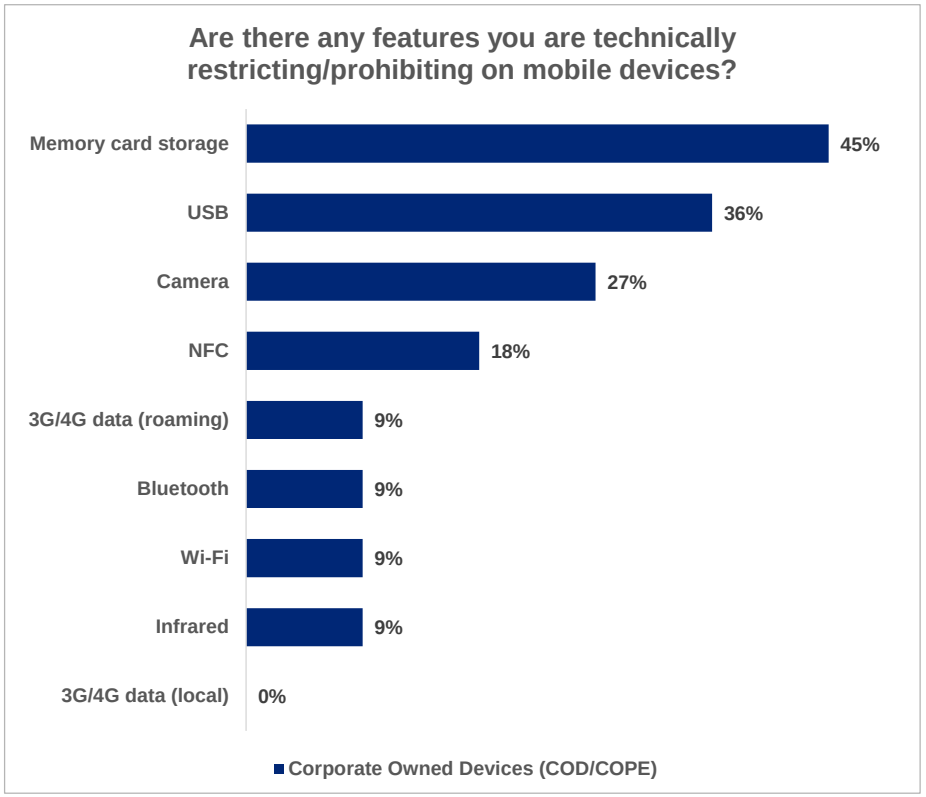


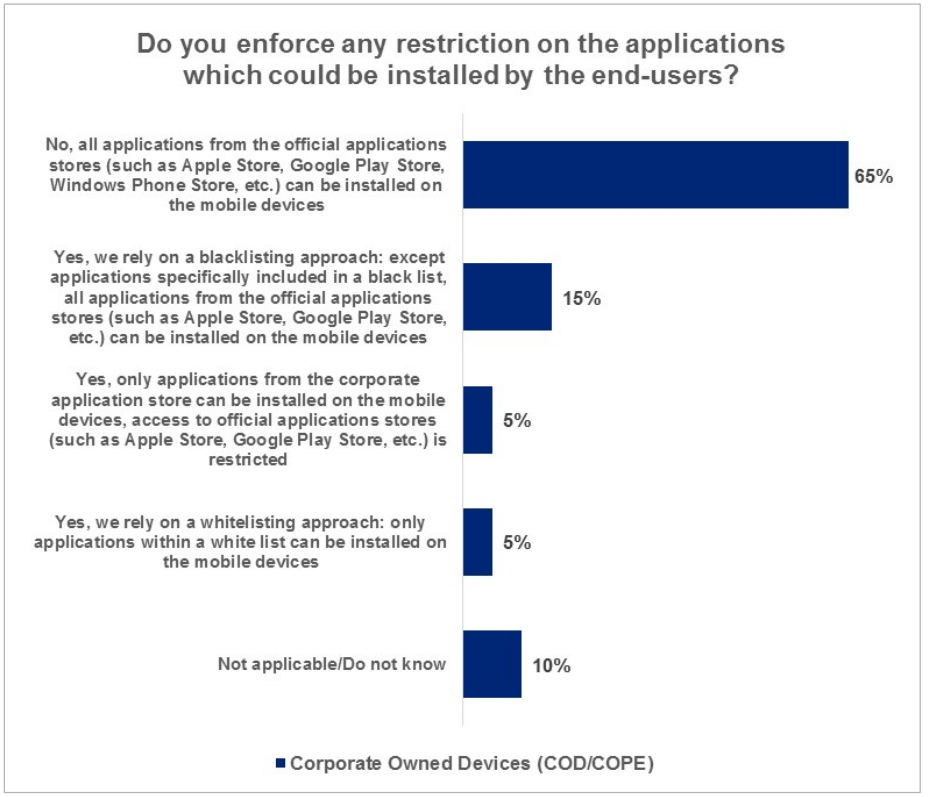
- **No specific controls based on the device location are implemented** by the surveyed organizations

