Gouvernance et contrôle des Systèmes d'Information

RÉFÉRENCE DSI

Jour 7 : BYOD – Gouvernance et Contrôle du risque

Jean-Marc Montels
Maximilien Stebler
Philippe Tronc

Le BYOD

Définitions :

BYOD = « Bring Your Own Device »

- Pratique qui consiste pour une entreprise publique ou privée de permettre, sous certaines conditions, à ses salariés, consultants ou prestataires extérieurs d'utiliser leurs matériels personnels (ordinateurs portables, tablettes et smartphones) à des fins professionnelles.

- La Commission générale de terminologie et de néologie traduit officiellement l'acronyme en AVEC pour « Apportez Votre Equipement Personnel de Communication » (JO du 24 mars 2013)

Le BYOD

Quelques définitions :

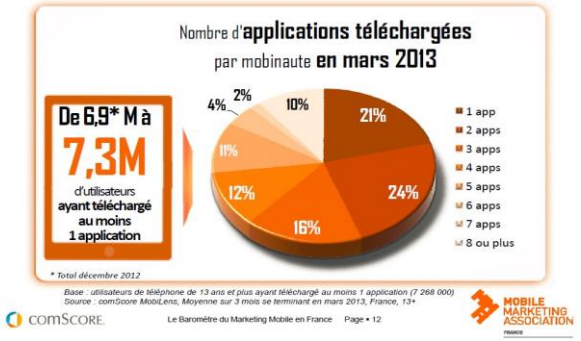
- Ce que BYOD est :
  - « Bring Your Own Device »
  - « IT consumerisation »
  - « AVEC » Apportez Votre Equipement personne Communication
  - « CYOD » Choose Your Own Device
  - « COPE » Corporate Owned, Personally Enabled
- Et aussi :
  - « Bring Your Own Cloud »
  - « Bring Your Own Application »
- Et demain :
  - « WearWare »

The Time Of The BYOC (Bring Your Own Cloud)

Les enjeux du côté des utilisateurs :

Le terminal mobile est un objet personnel !

http://www.slideshare.net/WSIdee/mettez-votre-entreprise-dans-le-tlphone-de-vos-clients



Le BYOD

Les enjeux du côté des métiers :

Dans le but de saisir de nouvelles opportunités, les lignes métiers mettent en place de nouvelles applications sur les terminaux.

Impact des tendances structurantes de la transformation numérique sur les RH

(sondage réalisé auprès du groupe de travail)

26% - Gestion de la mobilité
19% - Le *Cloud Computing*
14% - Le bénéfice des dynamiques collaboratives
9% - Les services associés
9% - Le SI : plateforme de services pour l'entreprise

la charte de Cisco, applicable à tous les terminaux et dans toute l'entreprise, a donné des gains de productivité équivalents à 30 minutes par employé par jour.

30+ minutes

.

vmware

Source : Etude réalisée par Vanson Bourne pour VMware en mars et avril 2013 auprès de 250 DSI et 500 salariés français - © Rumeur Publique

Le BYOD

Les enjeux du côté de la DSI :

Le type de terminaux ainsi que le type d'applications sont très hétéroclites

Les utilisateurs privilégient la facilité d'utilisation des terminaux en fonction de leurs préférences.

Les applications des terminaux mobiles ont souvent recours à plusieurs services de collaboration et de canaux de communications

Les utilisateurs ont en moyenne plus d'un terminal, les données de l'entreprise peuvent se trouver sur ceux-ci.

Augmentation drastique du nombre de terminaux à gérer.

Nouvelles technologies pour construire des applications natives, hybrides et web pour les terminaux mobiles

