BYOD: Audit and Security Concerns

John A. Gatto, CISA, CRISC
JAG Associates

Definition

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

Bring your own device

From Wikipedia, the free encyclopedia

- Bring your own device (BYOD) refers to the policy of permitting employees to bring their owned mobile devices (laptops, tablets, and smartphones) to their workplace, and to use those privileged company information. Also used to describe the rights using personally owned

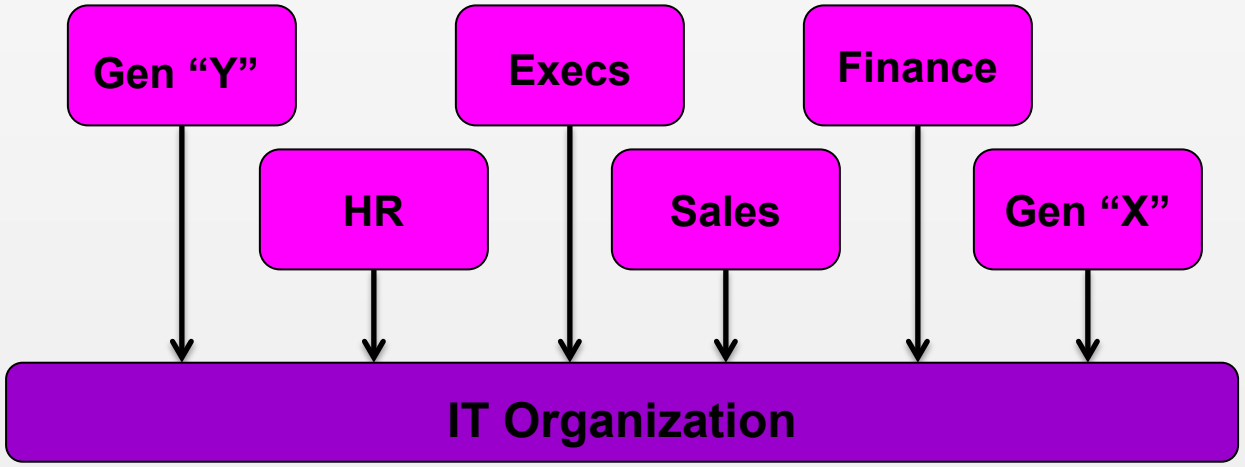
- BYOD is now common in the business world. **In most cases, BYOD is a trend.** Some believe that it allows employees be more productive, due to higher morale and convenience by using their own devices and **makes the company look like a flexible and attractive employer, and attract new hires.**

BYOD = Bring Your Own Disaster?

BYOD Drivers

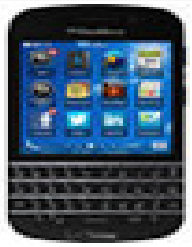
Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

Main corporate drivers are primarily financial, employee engagement and employee productivity



