



The image shows two logos. On the left, 'BYOB' is written in large, colorful, galaxy-themed letters. On the right, 'BYOD' is written in large, colorful letters, with 'B' in blue, 'Y' in purple, 'O' in orange, and 'D' in green. Above the 'BYOD' text are four icons: a smartphone, a mobile phone, a tablet, and a laptop. Below the 'BYOD' text is the phrase 'BRING YOUR OWN DEVICE'. Below the logos is a photograph of several people sitting around a wooden table, each using a mobile device (laptop, tablet, or smartphone).

BYOD: Bring Your Own Device

1

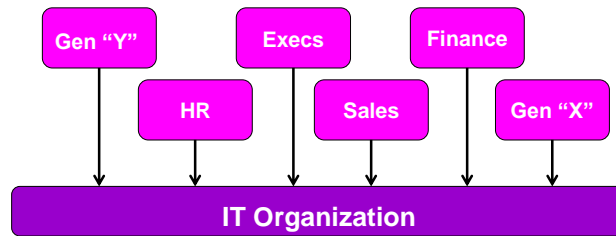
Definition

Bring your own device From Wikipedia, the free encyclopedia

Bring your own device (BYOD) refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications. The term is also used to describe the same practice applied to students using personally owned devices in education settings.

BYOD is making significant inroads in the business world. **In most cases, businesses simply can't block the trend.** Some believe that BYOD may help employees be more productive, increases employee morale and convenience by using their own devices and **makes the company look like a flexible and attractive employer, and attract new hires.**

BYOD Drivers



- Consumerization of Corporate IT
- Employers attempting to accommodate employee's digital preferences
 - Employees having greater influence in how they work

BYOD Examples

- Smartphones
- Laptops & Netbooks
- Tablets
- USB
- Digital Cameras
- Digital Cameras
- RFID/M-RFID
- Printers/Smart Cards
- Other Internet of things

Too Many Devices



BYOD: Bring Your Own Device

5

What Can Happen

- **Pressure from Senior Executives: make technology available; IT's desire - innovative and agile. Innovation versus Security.**
- **Lack of processes and procedures to prevent deployment outside of small (manageable) executive pool**
- **Devices deployed before standard security configuration is established and policies designed**
- **Devices can be deployed prior to implementation of enterprise support solution**
- **IT resources may have difficulty maintaining pace with hi-touch support model and highly mobile user base**

BYOD: Bring Your Own Device

6

Shades of BYOD

BYOD

- Bring your own device:
- Employees use their privately owned hard- and software
- IT-applications and company data of the employer are made available on the platform of the end-user

CYOD

- Choose your own device:
- Employer provides the hardware and the employee can choose e.g. the model

SYOD

- Smuggle your own device:
- People using a second tablet, smartphone or tablet
- Use that one also for company purposes next to the one provided by the employer

Amazing...



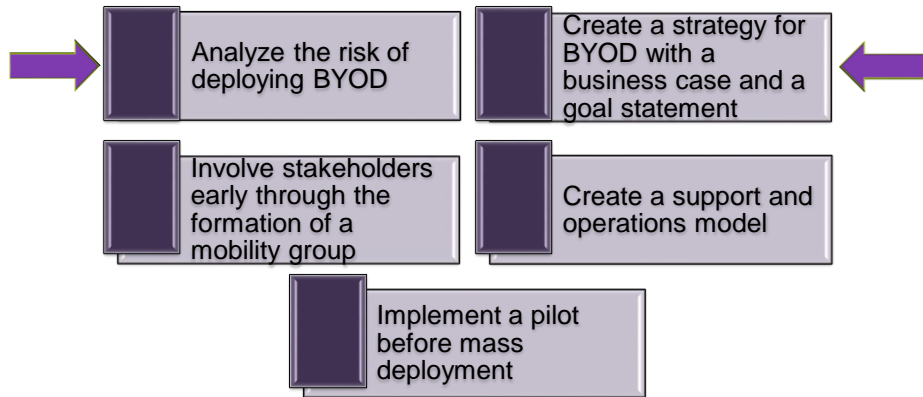
67% of cell phone owners check their phone for messages, alerts, or calls even when they don't notice their phone ringing or vibrating



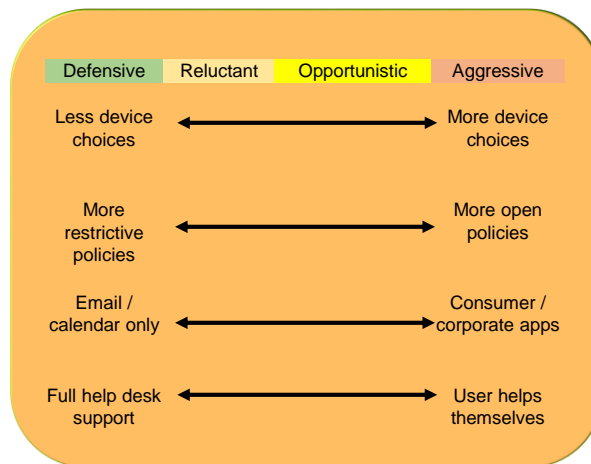
44% of cell phone owners have slept with phone next to the bed to make sure they didn't miss any calls, text messages, or other updates during the night

Source: Pewinternet.org

Implementing BYOD



Risk Tolerance



Successful Strategy



Trust Model

Assess the risk for common security issues on personal devices.

Outline remediation options — notification, access control, quarantine or selective wipe — issued depending on security concerns.

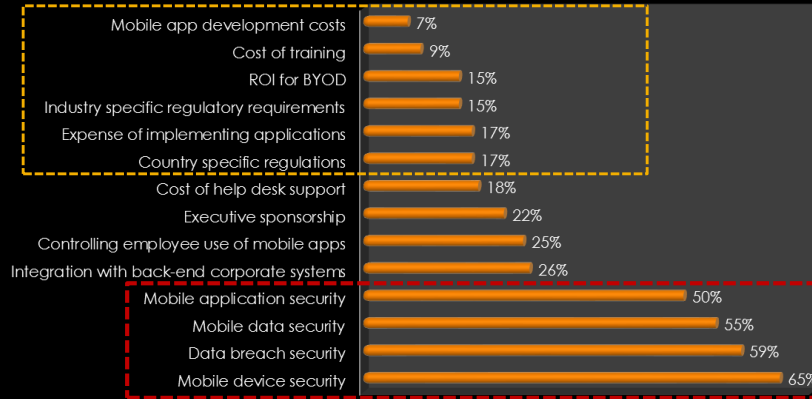
Set tiered policies for security, privacy and app distribution based on device ownership.