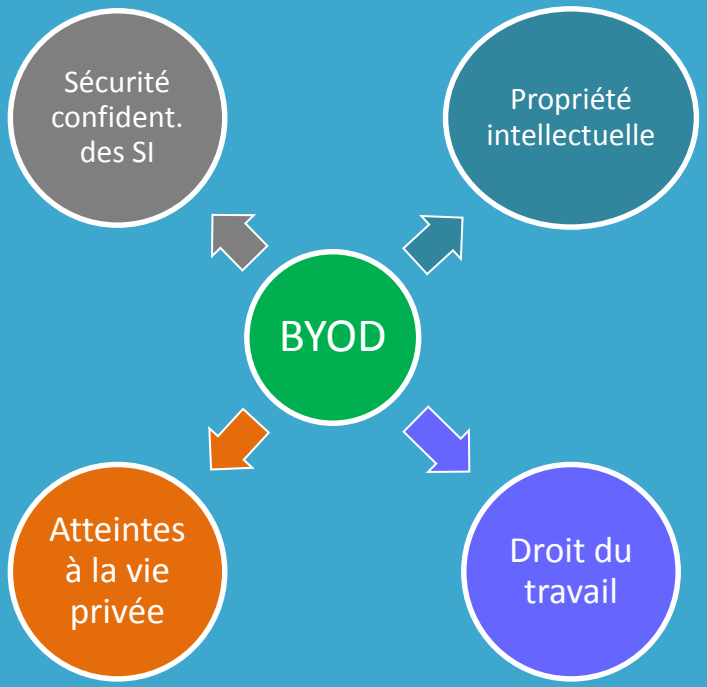
Le BYOD

Une approche globale

BYOD 2014+	Challenges
iOS Android Ultrabooks 	Comment fournir un service de qualité à mes utilisateurs et à mes invités ?
Quels réseaux ? 	Comment conserver la sécurité de mon réseau et de mes utilisateurs
Quels utilisateurs ? 	Comment minimiser l'impact sur mon infrastructure et sur mon organisation de support

Les risques liés au BYOD

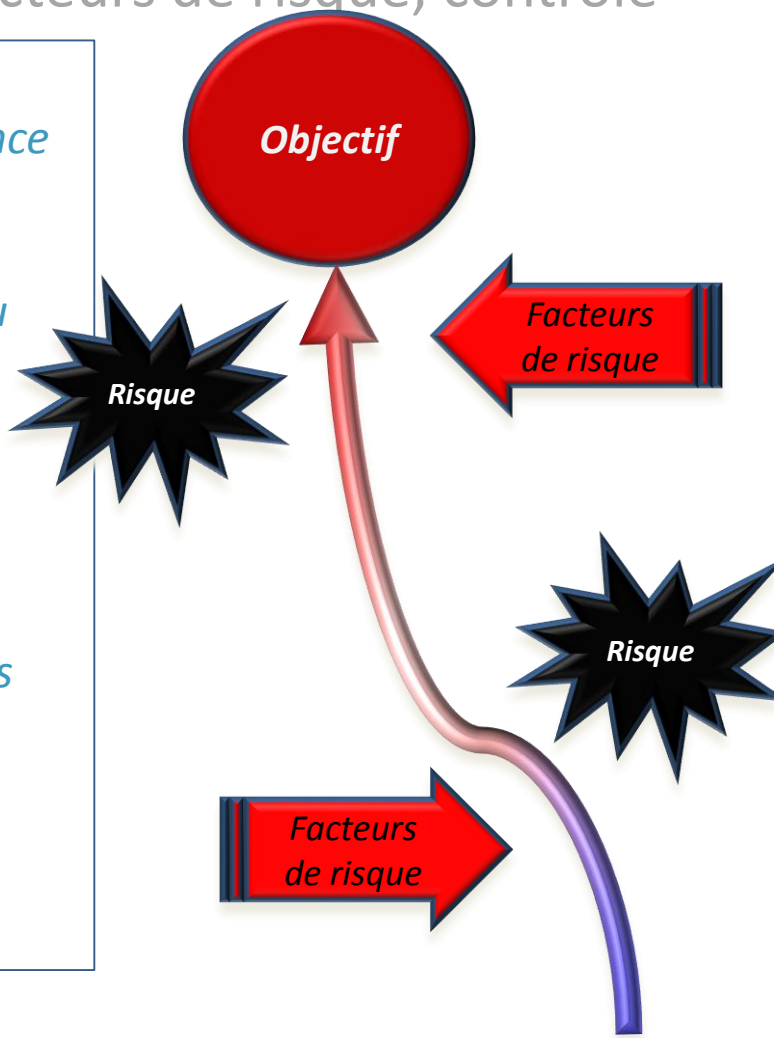
Les aspects juridiques et règlementaires