© 2015 Deloitte Tax & Consulting

Security & Controls

Specific restrictions on mobile devices



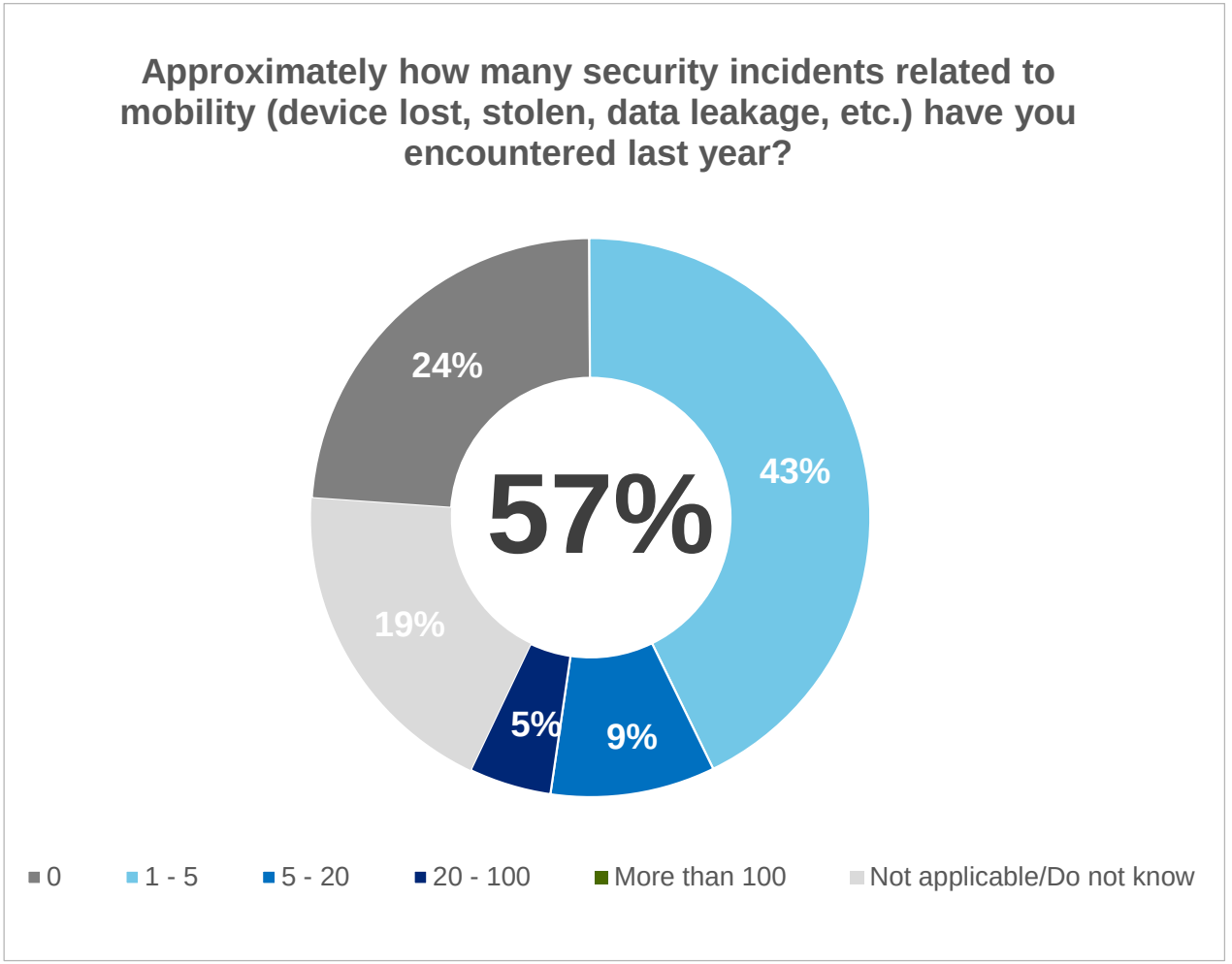


- **Very few usages are restricted on corporate devices**: with 45% of organizations blocking it, Memory Card storage is the most restricted feature
- In most organizations, all applications from the official applications stores can be installed