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

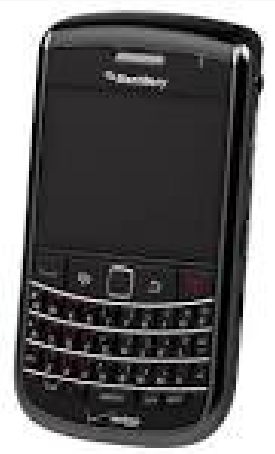
The Trouble Makers



Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

Too Many Devices

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL



What Can Happen

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

- 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

Shades of BYOD

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

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

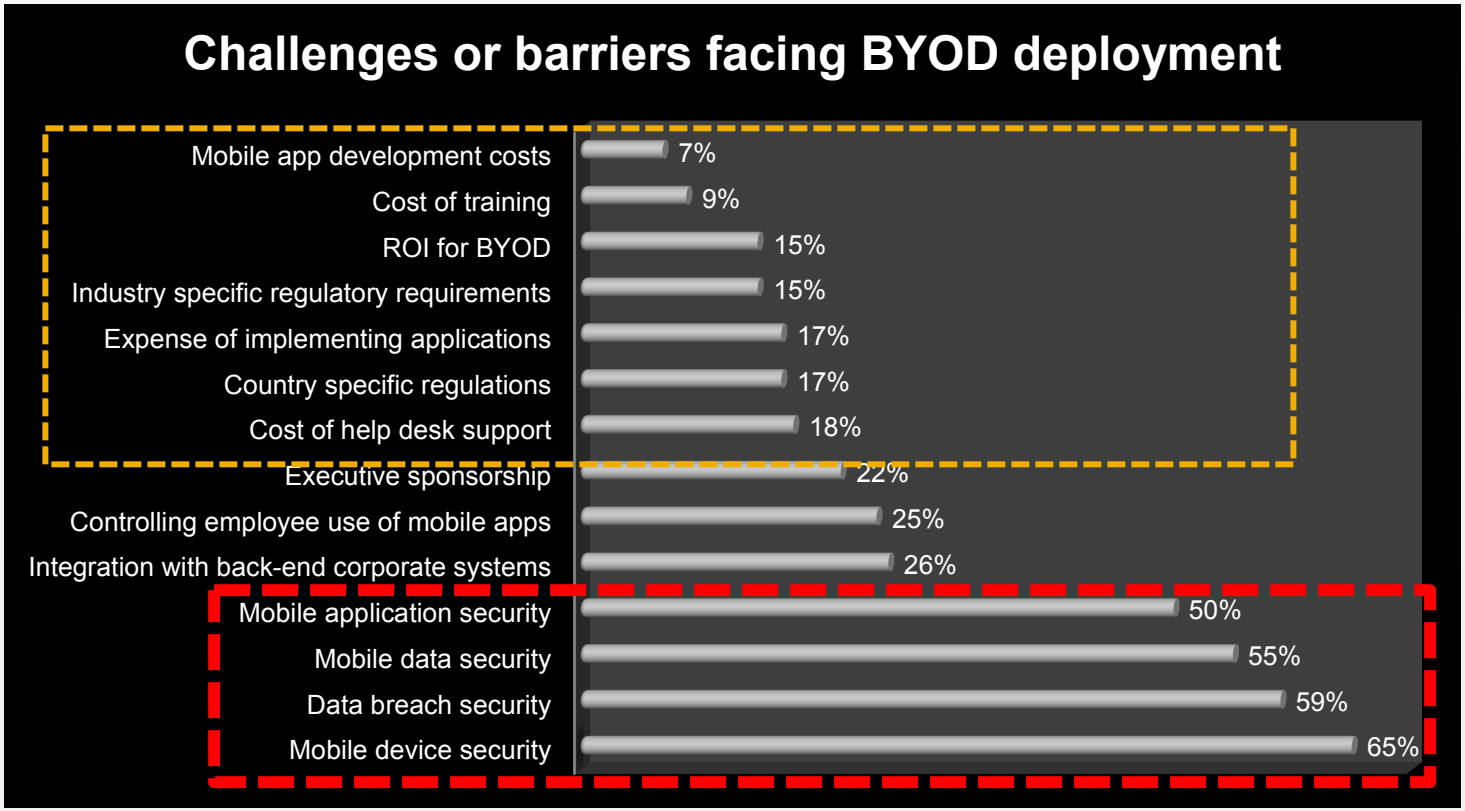
Implementing BYOD

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

- Analyze the risk of deploying BYOD
- Create a strategy for BYOD with a business case and a goal statement
- Involve stakeholders early through the formation of a mobility group
- Create a support and operations model
- Implement a pilot before mass deployment