Clearly establish the identity of the user and device through certificates or other means.

Ensure that security policies are sustainable and flexible enough to support a positive user experience without compromising data security.

Challenges

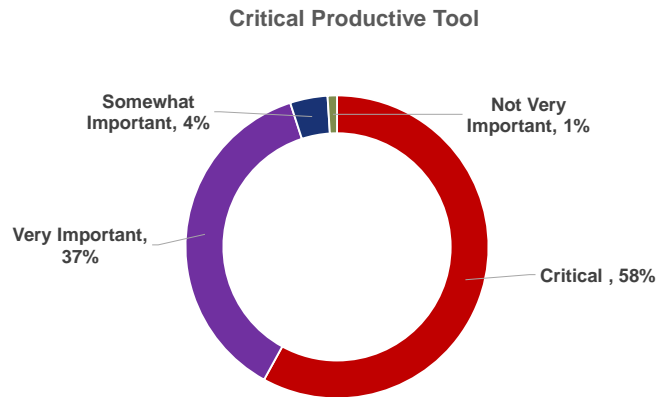
Challenges or barriers facing BYOD deployment



BYOD Statistics

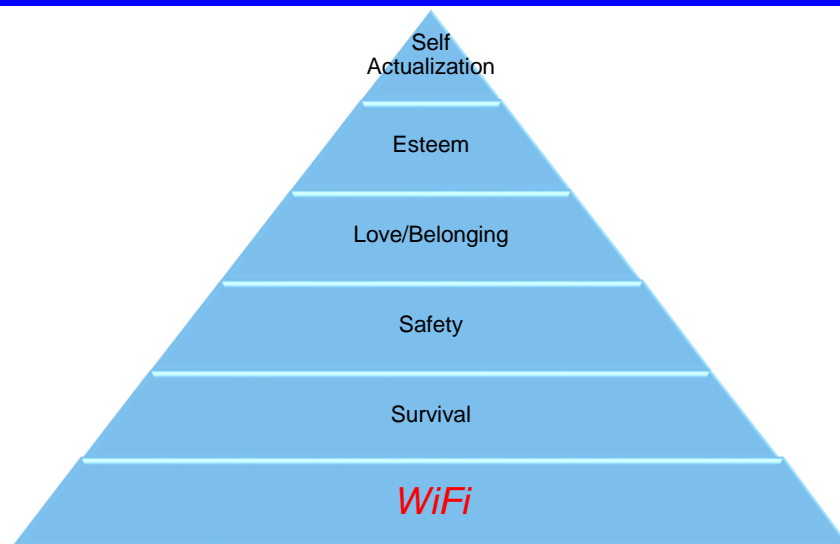
%	Explanation
67%	Of people use personal devices at work, regardless of the office's official BYOD policy (Source: Microsoft via CBS News)
77%	Of employees haven't received any education about the risks related to BYOD (Source: 2013 Data Protection Trends Research)
11%	Of end users access business applications from the corporate office 100% of the time (Source: Cisco)
46%	Of end users surveyed said network performance negatively affects mobile devices the most (Source: Cisco)
78%	Believe having a single mobile device helps balance employees' work and personal lives (Source: Samsung)
24%	Currently use a smartphone or tablet as their primary, work-related computing device (Source: Samsung)

Necessary Tool



Survey commissioned by Lookout and conducted by Enterprise Strategy Group.

Maslow's Hierarchy of Needs



Why BYOD Is a Concern

Unfriendly user keyboard leads to weak password

Devices are online longer and go more places

Easier to lose than laptop or tablet

Device defenses are not matured

Legit market for spyware

Users downplay risks associated with smartphones

Deploying BYOD

Initiation

Development

Implementation

Operations and Maintenance

Termination

Initiation Development Implementation Operations and Maintenance Termination

Before designing a mobile device solution

- Identify needs for mobile devices
- Provide a vision for how BYOD will support the organization's mission
- Create a high-level strategy for implementing mobile device solutions
- Develop a mobile device security policy and exceptions protocol
- Specify business and functional requirements for the solution