© 2015 Deloitte Tax & Consulting

Security & Controls

Security incidents



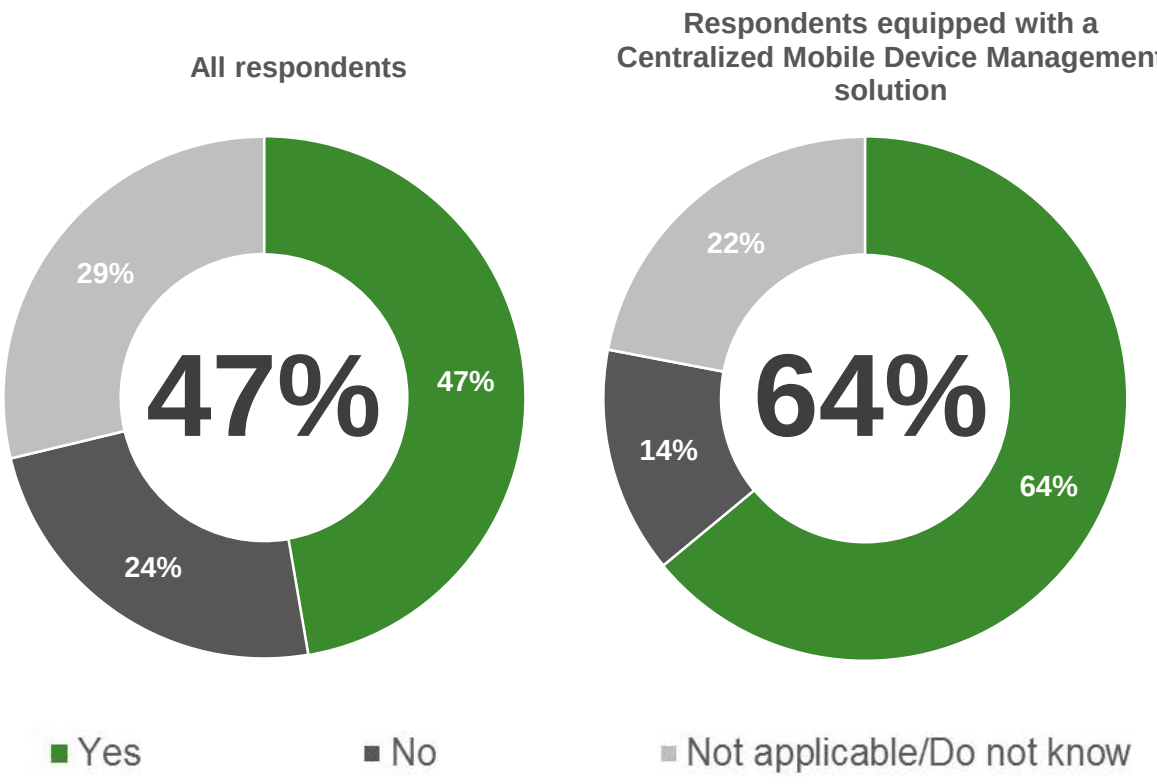
- At least **57% of respondents encountered security incidents related to mobile devices** during the last 12 months (knowing that 19% of respondents do not know)
- Number of incidents is proportional to the size of the organization
- In the majority of cases, and regardless of the organization size and mobile technology adopted, **remote wipe is used to limit impact of such incidents**

© 2015 Deloitte Tax & Consulting

Security & Controls

Detection of devices which have been rooted or jailbroken

Do you have any specific control in place to detect devices which have been rooted or jailbroken?