Challenges

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL



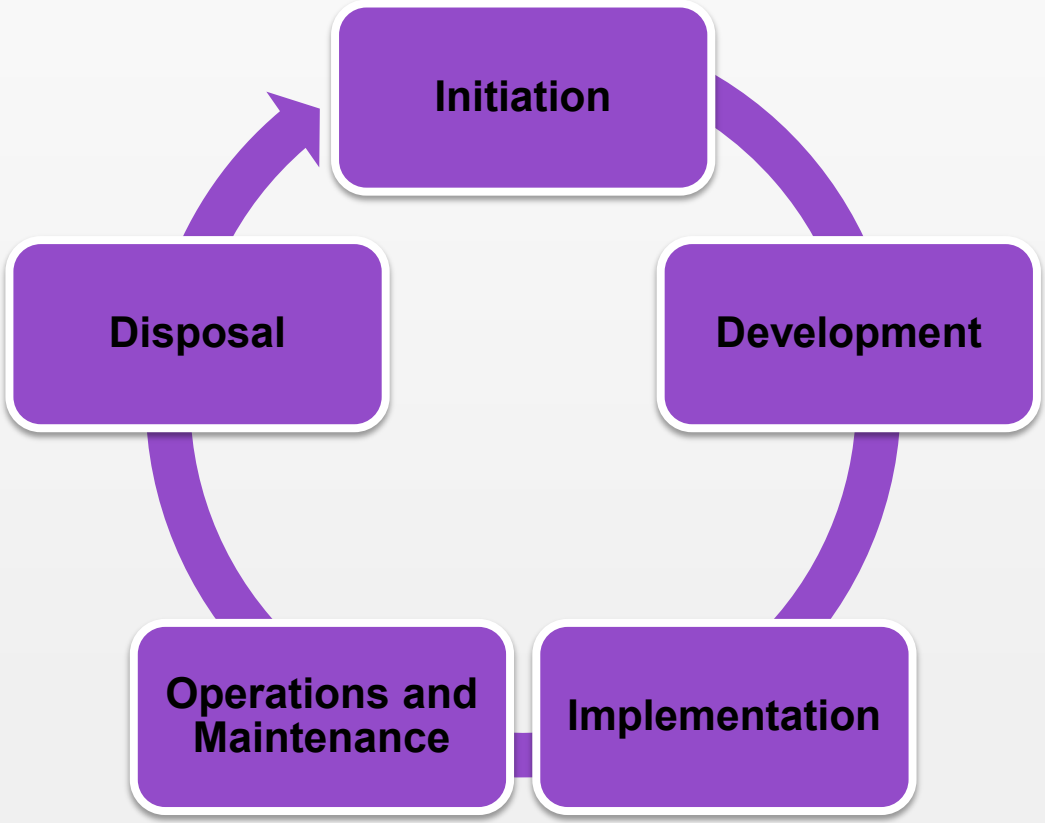
BYOD Statistics

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

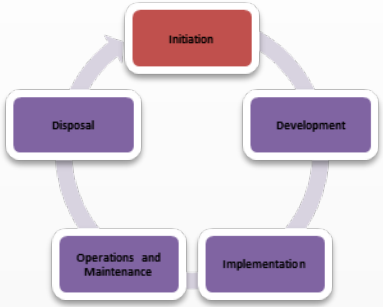
%	Explanation
67%	Of people use personal devices at work, regardless of the office's official BYOD policy (Source: Microsoft via CBS News)
77%	Of employees haven't received any education about the risks related to BYOD (Source: 2013 Data Protection Trends Research
11%	Of end users access business applications 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)

Deploying BYOD

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL



Initiation

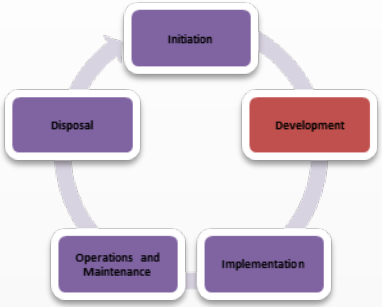


Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

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
- Specify business and functional requirements for the solution

Development



Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

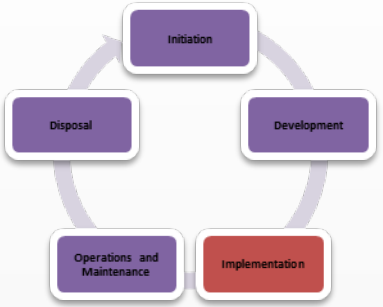
Specify the technical characteristics:

- 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

Implementation



Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

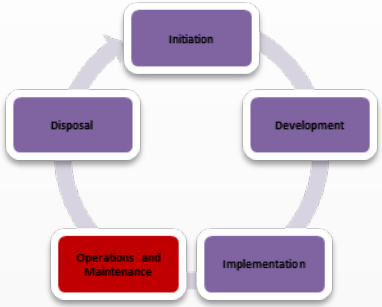
Equipment is configured to meet operational and security requirements

Mobile device security policy documented in the system security plan, installed and tested as a pilot

Mobile device security policy is activated on a production network

Integration with other security controls and technologies, such as security event logging and authentication servers

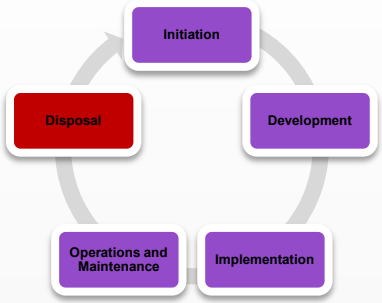
Operations And Maintenance



Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

Ongoing security-related tasks:

Disposal

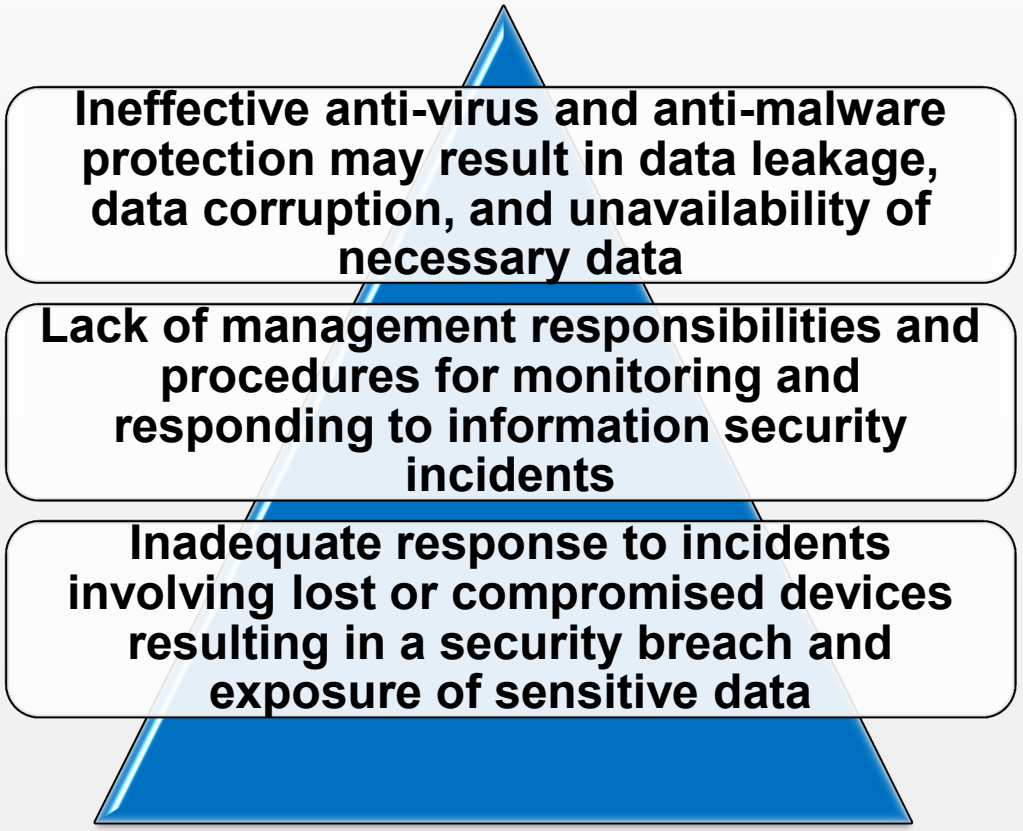


Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

Mobile device is retired:

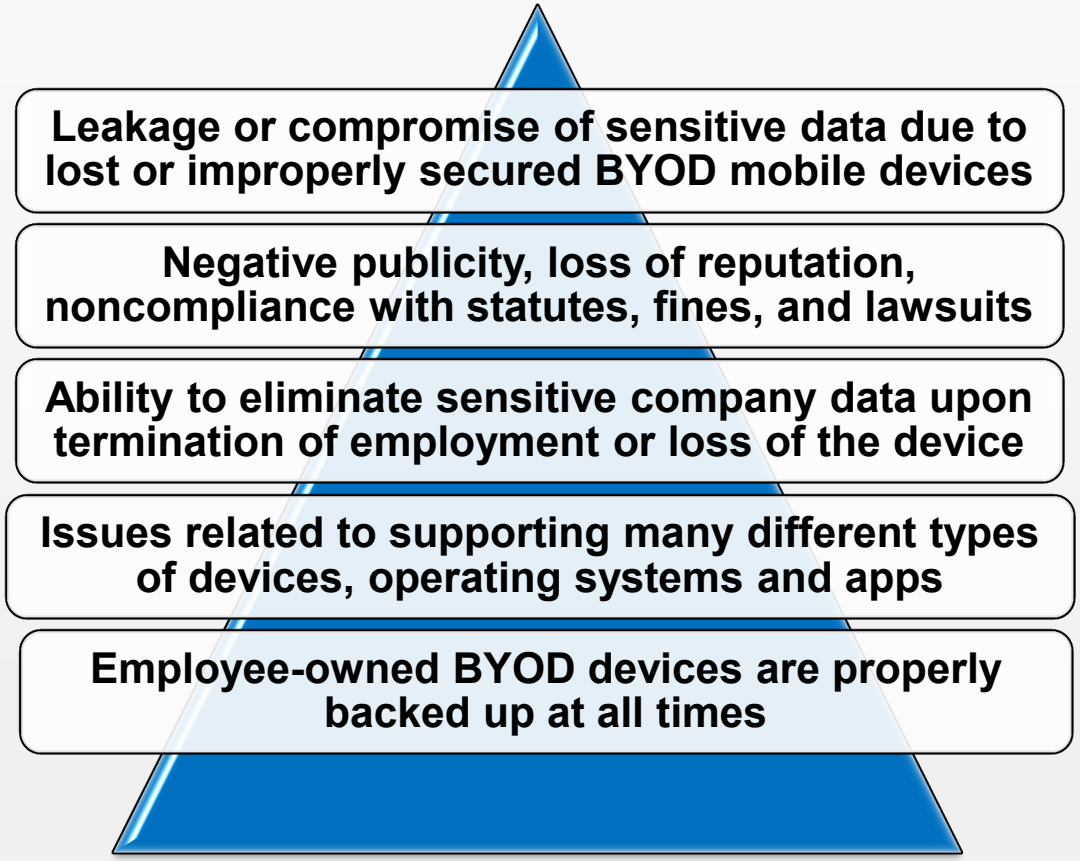
Risks

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL



Risks

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL



Benefits

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

Improved business and employee collaboration

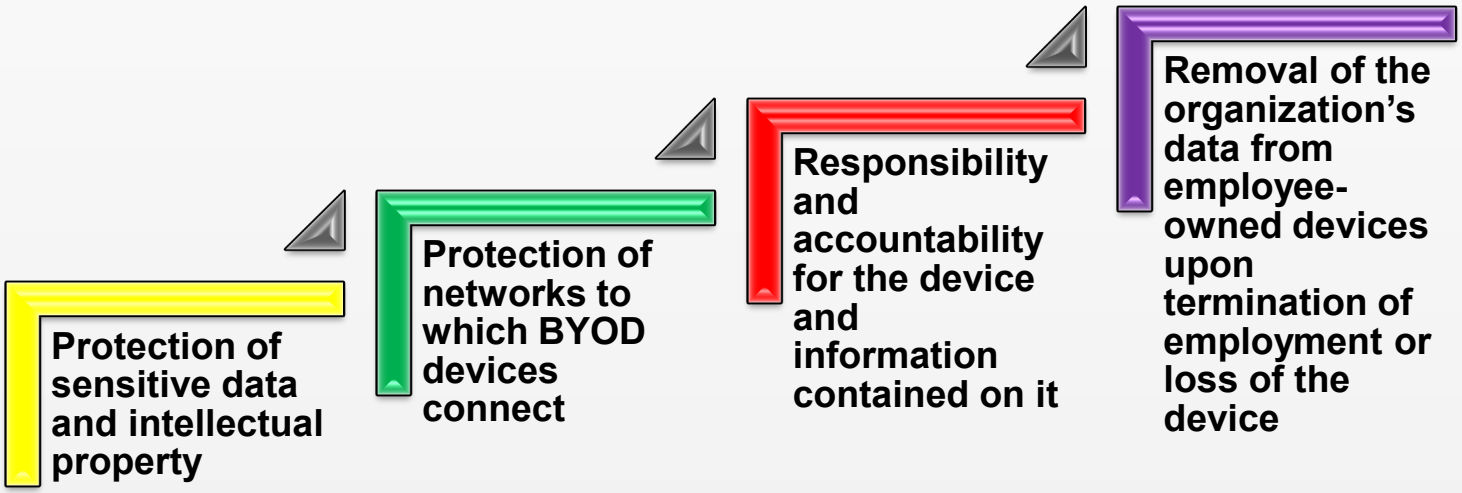
Increased productivity

Attract / keep employees

Decreased worker latency

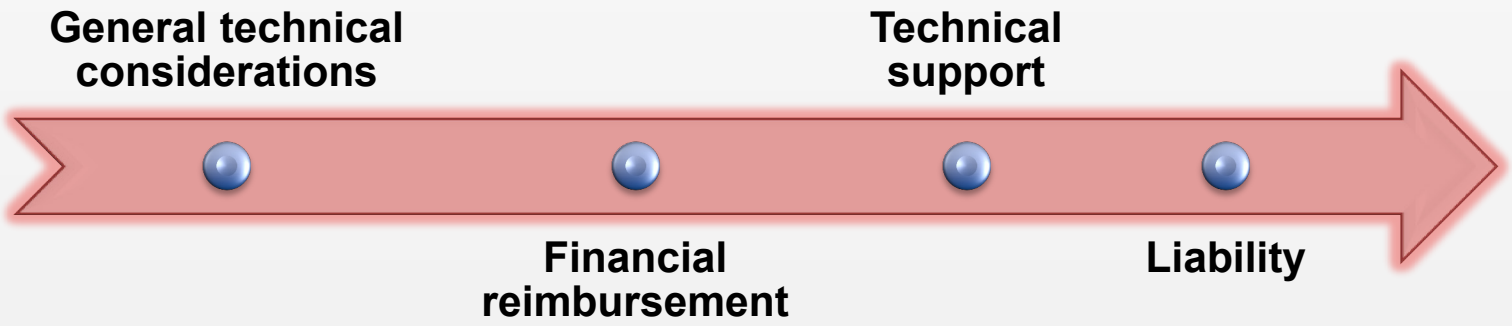
Primary Security and Control Issues

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL



BYOD Program and Policy

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL



General technical considerations | Financial reimbursement | Technical support | Liability

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

What

- Devices / mobile operating systems can we support?
- Are our 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?

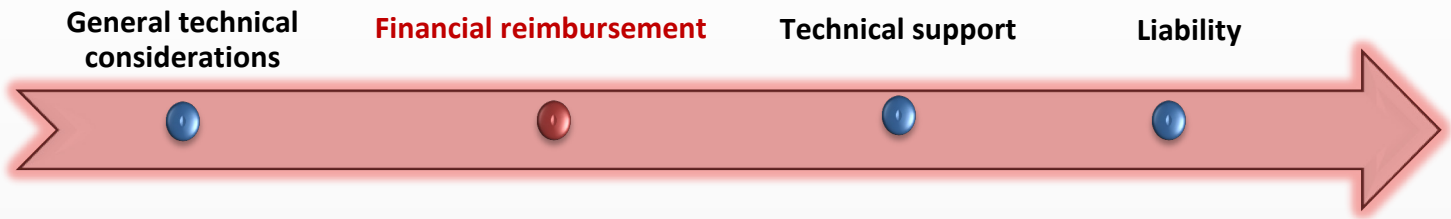
How

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

Things to Consider (TTC) – General Technical