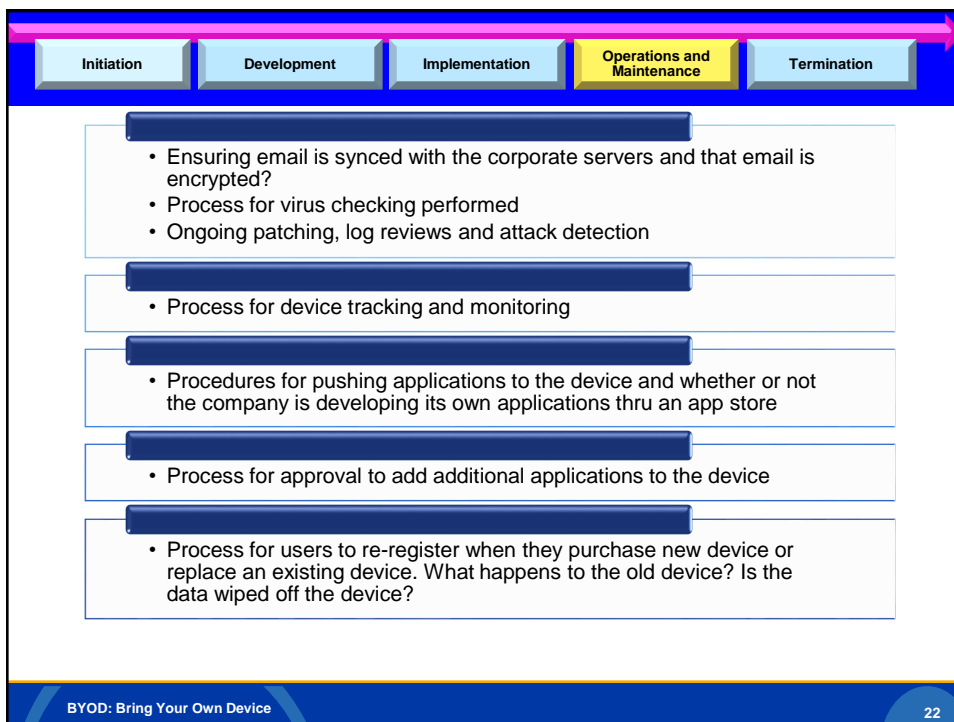
BYOD: Bring Your Own Device 19

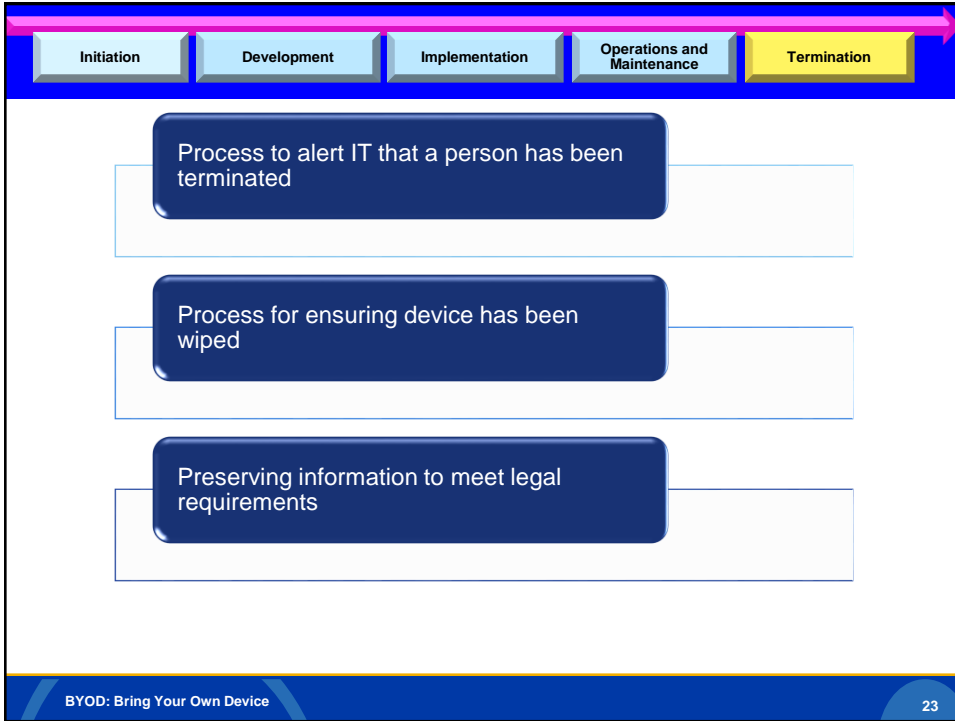
Initiation Development Implementation Operations and Maintenance Termination

Specify the technical characteristics:

- Authentication methods and the cryptographic mechanisms used to protect communications and stored data
- Types of mobile devices (brands, operating systems, etc.) to be authorized for use should also be considered, since they can affect the desired policies
- Mobile device security policy can be employed and enforced by all authorized clients
- MDM cloud based or internal
- Solution hosted by third party or internally

BYOD: Bring Your Own Device 20





Risk – Lack of Awareness

89%
unaware that smartphones can transmit confidential payment information such as credit card details without the user being prompted

67%
do not use keypad locks or passwords

65%
worry more about security on their laptop or desktop PC than their mobile device

Protiviti Survey - 2014

BYOD: Bring Your Own Device

25

Risk – Lost or Stolen

Unattended device

Unauthorized Access

Data theft

BYOD: Bring Your Own Device

26

Risks

Malware infection leading to leakage, corruption or unavailability of data

Leakage or compromise of sensitive data due to lost or improperly secured BYOD mobile devices

Negative publicity, loss of reputation, noncompliance with statutes, fines, and lawsuits

Ability to eliminate company data upon termination of employment or loss of the device


Supporting many different types of devices, operating systems and apps

Employee-owned BYOD devices are properly backed up at all times


Attack surface increase by a factor of 1,000 by the sheer number of vulnerable applications and devices the attacker is able to leverage

BYOD: Bring Your Own Device
27


Benefits




Improved business and employee collaboration



Increased productivity



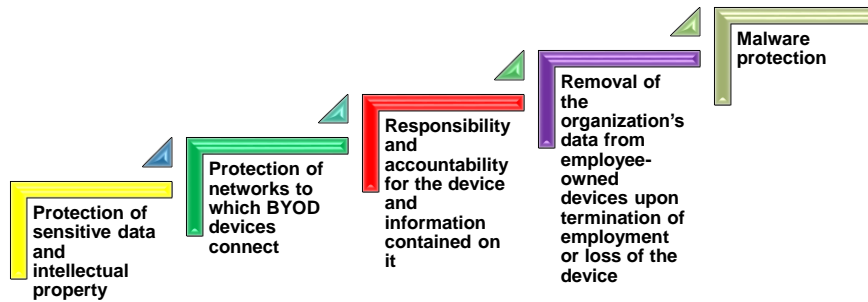
Attract / keep employees



Decreased worker latency

BYOD: Bring Your Own Device
28

Primary Security & Control Issues



Securing the Mobile Workforce

- 1 • Update Security and Privacy Policies
- 2 • Determine what internal resources to make available
- 3 • Create mobile provisioning / wipe/ support processes
- 4 • Determine technical requirements for management tools
- 5 • Select products that meet #4
- 6 • Implement and test
- 7 • Roll out – controlled
- 8 • Evaluate and test implementation against requirements
- 9 • Access logging and file integrity monitoring with centralized log repository
- 10 • Accessing content / internal resources

BYOD Program and Policy

BYOD: Bring Your Own Device
31

General technical considerations Financial reimbursement Technical support Liability

What

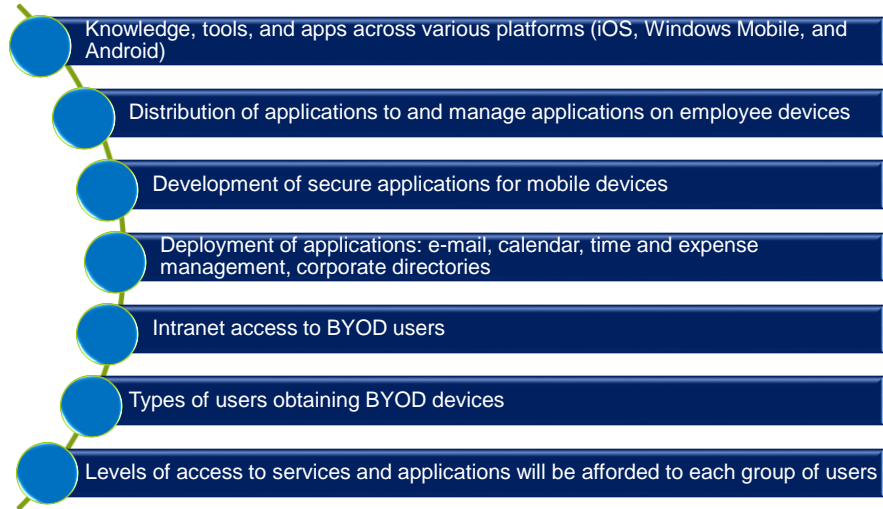
- Devices / mobile operating systems can we support?
- Are the security requirements at each level: devices, applications and data access?
- Risks are introduced by allowing access corporate data via personal devices?
- Level of tolerance do we have for those risks?