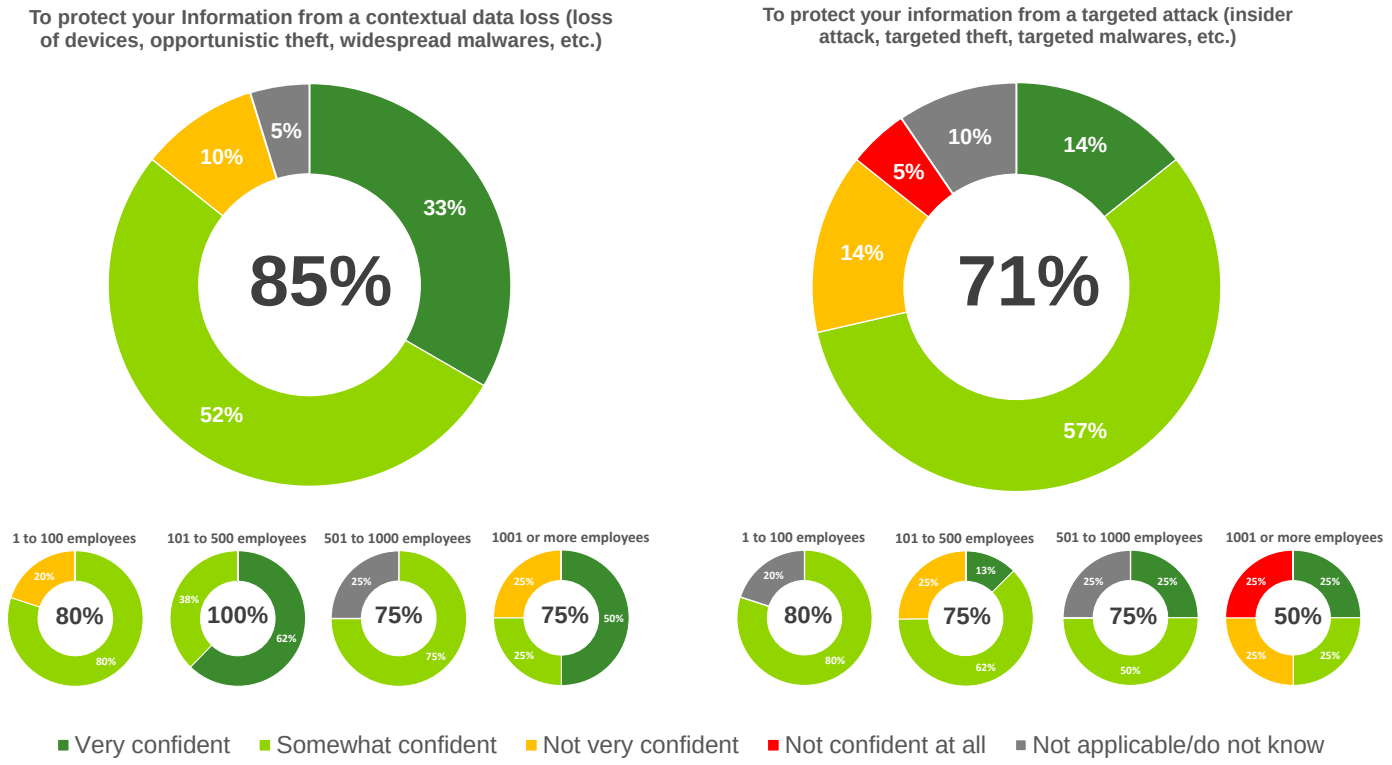
- Only **47%** of surveyed organizations have implemented specific controls to detect devices which have been rooted or jailbroken
- This proportion increases to **64%** where surveyed organizations are equipped with a centralized Mobile Device Management solution

© 2015 Deloitte Tax & Consulting

Security & Controls

Confidence in the effectiveness of security controls

How confident are you in the effectiveness of the security controls which have been implemented?



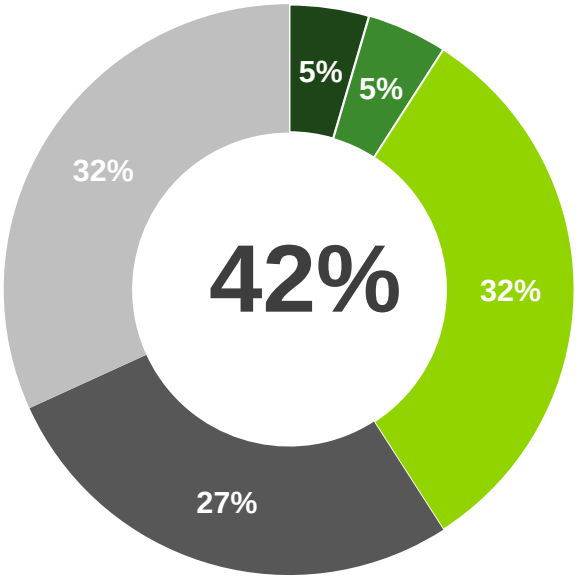
- Overall, the **confidence level in the effectiveness of the implemented security controls is good**
- **Largest surveyed organizations** (>1,000 employees) **tend to be less confident**: potentially more aware of the threat landscape and more exposed to targeted attacks on mobile technology