A cœur de la gouvernance : le risque

Risque, facteurs de risque, contrôle

- *Les facteurs de risques sont des événements ou des circonstances qui rendent la probabilité de survenance du risque plus importante.*
- *Le risque en tant que tel n'a que deux états : actif ou inactif.*
- *Il faut donc maîtriser (contrôler) les facteurs qui peuvent activer le risque.*
- *Il est possible de transférer les risques (contrats commerciaux, assurances, réassurances) voire de les déléguer (sous-traitance avec engagements)*
- ***Décliner cette approche pour le BYOD***



Les risques liés au BYOD

La propriété intellectuelle

- Apporter son propre matériel en entreprise comporte des risques en termes de respect des droits de propriété intellectuelle des tiers :
  - Exemple : Non-respect du périmètre des licences souscrites par un salarié à titre personnel. l'utilisation quotidienne dans le cadre de son travail d'un logiciel non destiné à un usage commercial.
  - « La violation de l'un des droits de l'auteur d'un logiciel(…) », constitue un délit de contrefaçon selon Art. L.335-3 du Code de la propriété intellectuelle.
  - Même si à l'origine, il y a faute du salarié (usage non autorisé d'un logiciel) c'est l'entreprise qui est civilement responsable. Responsabilité du commettant (employeur) du fait de ses préposés (salariés). Art. 1384 al. 5 du code civil.

Les risques liés au BYOD

Droit du travail

- Utiliser son appareil personnel dans un cadre professionnel génère des problématique relevant du droit du travail, et nécessite une réflexion sur la politique RH de l'entreprise:
  - Exemple : Une entreprise permet à certains salariés d'utiliser leur smartphone à des fins professionnelles (VIP…), mais le refuse à d'autres…
  - Exemple : Un salarié envoie régulièrement des mails professionnels et répond souvent à des clients sur son smartphone personnel en dehors de ses heures de travail….
  - « Nul ne peut apporter aux droits des personnes et aux libertés individuelles collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché »
  - Risques juridiques :
    - Discrimination pratiquée au sein de l'entreprise.
    - Eventuelle requalification d'une partie du temps passé hors de l'entreprise en temps de travail (heures supplémentaires-> contestation du montant des indemnités,…)

Les risques liés au BYOD

Atteintes à la vie privée

- Le BYOD soulève des problématique en matière d'atteintes à la vie privée:
  - Exemple : Un salarié apporte sa tablette sur son lieu de travail. L'employeur souhaite consulter fichiers et dossiers pendant une pause.
  - Risques juridiques : Confusion entre **données privées**, auxquelles l'employeur ne peut y avoir accès sans le consentement et hors de la présence du salarié et **données professionnelles** contenues sur un outil personnel
    - « Droit au respect de la vie privée du salarié (art.9 du Code civil), même sur son lieu de travail ». « Fichiers crées par un salarié grâce à l'outil informatique sont présumés professionnels : l'employeur peut y accéder librement ». Pour les « Fichiers/mails identifiés « PERSONNEL » l'employeur peut y avoir accès qu'en présence du salarié, ou si celui-ci a été dûment appelé »
    - Une clé USB connectée à un outil informatique mis à disposition est présumée être utilisée à des fins professionnelle…
  - Applicable aux smartphones, tablettes ou ordinateurs portables connectés au SI de l'entreprise ? Aucune jurisprudence à l'heure actuelle…

Les risques liés au BYOD

Sécurité - confidentialité des SI

- Le BYOD entraine des risques en termes de sécurité des SI et d'atteintes à la confidentialité des données.
  - Exemple :
    - Le vol ou la perte du device personnel avec des données de l'entreprise.
    - la mauvaise protection du device contre les malwares, Spywares, Virus.
    - La non connaissance par l'utilisateur des règles élémentaires de sécurité en terme de réseau, de gestion des mots de passe…
    - Le dépôt des données sur des sites hors de contrôle de l'entreprise : qualité de service, Patriot Act, départ du collaborateur…
  - En Droit, le caractère confidentiel de certaines informations résulte de la volonté des parties (ex. : clause de confidentialité dans le contrat de travail)
  - Certaines données ont un caractère confidentiel, secret ou sensible en application de la réglementation en vigueur
  - Risque de coupure des services SI impliquant une discontinuité de service -> baisse de productivité

Les risques liés au BYOD

Synthèse

BYOD : Un défi juridique à anticiper

- Il n'existe aucun cadre juridique ou règlementaire pour le BYOD. A l'heure actuelle aucun texte légal ou règlementaire n'encadre cette pratique. Un vide juridique
- Le Byod soulève de nombreuses problématiques juridiques qu'il conviendra d'appréhender.