How

- Can we manage the deployment without risking sensitive data?
- Can we prevent intruding on the employee's right to privacy on their devices?

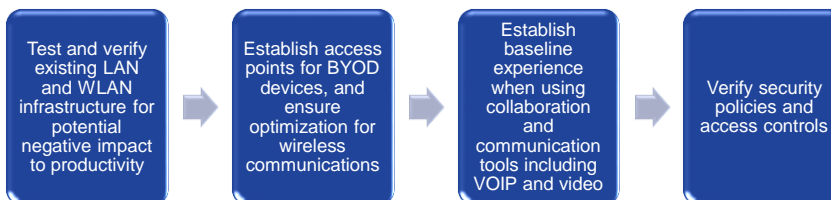
BYOD: Bring Your Own Device
32

TTC - Things to Consider



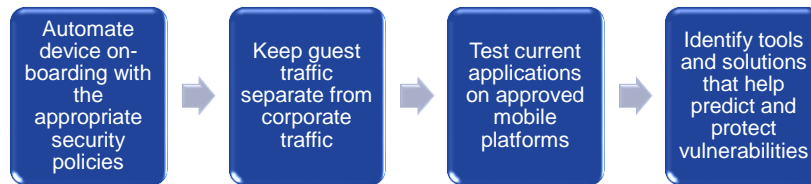
IT Checklist: Network

A dedicated mobility infrastructure and corresponding policies helps IT proactively mitigate many of the risks that arise when extending device, application, and data access.



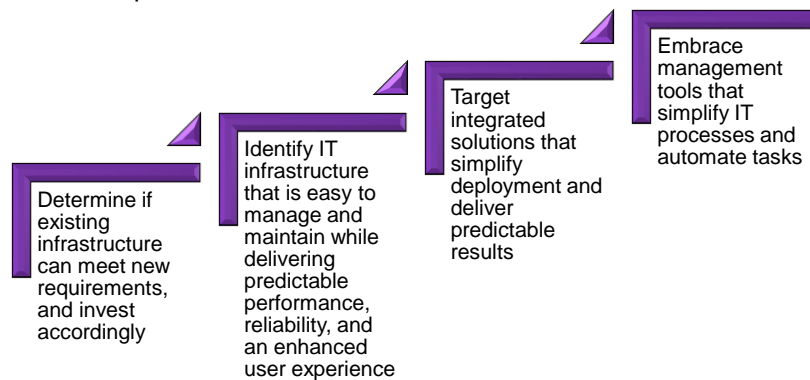
IT Checklist: Security

Security: an integral part of each step taken to enable a more productive business environment.



IT Checklist: Server & Storage

Infrastructure solution that provides improved management capabilities including the abilities to increase visibility, proactively detect potential problems, and automate routine IT tasks.



IT Checklist: Collaboration / Communication

File-sharing and e-mail are needed to promote reliable and efficient communications that will improve productivity. These applications require high bandwidth, which current networking IT may not be able to provide.

1. Evaluate tools with leading users who will embrace and promote collaboration
2. Deploy infrastructure that can meet performance demands of the business
3. Test various network access scenarios to ensure compatibility, and detect potential security issues
4. Test 1-to-1, and 1-to-many connection scenarios, including out-of-network connections

BYOD: Bring Your Own Device 37

General technical considerations
Financial reimbursement
Technical support
Liability

Determine how - and whether - to pay for employees' use of mobile devices. One of three basic categories:

	Direct Billing: organization buys the device, pays for its data plan, and all charges are billed directly
	Stipend: organization offers a monthly stipend to support the employee's use of the device, typically added to a paycheck
	Expense: organization does not purchase phones or data plans, but each department manager can approve or reject a certain amount of employee spending on these items, reimbursing the employee based on expense reports

BYOD: Bring Your Own Device 38

TTC – Financial Reimbursement

Reimbursement items: equipment, voice, data, etc. and the conditions (business vs. personal usage, manager approval)

Ineligible reimbursements: ringtones, 411 calls, etc.

Caps on reimbursements (fixed monthly stipend or maximum expense-back limits)

Full or partial reimbursement of device acquisition or replacement costs

Pay for services extended to employees on mobile devices

Employee provided with a smartphone for after-hours calls - receive overtime pay for taking those calls

General technical considerations

Financial reimbursement

Technical support

Liability

What levels of support will be provided?

Are all employees eligible for mobile access to company data and applications?

Restrict access based on role, title, manager approval, etc.?

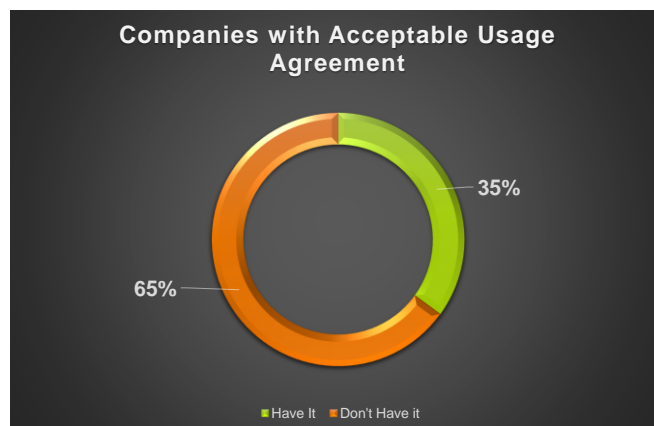
Restrict access to particular company applications or data? If so, which apps and data?

Support all devices? Only corporate data or apps?
Custom apps on personally owned devices?