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

- Knowledge, tools, and apps across various platforms (iOS, Windows Mobile, and Android)
- Distribution of applications to and manage applications on employee devices
- Development of secure applications for mobile devices
- Deployment of applications: e-mail, calendar, time and expense management, corporate directories
- Intranet access to BYOD users
- Types of users obtaining BYOD devices
- Levels of access to services and applications will be afforded to each group of users



- 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

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

TTC – Financial Reimbursement

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

- 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

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

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?

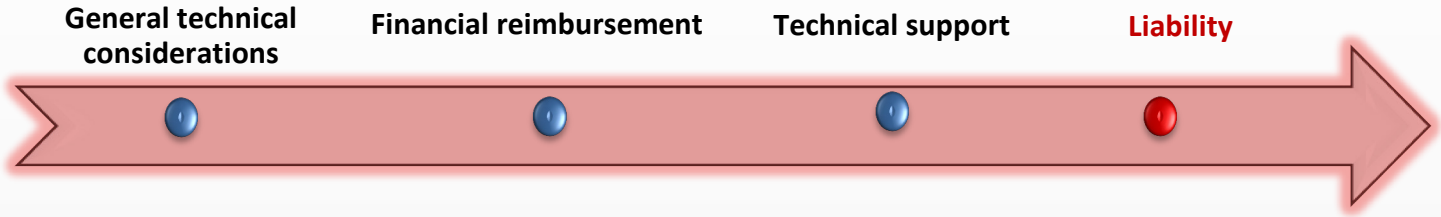
Support all devices? Only corporate data or apps?
Custom apps on personally owned devices?