© 2015 Deloitte Tax & Consulting

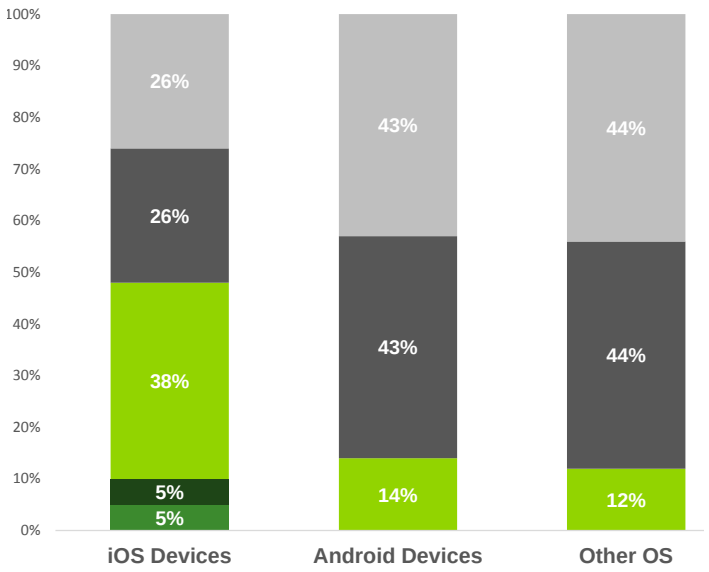
Infrastructure & Technology

Patch management requirements for Mobile Devices

Do you enforce specific patch management requirements for Mobile Devices?



Do you enforce specific patch management requirements for Mobile Devices (view by devices/OS type)?



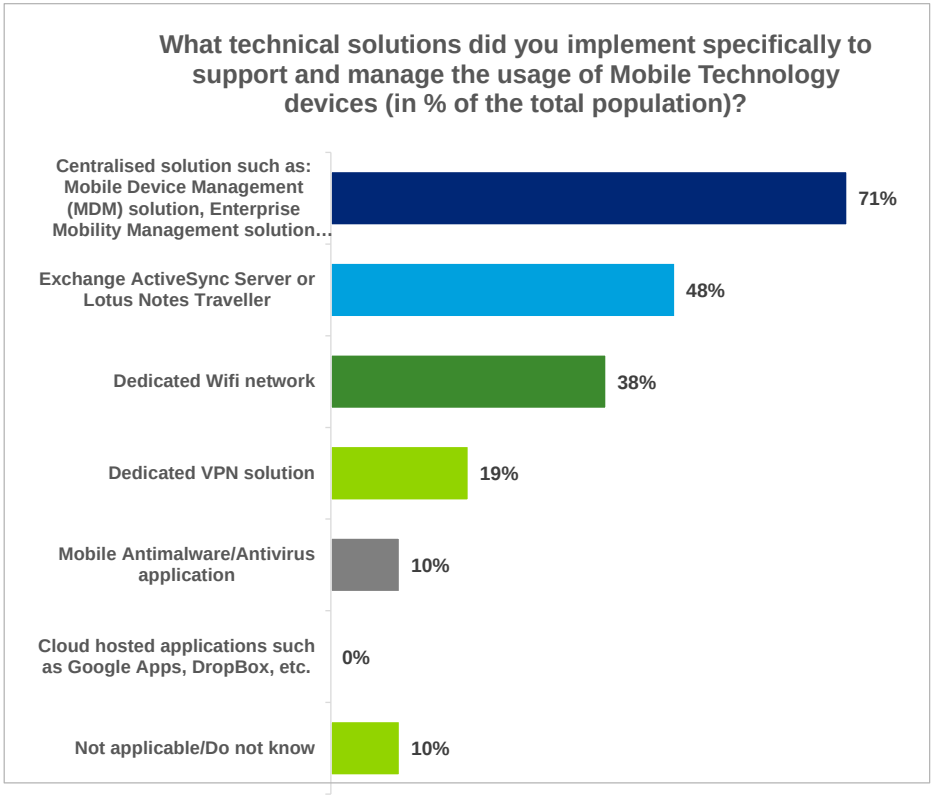
- Yes, only registered devices with an up-to-date operating systems (including latest patch) and up-to-date applications are allowed to access corporate data
- Yes, only registered devices with an up-to-date operating system (including latest patch) are allowed to access corporate data
- Yes, only registered devices with a specific OS and a minimum version (such as iOS 8.X) are allowed to access corporate data
- No, any registered device is allowed to access corporate data
- Not applicable/Do not know