TTC – Technical Support

- Regulations that govern data the organization needs to protect
 - Security measures needed (passcode protection, jailbroken/rooted devices, anti-malware apps, encryption, device restrictions, backup)?
 - Forbidden apps: IP scanning, data sharing, Dropbox
- Acceptable Usage Agreement (AUA)
 - Employees access: email, wireless networks or VPNs, CRM
 - Collection of work related data from employees' devices - personal data is never collected

AUA



Source: <http://www.rapid7.com>

General technical considerations Financial reimbursement Technical support **Liability**

Liability

- Who is responsible if the device is lost or stolen or the device is wiped and personal data is lost?
- Do BYOD procedures comply with legal requirements and minimize the organization's exposure to legal actions?
- Are Legal Hold policy and procedures in place / enforced?
- Is Corporate content on employee devices managed without interfering with personal use?
- Must users sign an acceptable use policy before connecting personal devices to the corporate network?
- Does the Policy address the use of devices by users other than the corporate end user?

BYOD: Bring Your Own Device 43

Control Considerations

People	Process	Technology
<ul style="list-style-type: none"> P & P End User Responsibilities Training 	<ul style="list-style-type: none"> Request access to data Distribution of access when requested Tracking these requests Policy signed before access 	<ul style="list-style-type: none"> Encrypt data Strong passwords Auto wipe Locking Remote wipe Authentication controls to corporate network

BYOD: Bring Your Own Device 44

Mobile Security Tasks

- Detection & remediation of mobile malware
- Detection & remediation of compromised operating systems
- Detection & remediation of sideloaded apps
- Detection & remediation of network-based “man-in-the-middle” attacks
- Detection & remediation of non-compliant/“risky” apps
- Ease and depth of integration with your Enterprise Mobility Management (EMM) and Mobile Device Management (MDM) platforms

Risk Mitigation - Security

Secure data transmission

Update the smartphone OS whenever any application patches or OS upgrades are released

Require the use of a pass code to lock the device in order to avoid data leakage if the device were to be used by a stranger

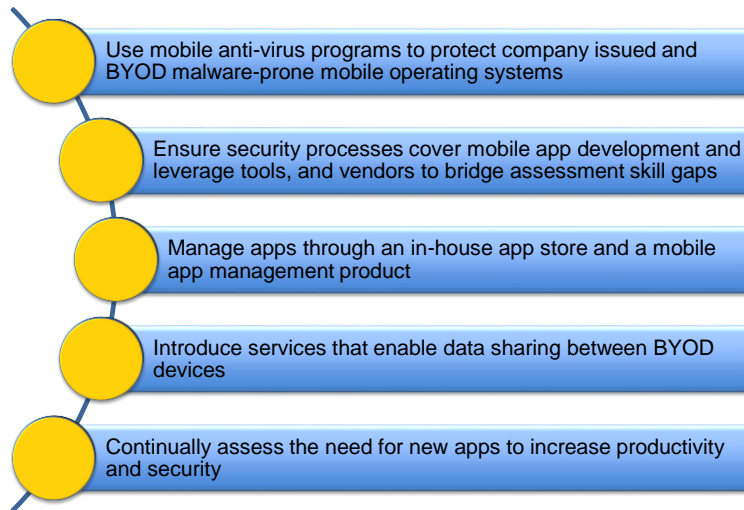
Do not “jailbreak” root or modify the OS files

Install antivirus and firewall software to detect and stop any infection and intrusion

Install device-tracking applications to find the phone if it is lost or stolen

Regularly back up or synchronize the settings and other personal information in order to avoid the loss of data due to theft

Risk Mitigation - Applications



Risk Mitigation - Regulatory

Involve Legal and HR in the countries where BYOD will be used to understand local privacy and data security laws

Create a policy structure that is a streamlined governance workflow and ensuring the policy approval process is faster and more agile

Create policies for each geographical area that expand on the general BYOD policy

Ensure your policy addresses the risk areas

Review, monitor and revise policies regularly

Ensure IT has the right processes in place to support the policy

Other Mitigating Controls

	Corporate counsel involvement in recruitment processes
Unified policy, awareness, regulation and compliance	
	Device protection and future consideration
Training and policy management	

BYOD: Bring Your Own Device
49

BYOD Privacy

Logical access to the device	Working extra without compensation	Personal data moving into cloud or part of corporate big data
Pictures, videos, other media	Phone records or contacts	GPS settings
Personal financial data	Personal emails	Web browsing history

BYOD: Bring Your Own Device
50

Privacy Laws

US-EU Safe Harbor Framework

Children Online Privacy Protection Act (COPPA)

Section 5 of FTC Act for Consumer Protection

Gramm-Leach-Bliley Act (GLBA)

Fair Credit Reporting Act (FCRA)

Identity theft under the Fair and Accurate Credit Transactions Act (FACTA)

Telephone Consumer Protection Act (TCPA)

Health Information Portability and Accountability Act (HIPAA), USA

EU Directive, European Union

Personal Information Protection and Electronic Documents Act (PIPEDA), Canada

Organization for Economic Co-operation and Development (OECD) Guidelines

The Privacy Act 1988, Australia

Mobile Security is Critical

Safeguards sensitive company data that even security - minded employees may put at risk. Not because they are careless or irresponsible but because they are human and doing important, time-sensitive work. They should not have to think about security.

Mobile Security Tasks

Detection & remediation of:

- mobile malware
- compromised operating systems
- side loaded apps
- network-based “man-in-the-middle” attacks
- non-compliant/“risky” apps

Ease and depth of integration with:

- Enterprise Mobility Management (EMM)
- Mobile Device Management (MDM) platforms

Employees' Concerns



What can my employer see on my phone and what can they NOT see?



Can See

- Carrier
- Country
- Make & Model
- OS version
- Phone number
- List of apps
- Corporate e-mail and data

Cannot See

- Personal email and data
- Texts
- Photos
- Videos
- Voicemail
- Web Activity

MDM

- **Mobile device management (MDM)** is the administrative area dealing with deploying, securing, monitoring, integrating and managing mobile devices, such as **smartphones, tablets** and laptops, in the workplace. The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise, while simultaneously protecting the corporate network.