TTC – Technical Support

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

- 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



Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

- 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?
- Policy regarding use of devices by users other than the corporate end user?

Risk Mitigation - Security

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

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

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

- Use mobile anti-virus programs to protect company issued and BYOD malware-prone mobile operating systems
- Ensure security processes cover mobile app development and leverage tools, and vendors to bridge assessment skill gaps
- Manage apps through an in-house app store and a mobile app management product
- Introduce services that enable data sharing between BYOD devices
- Continually assess the need for new apps to increase productivity and security

Risk Mitigation - Regulatory

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

- 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

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

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

BYOD Privacy

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

- 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

MDM

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

- 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.

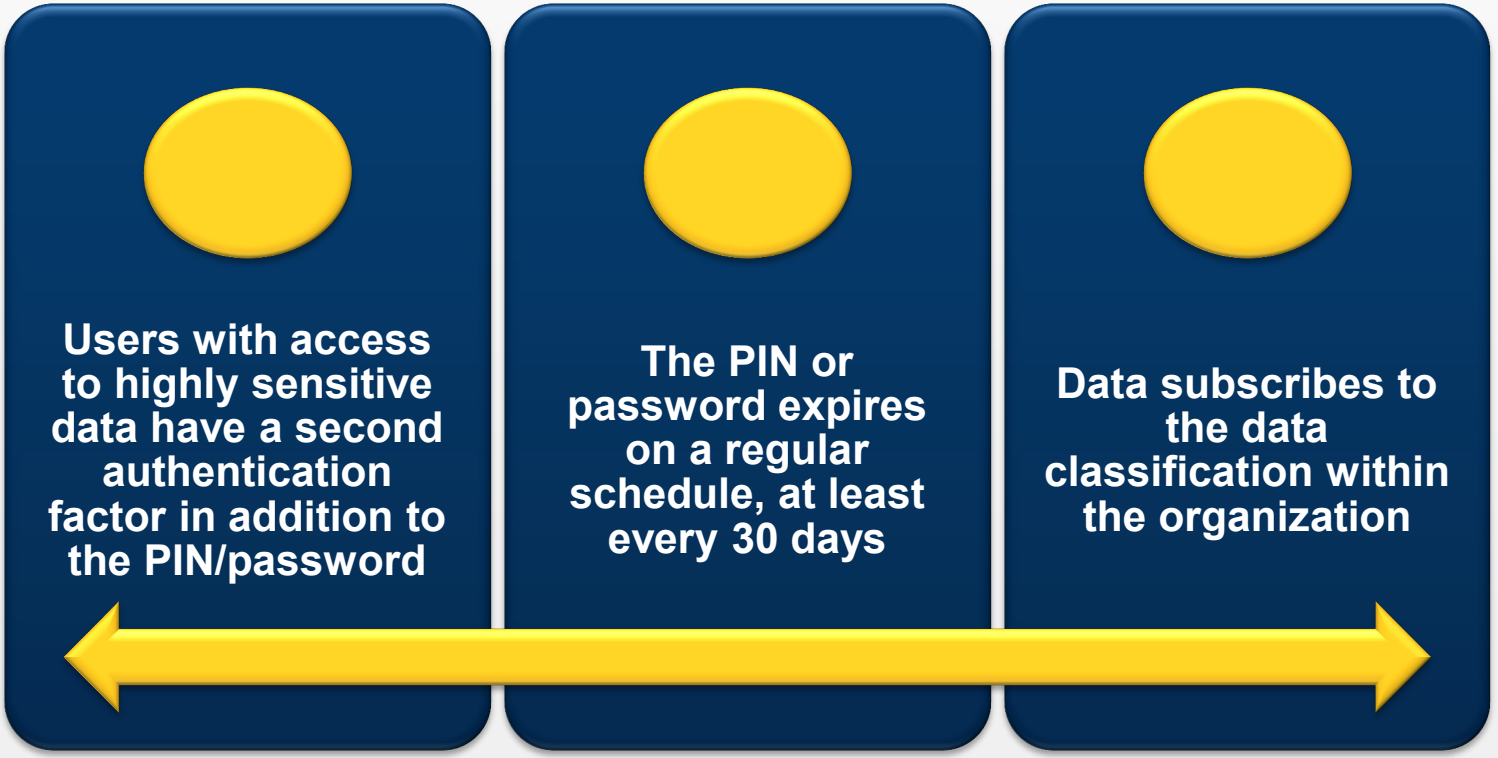
Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