Les solutions

- **Anticiper** les risques évoquées
- **Encadrer** l'utilisation du BYOD au sein de l'entreprise en prévoyant des règles claires assorties de sanctions en cas de non respect.
- **Elaborer** une politique DSI et RH globale en la matière

Elaborer / Actualiser le « Charte informatique » de l'entreprise en concertation avec la DSI s'agissant des solutions « techniques » du BYOD

Les risques liés au BYOD

Synthèse

BYOD / Risques	Ce qui doit être prévu
Propriété intellectuelle	➢ Révision de la politique de gestion des licences de logiciel.
	➢ Informer les salariés des terminaux/logiciels tolérés.
	➢ Obligation générale de respecter la réglementation PI
Droit du travail	➢ Révision des contrats de travail (condition d'usage d'un smartphone …)
	➢ Prévoir la procédure à appliquer en cas de départ / absence d'un salarié
	➢ Opposabilité de la charte informatique aux salariés
Atteintes à la vie privée	➢ Mise en place de procédures pour la séparation des données personnelles / professionnelles
	➢ Mise en place de la protection des données professionnelles
	➢ Mise en place d'une politique de surveillance des données
	➢ Prévoir la procédure à appliquer pour accéder aux terminaux personnels en cas de risques ou d'urgence
Sécurité/Confidentialité	➢ Mise en place de mesures de sécurité (effacement des données à distance, antivirus, MDM, MDS,…)
	➢ Protection des login / mots de passe
	➢ Mise en place de mesures en cas de perte/vol d'un matériel
	➢ Obligation générale de confidentialité / vigilance des salariés

- Le phénomène du BYOD est un risque mais peut être transformé en une opportunité de création de valeur.
  - Un outil commercial performant.
  - Attraction des talents
  - E-réputation.
  - Satisfaction des utilisateurs
  - Productivité
  - …

La Gouvernance du BYOD

La gouvernance du BYOD

Les règles de base

Une structure de gouvernance

Objectif : BYOD est soumis à la surveillance et au suivi par le management

- La politique BYOD doit être approuvée par la Direction Générale.
- La Direction Générale reçoit un rapport régulier sur les usages BYOD.
- La Direction Générale reçoit un rapport régulier sur la gestion des risques.

La Politique BYOD

Objectif : Les règles concernant les initiatives BYOD sont définies, documentées, validées, implémentées et maintenues.

- Accord employé/entreprise sur le BYOD = Politique d'usage des périphériques mobiles.
- Les processus BYOD sont intégrés dans la politique et les règles RH.
- Un accès limité pour les tiers, lorsqu'ils se connectent au réseau et au système informatique de l'entreprise
- Les exceptions à la politique BYOD sont listées et validées.

La gouvernance du BYOD

6 points incontournables

Légal

Objectif : Les procédures BYOD sont conformes aux exigences légales et minimisent les risques d'exposition de l'entreprise aux actions juridiques.

- Veille juridique pour identifier les impacts potentiels sur l'approche BYOD.
- Mettre à jour les procédures BYOD en fonction.

Support utilisateur

Objectif : Implémenter une fonction support dédiée au BYOD.

- Identifier les compétences nécessaires à l'environnement BYOD.
- Mettre en place les processus pour supporter l'usage du BYOD en entreprise.

La gouvernance du BYOD

6 points incontournables

Gestion des risques

Objectif : Le BYOD est soumis à des processus d'évaluation des risques.

- Evaluation initiale des risques (avant la mise en œuvre du programme)
- Evaluation continue des risques

Formation

Objectif : Une formation orientée utilisateurs BYOD avec suivi régulier

- Formation initiale : Les utilisateurs du BYOD doivent suivre une formation initiale sur la politique et procédures BYOD.
- Sensibilisation et formation à la sécurité de manière annuelle.