The ideal mobile device management tool:

Is compatible with all common handheld device operating platforms and applications

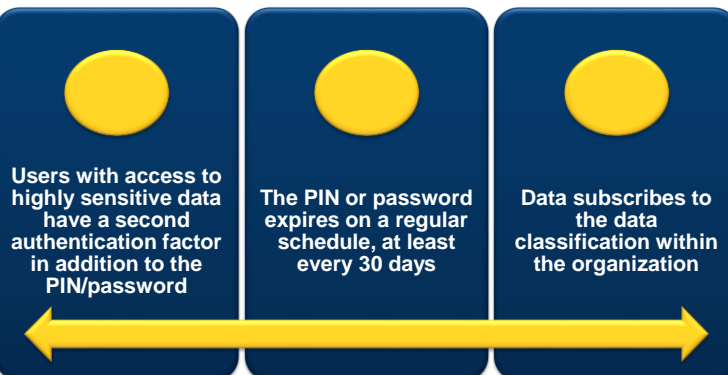
Can function through multiple service providers

Can be implemented directly over the air, targeting specific devices as necessary

Can deploy next-generation hardware, operating platforms and applications quickly

Can add or remove devices from the system as necessary to ensure optimum network efficiency and security

Device Access Restrictions



Device Access Restrictions

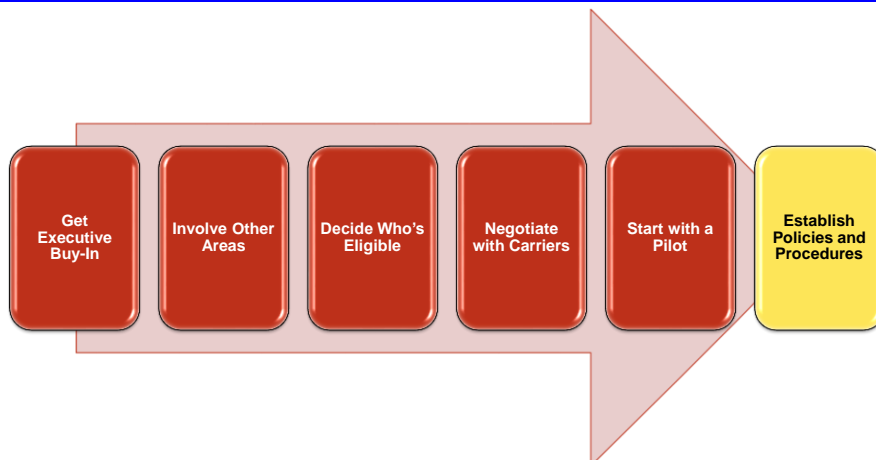
The device:

- locks automatically after five minutes of inactivity
- locks after three unsuccessful PIN/password attempts
- pauses for an incremental time before the next attempt

BYOD users agree in writing:

- to report loss of their device(s) without delay
- that enterprise data and apps on the device may be remotely wiped if the device is lost or stolen, or on termination of employment
- that the enterprise data and apps on the device may be remotely wiped after a specific number of unsuccessful login attempts

Governance for BYOD



Roll Out the Program

Select the pilot

- Sample group of users to complete the device registration and configuration process
- Distribute the BYOD mobile device policy or end-user agreement at this stage to ensure users understand the terms of the program
- Include a large percentage of business and non-technical users to get a better understanding of the average BYOD user experience
- IT operations staff participate to ensure any technical issues are discovered during the pilot phase








Survey employees to continually improve the user experience

- Survey users during every phase of the BYOD implementation to make sure the program is meeting employee needs and expectations
- Registration survey captures the user's first experience with the BYOD program, and can identify any gaps in the device registration process
- Follow-up or closing survey provides both specific and open-ended questions to gather feedback about the overall user experience during the pilot test

BYOD Policy

- General security requirements for mobile devices
- Authentication (passcode/PIN) requirements
- Storage/transmission encryption requirements
- Requirements to automatically wipe devices after a number of failed login attempts
- Usage restrictions for mobile devices
- Company liability

BYOD Policy

	Rights to monitor, manage and wipe
	Support model
	Leading practices for mobile data usage on international travel
	Acceptable use (if different from the normal acceptable use policy)
	Secure devices and apps
	Breach investigation and notification
	Data ownership and recovery

Security Awareness Training

Leverage existing security awareness program	Clearly articulate the security risks associated with smartphones
	Make sure employees understand acceptable use policies
	Limit employee's abilities to install applications
	Provide appropriate training where necessary
	Encourage healthy skepticism

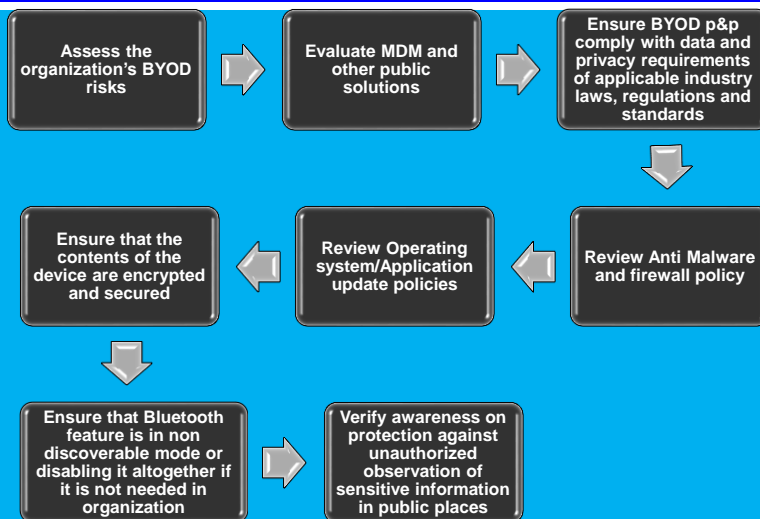
Topics to Discuss

- Avoid browsing unencrypted websites
- Phone software updates
- Securing home Wi-Fi
- Avoid "always on" Wi-Fi

- Awareness of data
- Personal data
- Company data
- Social engineering

- Health data
- Communication data
- Physical security
- Reporting theft/misuse

Audit's Role



Key Controls

Risk Management

- BYOD is subject to routine risk assessment processes.
- Risk assessment was performed prior to acceptance of the program
- Subsequent risk assessments are performed after the initial one for new uses or devices

Policies

- Policies defined, documented, approved, implemented and maintained
- Exemptions from BYOD policies are appropriately controlled and monitored
- Employees must sign the BYOD agreement before device activated on company network