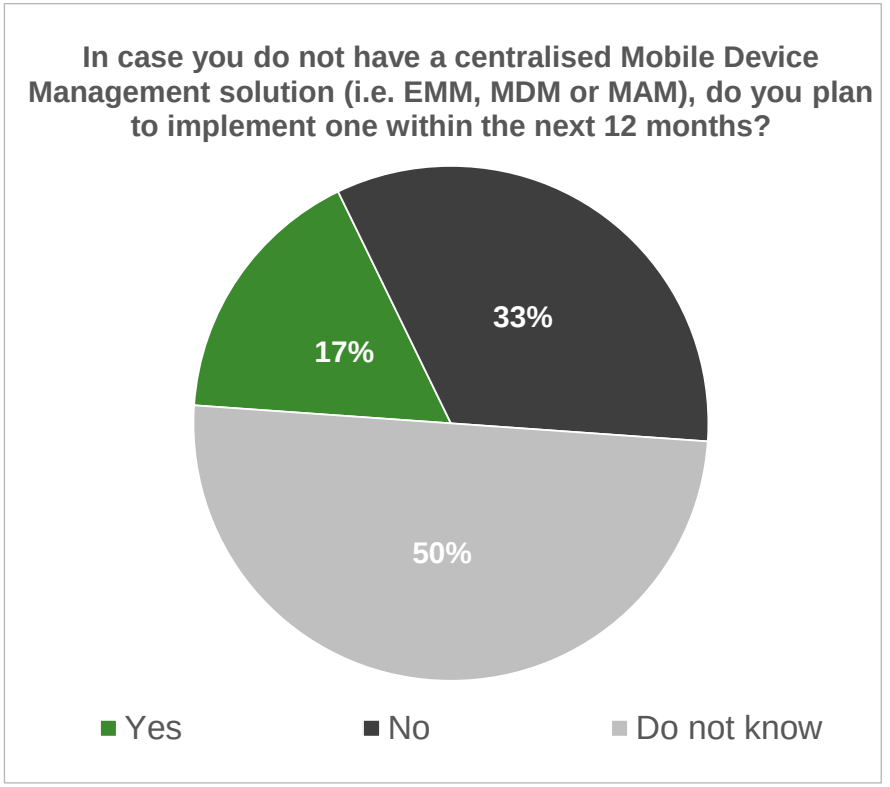
- Only **42% of surveyed organizations confirmed they enforce patch management requirements** for devices allowed to access corporate data
- Patch management requirements enforcement is higher for iOS devices than Android or other OS

© 2015 Deloitte Tax & Consulting

Infrastructure & Technology

Technical solutions in place



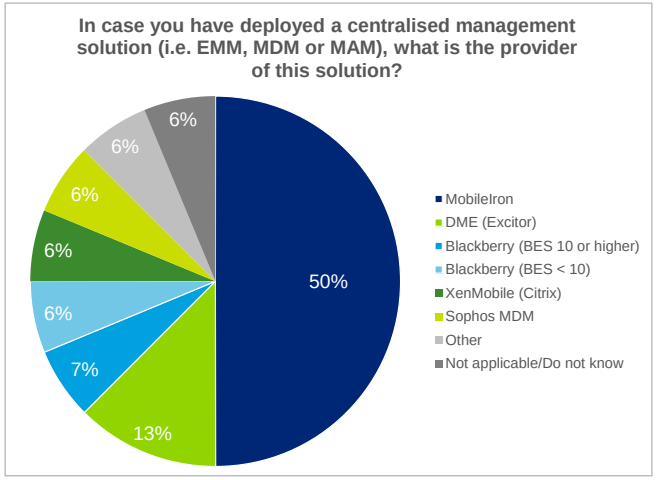


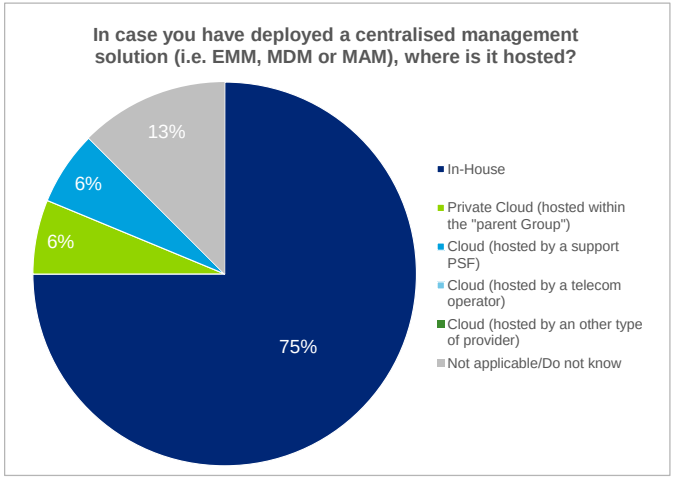
- Large surveyed organizations (>500 employees) have systematically deployed a Centralized solution (except one “Not applicable/Do not know”)