La gouvernance du BYOD

6 points incontournables

Sécurité du périphérique mobile

Objectif : Les utilisateurs doivent maintenir les procédures de sécurité de base.

- Restriction des accès au périphérique mobile.
- Accès aux données / cryptage / protection des données.
- Appareils mobiles sont tenus d'avoir des défenses anti-malware standards.

Gestion des périphériques

Objectif : identifier, contrôler et entretenir les éléments de configuration

- Gestion centralisée des périphériques : caractéristiques, configuration, propriétaire, ...
- Une Gestion centralisée des procédures informatiques / Surveillance de l'utilisation BYOD.
- La gestion à distance des périphériques

La gouvernance du BYOD

Conclusion

Le BYOD renforce les besoins en gestion et en gouvernance des données de l'entreprise

La gouvernance des données implique dans l'évaluation, la création, le stockage, l'utilisation, l'archivage et la suppression des données et des informations. Elle comprend les processus, les rôles, les normes et les mesures qui assurent l'utilisation efficace et efficiente des données et de l'information pour permettre à une organisation d'atteindre ses objectifs.

- Politiques de données
- Le classement des données et leur évaluation
- Qualité des données (exactitude, accessibilité, cohérence, exhaustivité,…..)
- La conformité des données aux aspects réglementaires
- La sécurité des données
- La propriété des données…

BYOD – Les outils

Un peu de culture « technique »