BYOD: Bring Your Own Device
65

Key Controls

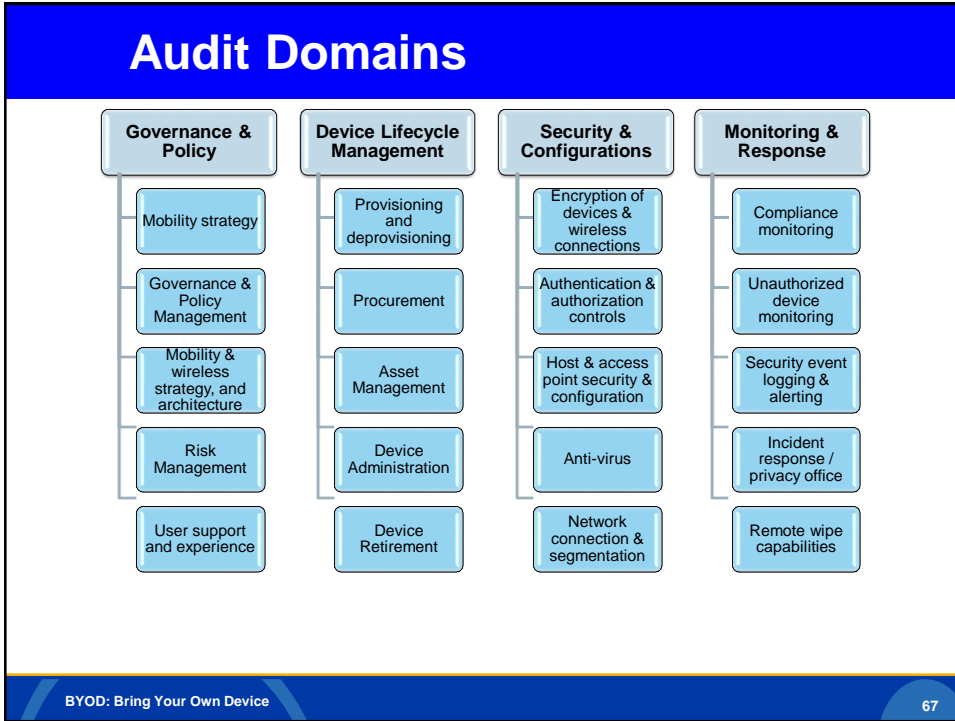
Mobile Device Management

- An industry standard has been implemented
- The MDM provides adequate querying and reporting capabilities to manage the BYOD population proactively
- MDM has critical security features: remote lock and wipe, permission based access, over the air distribution of apps,
- Enterprise app store is private to BYOD devices

Security / Governance

- BYOD is subject to oversight and monitoring by management
- Data access is aligned with organization data classification requirements and employee job function
- BYOD users are required to maintain basic security procedures for the device
- Approvals for new applications being rolled out
- Strong encryption is deployed

BYOD: Bring Your Own Device
66



Pilot Test

	Tester	
	Device	
	OS	
	Version	
	Carrier	
	Date Tested	
	Environment	DEV
	TEST	
User	Compose email	
User	Send email	
User	Receive Email	
User	Open attachment	
User	Setup meeting invite	
User	Receive invitation	
User	Add contacts	
User	View directory	
User	OOO setup	
User	Access secure browser	
User	Test Device wipe – was personal data intact	
User	Setup a policy in Good to test policy e.g. sending of attachment	
User	Test password enforcement & remote lock/unlock	
	Call help desk – device lost – did they report to Privacy	
	How long did the wipe take	
User	Comments/Issues	

BYOD: Bring Your Own Device
68

Pilot Test

		Tester
		Carrier
		Date Tested
		Environment
	TEST	DEV
Admin	Perform a software update	
Admin	Push out app from Good NOC	
Admin	Test wiping data in Good Container	
Admin	Test Good Monitoring Portal. Ensure it provides real-time visibility from our NOC to the device	
Admin	Check Integration into LDAP	
Admin	Test user provisioning	
Admin	Check EULA presented to end user on provisioning	
Admin	Test over the air provisioning	
Admin	Test Good data cannot be saved to removable storage	
Admin	Test backup and restore of Good Server	
Admin	Test/Detect Jail Broken devices	
Admin	Check voicemail	
Admin	Test Container wipe	
Admin	Provision user account in Good	
Admin	View an attachment	
Admin	Inventory applications	
Admin	Test Jailbreak detection, password limit and auto device wipe.	
Admin	Test email synchronization	

Control Group	Control Number	Control Description	Inquiry and Examination
Access Request and Setup	ARS.1	All access granted to GOOD application should be accompanied with a formal submitted request, a valid business reason, user acceptance of the end user license agreement, and proper management approval.	<p><u>Inquiry & Observation</u></p> <ol style="list-style-type: none"> Perform a walkthrough and confirm that the control activity is operating as documented. If not, modify as necessary to show the current state of processing. Inquire and document the requirements for BYOD access procurement. This should include the business need and required approvals necessary for access procurement. <p><u>Examination</u></p> <ol style="list-style-type: none"> Obtain a listing of current BYOD users for the period from 6/24/2013 through 7/24/2013. From the listing obtained, select a sample in accordance with sampling guidance (the lesser of 10% of the population or 25, with a minimum of 5 samples). <p><i>Note: Where feasible a full population will be tested.</i></p> <ol style="list-style-type: none"> For each sample perform the following test steps: <ol style="list-style-type: none"> Confirm that a formal request including business need has been submitted in CA service desk. Confirm that the appropriate approvals have been obtained; User, Manager, Cost Center Manager, and SVP (non-exempt) Confirm that each user has accepted the end user license agreement (EULA). Document any exceptions.


Control Group	Control Number	Control Description	Inquiry and Examination
Access Request and Setup	ARS.2	Ensure that management reviews or reallocates user access rights at regular intervals using a formal process. User access rights should be reviewed or reallocated after any job changes, such as transfer, promotion, demotion or termination of employment. Authorizations for special privileged access rights should be reviewed independently at more frequent intervals.	<u>Inquiry & Observation</u> <ol style="list-style-type: none"> 1. Perform a walkthrough and confirm that the control activity is operating as documented. If not, modify as necessary to show the current state of processing. 2. Inquire and document the requirements for BYOD access modifications. 3. Inquire and document the recertification process for BYOD users.
Device Usage	DU.1	Training and awareness programs are developed and distributed, or are readily available, to all users who have been granted access to GOOD application.	<u>Inquiry & Observation</u> <ol style="list-style-type: none"> 1. Perform a walkthrough and confirm that the control activity is operating as documented. If not, modify as necessary to show the current state of processing. 2. Inquire and document all training and awareness programs regarding BYOD. 3. Inquire and document processes for reviewing and updating BYOD training and awareness programs on a periodic basis.