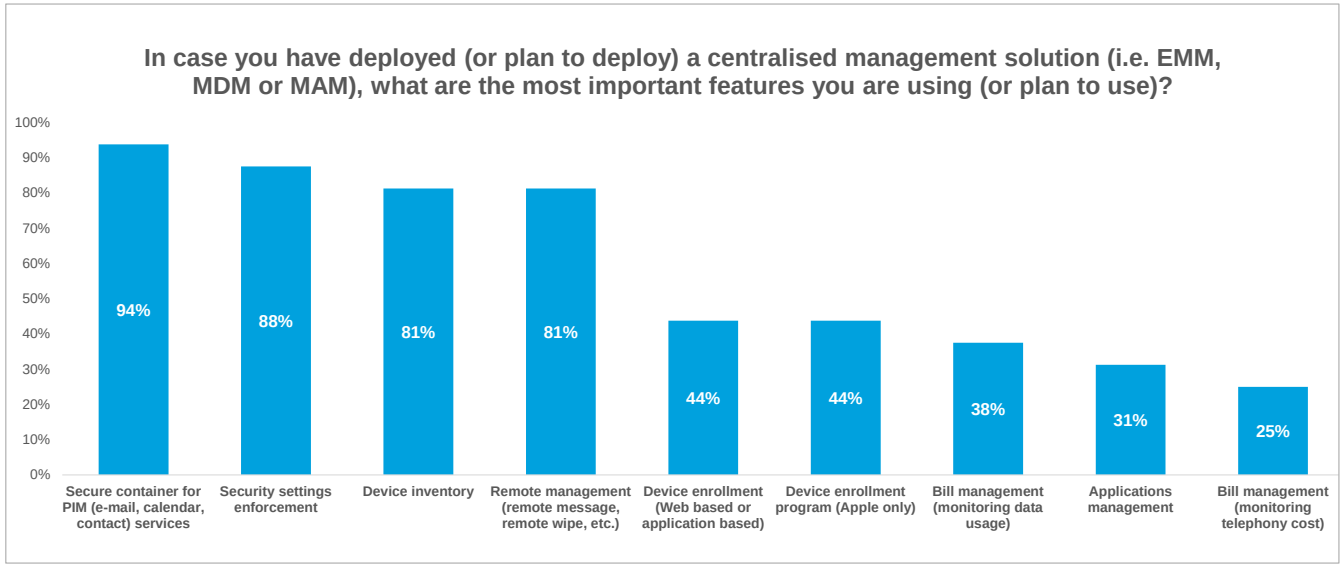
© 2015 Deloitte Tax & Consulting

Infrastructure & Technology

Centralized management solution (EMM, MDM or MAM)







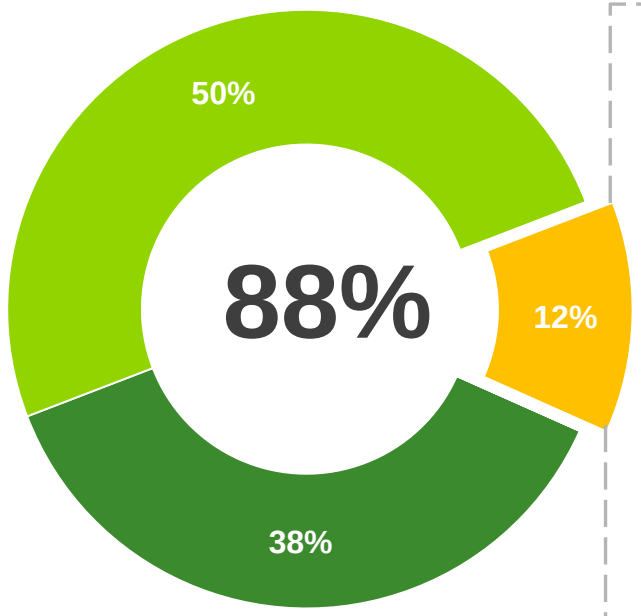
- **MobileIron has been chosen by 50% of the respondents** using a MDM solution
- Only 12% of the respondents have their MDM platform hosted in the cloud (by the Group or by a Support PSF)

© 2015 Deloitte Tax & Consulting

Infrastructure & Technology

Satisfaction with the implemented technical solutions

How satisfied are you with the technical solutions you have implemented?