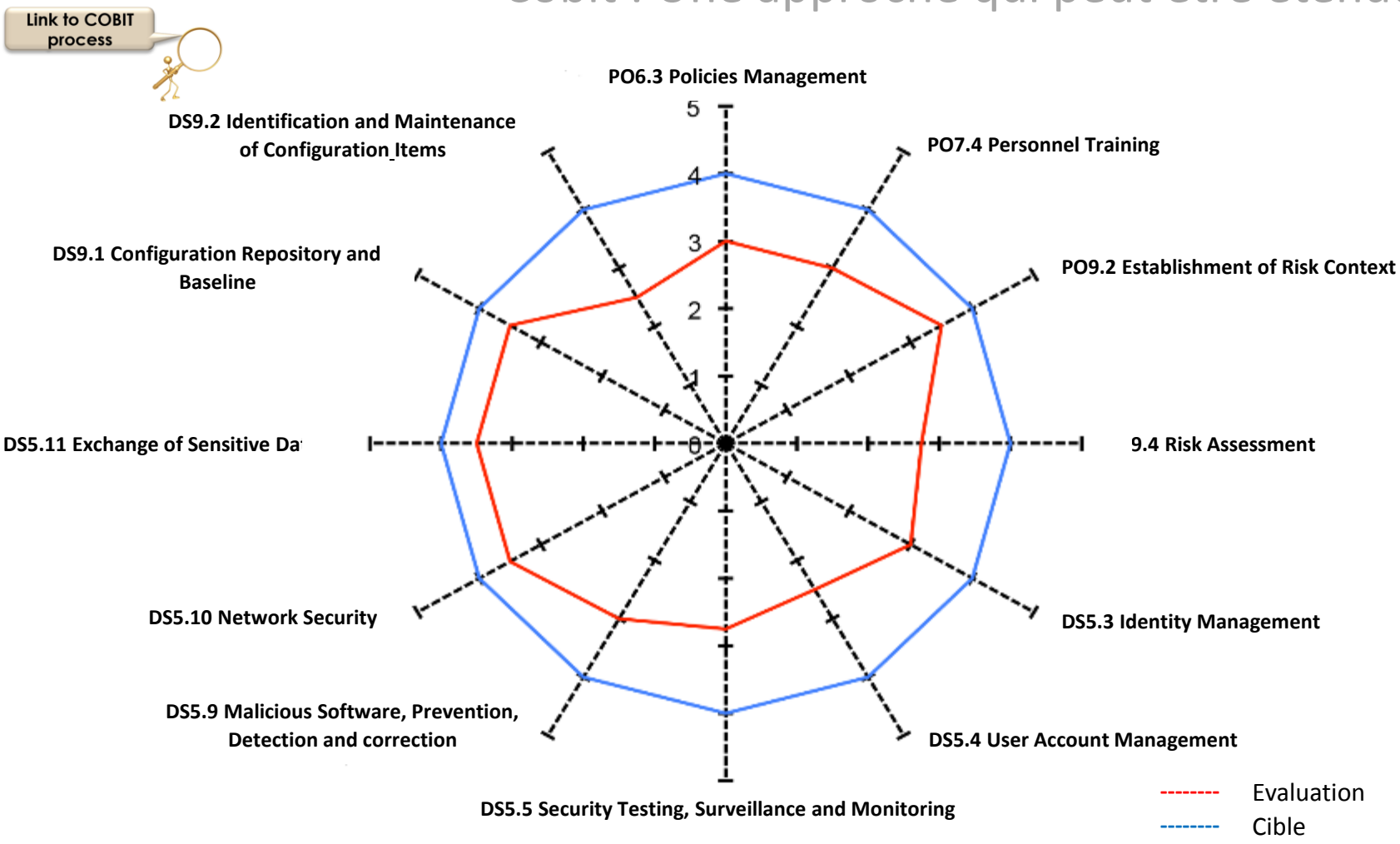
La matrice des modèles

Qui est propriétaire de quoi ?

Appellation	Nom Complet	Description	Propriétaire du périphérique	Propriétaire des applications	Propriétaire du réseau poste de travail	Niveau de gestion pour l'entreprise
	Modèle standard	Ce modèle est celui classique qui considère que les périphériques dits mobiles sont gérés comme des postes de travail bureautiques traditionnels	Entreprise	Entreprise	Entreprise	Périphérique
BYOD	Bring your own Device	L'entreprise permet aux utilisateurs d'apporter leurs périphériques personnels pour se connecter aux services délivrés par l'entreprise. Lorsque cette stratégie est étendue à d'autres types d'appareils (stockage, etc.) on parle alors de BYOT « Bring Your Own Technology »	Utilisateur	Utilisateur et Entreprise	Entreprise	Périphérique (avec accord de l'utilisateur)
BYOA ou BYON	Bring Your Own Access Bring your Own Network	L'entreprise ne gère plus de parc informatique, ni de réseau de type poste de travail. Chaque utilisateur est libre de contracter avec un opérateur réseau et de choisir la nature de sa connexion (WiFi, femtocell, tethering). Ce modèle se comprend si l'ensemble des applications de l'entreprise sont accessibles via un accès par Internet	Utilisateur	Utilisateur et/ou Entreprise	Utilisateur	Application
PYCA	Push Your Corporate Application	L'entreprise ne gère plus de parc informatique au sens des périphériques utilisés, et se préoccupe de mettre en œuvre et de tenir à jour un magasin d'applications qui lui appartient dans lequel l'utilisateur vient se servir s'il en a le droit	Utilisateur	Entreprise	Entreprise	Application
CYOD	Choose Your Own Device	L'entreprise permet à l'utilisateur de choisir un périphérique dans une liste délimitée qu'elle tient à disposition	Entreprise	Entreprise	Entreprise	Périphérique
COPE	Company Owned Personnally Enabled	L'entreprise choisit le périphérique, mais permet à l'utilisateur de se servir à des fins personnelles en y installant des applications dont il est le propriétaire	Entreprise	Utilisateur et/ou Entreprise	Entreprise	Périphérique
BYOA ou BYOS	Bring Your Own Application Bring your Own Software	L'utilisateur peut se servir d'applications personnelles dont il est le propriétaire ou l'utilisateur légal pour travailler dans le cadre de l'entreprise	Utilisateur et/ou Entreprise	Utilisateur	Entreprise	Application

Byod et Cobit

Cobit : Une approche qui peut être étendue



- 4 outils chez les leaders :
  - Xen mobile (citrix)
  - Jabber (Cisco)
  - Xenprise
  - Systèm Center (Microsoft)

- Une référence à suivre : Gartner Magic Quadrant for Mobile Device Management

Les acteurs clés du MDM

Source Gartner Group

FIN

DE LA

SEPTIEME JOURNEE