More at the end

BYOD: Bring Your Own Device 71

<h2>Conclusion</h2>	
■	Request & Authorization Process
■	Mobile Device Management (MDM) Solution
■	Monitoring
■	Asset Management (inventory)
■	Security Awareness & Training
■	Patch Management
■	User Agreement
■	Incident Response
■	Help Desk Procedures

BYOD: Bring Your Own Device 72



John A. Gatto
312 402 4731
johnagatto@comcast.net

BYOD: Bring Your Own Device

Control Group	Control Number	Control Description	Inquiry and Examination
Device Usage	DU.2	All GOOD profiles require devices to conform to policies and standards regarding access controls (screen lock, password settings, time out settings, etc...).	<p><u>Inquiry & Observation</u></p> <ol style="list-style-type: none"> 1. Perform a walkthrough and confirm that the control activity is operating as documented. If not, modify as necessary to show the current state of processing. 2. Inquire and document all GOOD profiles and their accompanied settings. <p><u>Examination</u></p> <ol style="list-style-type: none"> 1. Obtain a device with each available GOOD profile, or have each profile individually tested by being pushed separately. 2. For each sample perform the following test steps: <ol style="list-style-type: none"> a) Confirm that profile enforces access controls that are in-line profile definitions. b) Confirm that controls align with industry best practices: <ul style="list-style-type: none"> • Lock Settings • Password Settings • Time-out Settings 3. Document any exceptions.

BYOD: Bring Your Own Device 74

Control Group	Control Number	Control Description	Inquiry and Examination
Device Usage	DU.3	<p>GOOD application and server activity will be logged at a device/user level. This includes, but is not limited to:</p> <ul style="list-style-type: none"> • Amount of data the device is requesting from the server • Downloading (files) from the server • Usage statistics 	<p><u>Inquiry & Observation</u></p> <ol style="list-style-type: none"> 1. Perform a walkthrough and confirm that the control activity is operating as documented. If not, modify as necessary to show the current state of processing. 2. Inquire and document the requirements for logging and reporting as well as the processes for reviewing logs and reports. 3. Inquire and document what activities will trigger alarms regarding GOOD usage or security. <p><u>Examination</u></p> <ol style="list-style-type: none"> 1. Obtain a listing of users with access for the period from 6/24/2013 through 7/24/2013. 2. AS will judgmentally select one user from the listing. 3. For the user selected perform the following test steps: <ol style="list-style-type: none"> a) Ensure that all required metrics are being recorded for the device/user. 4. Document any exceptions.

BYOD: Bring Your Own Device 75

Control Group	Control Number	Control Description	Inquiry and Examination
Termination of BYOD Usage	T.1	<p>Upon termination (voluntary or involuntary) access to GOOD application will be requested and removed in a timely manner in accordance with corporate policies.</p>	<p><u>Inquiry & Observation</u></p> <ol style="list-style-type: none"> 1. Perform a walkthrough and confirm that the control activity is operating as documented. If not, modify as necessary to show the current state of processing. 2. Inquire and document the policies and processes for termination of GOOD usage (voluntary or involuntary), specifically, AS will inquire and document the termination process for the following scenarios: <ol style="list-style-type: none"> a) FMLA b) Voluntary end of usage c) Involuntary end of usage d) Lost/Stolen device end of usage <p><u>Examination</u></p> <ol style="list-style-type: none"> 1. If possible, AS will execute each of the following scenarios: <ol style="list-style-type: none"> a) FMLA b) Voluntary end of usage c) Involuntary end of usage d) Lost/Stolen device end of usage 2. For each scenario executed, perform the following test steps: <ol style="list-style-type: none"> a) Ensure that all termination requests were formally documented and approved. b) Ensure that access was removed and device can no longer access GOOD servers. c) If a device or Good wipe is necessary, ensure that the wipe was completed successfully. 3. Document any exceptions.

BYOD: Bring Your Own Device 76

<u>Control Group</u>	<u>Control Number</u>	<u>Control Description</u>	<u>Inquiry and Examination</u>
Termination of BYOD Usage	T.2	In the event of a lost, stolen, or misplaced device the GOOD application will be remotely wiped to ensure that unauthorized access is avoided.	<p><u>Inquiry & Observation</u></p> <ol style="list-style-type: none"> 1. Perform a walkthrough and confirm that the control activity is operating as documented. If not, modify as necessary to show the current state of processing. 2. Inquire and document the policies and processes for remotely wiping devices. 3. Inquire and document the different types of remote wiping methods that can be utilized and how the BYOD team validates that the wipe occurred.
Application Security	AS.1	GOOD application conforms to industry standard of encryption requirements and techniques.	<p><u>Inquiry & Observation</u></p> <ol style="list-style-type: none"> 1. Perform a walkthrough and confirm that the control activity is operating as documented. If not, modify as necessary to show the current state of processing. 2. Inquire and document encryption policies and standards utilized by GOOD.

BYOD: Bring Your Own Device 77

<u>Control Group</u>	<u>Control Number</u>	<u>Control Description</u>	<u>Inquiry and Examination</u>
Application Security	AS.2	GOOD application and devices will only use secure channels to connect devices to associated technologies.	<p><u>Inquiry & Observation</u></p> <ol style="list-style-type: none"> 1. Perform a walkthrough and confirm that the control activity is operating as documented. If not, modify as necessary to show the current state of processing. 2. Inquire and document the connection process utilized by GOOD application to HCSC servers.
Application Security	AS.3	GOOD application and profile updates are provided in accordance to policy requirements.	<p><u>Inquiry & Observation</u></p> <ol style="list-style-type: none"> 1. Perform a walkthrough and confirm that the control activity is operating as documented. If not, modify as necessary to show the current state of processing. 2. Inquire and document the process of application and profile updates.
Application Security	AS.4	GOOD application will log and report all activities and events (unsuccessful login attempts, last login, etc....) that are outlined in the corporate policy.	<p><u>Inquiry & Observation</u></p> <ol style="list-style-type: none"> 1. Perform a walkthrough and confirm that the control activity is operating as documented. If not, modify as necessary to show the current state of processing. 2. Inquire and document all activities that are being logged and reported on and ensure that devices are recording data appropriately.

BYOD: Bring Your Own Device 78