- 1 - Exceeds my expectations
- 2 - Fully satisfied
- 3 - Satisfied
- 4 - Somewhat unsatisfied
- 5 - Unsatisfied
- Not applicable/Do not know

Current limitations

- Difficulties to address non-PIM use cases (containerization of business applications is complex)
- User-friendliness of non-native e-mail/calendar applications
- MS Office document viewer applications should be improved

Additional limitations for Non-MDM users:

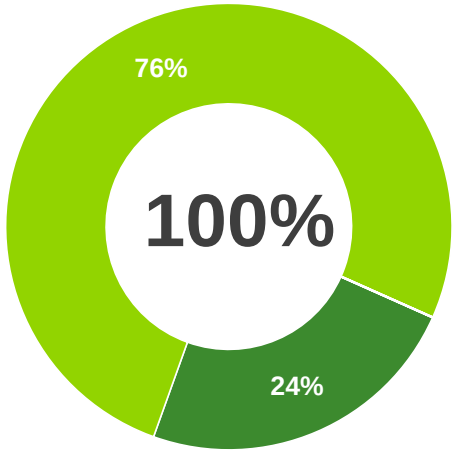
- Limited centralized management capabilities
- No ability to manage other devices than BES <10 + end of support

- **88% of surveyed organizations are at least satisfied** with the technical solutions implemented to support mobile technology
- **User-friendliness of PIM applications** and **ability to containerize business applications** become **key differentiators** for mobile management solutions

© 2015 Deloitte Tax & Consulting

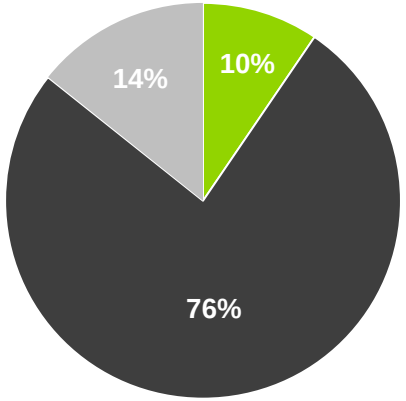
Value & Perception

Based on feedback from lines of business and other internal sources, how effective are mobile technology initiatives at meeting the needs and expections of the organisation ?



- Very effective
- Somewhat effective
- Ineffective
- Not applicable/do not know

What is your position regarding the usage of wearable technologies (such as smartwatches, smartglasses, etc.) ?



- The usage of wearable technologies is already covered and controlled by our policies
- We expect that the corporate usage of wearable technologies will bring an added value for our company within the next 2 years
- We expect that the usage of wearable technologies will be covered and controlled by our policies within the next 2 years
- The usage of wearable technologies has not been considered yet
- Not applicable/do not know

- **100% of the respondents are confident in the effectiveness of their mobile solutions** to satisfy the needs of their business
- Only 10% of the respondents have already considered the usage of wearable devices

© 2015 Deloitte Tax & Consulting

Key Definitions

Terms	Definitions
Mobile Technologies	In this study, by Mobile Technologies we mean the usage of Mobile devices (smartphones and tablets such as Blackberry devices, iOS devices, Android devices, etc.) and any systems used to manage and/or secure these devices. The usages of smartphones and tablets are distinct in the survey.
Corporate data	By Corporate data we mean any data which is stored or go through the information system of the company, such as e-mails, documents, access to corporate applications, etc.
COD	Corporate Owned Devices. This is applicable when the company pay for mobile devices which are used by the employees. Such devices could be Personally Enabled (COPE).
BYOD	Bring Your Own Devices. This is applicable when the employees use their own mobile devices to access corporate data.
MDM	Acronym referring to the Mobile Device Management solutions.
EMM	Acronym referring to the Enterprise Mobility Management solutions.
MAM	Acronym referring to the Mobile Applications Management solutions.

© 2015 Deloitte Tax & Consulting

Deloitte’s Information & Technology Risk
Key Contacts

Cyber Risk Services

Roland Bastin
Partner
+352 451 452 213
rbastin@deloitte.lu

Stéphane Hurtaud
Partner
+352 451 454 434
shurtaud@deloitte.lu

Laurent de la Vaissière
Directeur
+352 451 452 010
ldelavaissiere@deloitte.lu

Maxime Verac
Manager
+352 451 454 258
mverac@deloitte.lu

© 2015 Deloitte Tax & Consulting

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/lu/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s more than 220,000 professionals are committed to becoming the standard of excellence.

In Luxembourg, Deloitte consists of more than 90 partners and about 1,800 employees. For over 65 years, Deloitte has delivered high added-value services to national and international clients. Our multidisciplinary teams consist of specialists from different sectors delivering harmonized quality services to our clients in their field.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2015 Deloitte Tax & Consulting