My Data

Company Data

Device Access Restrictions

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL



Device Access Restrictions

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

The device:

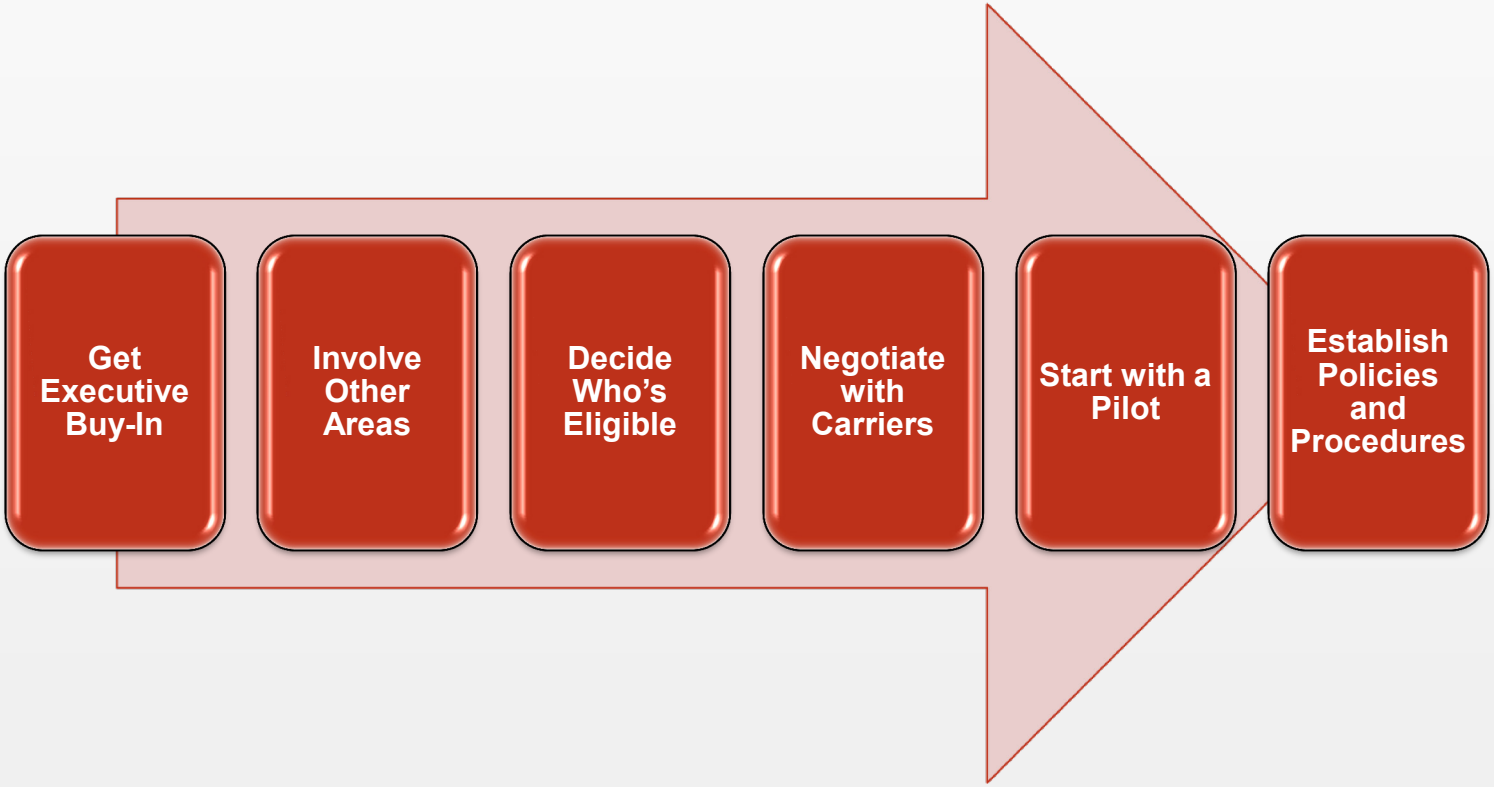
- locks automatically after five minutes of inactivity
- locks after three unsuccessful PIN/password attempts
- pauses for an incremental time before the next attempt

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 Programs

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL



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

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

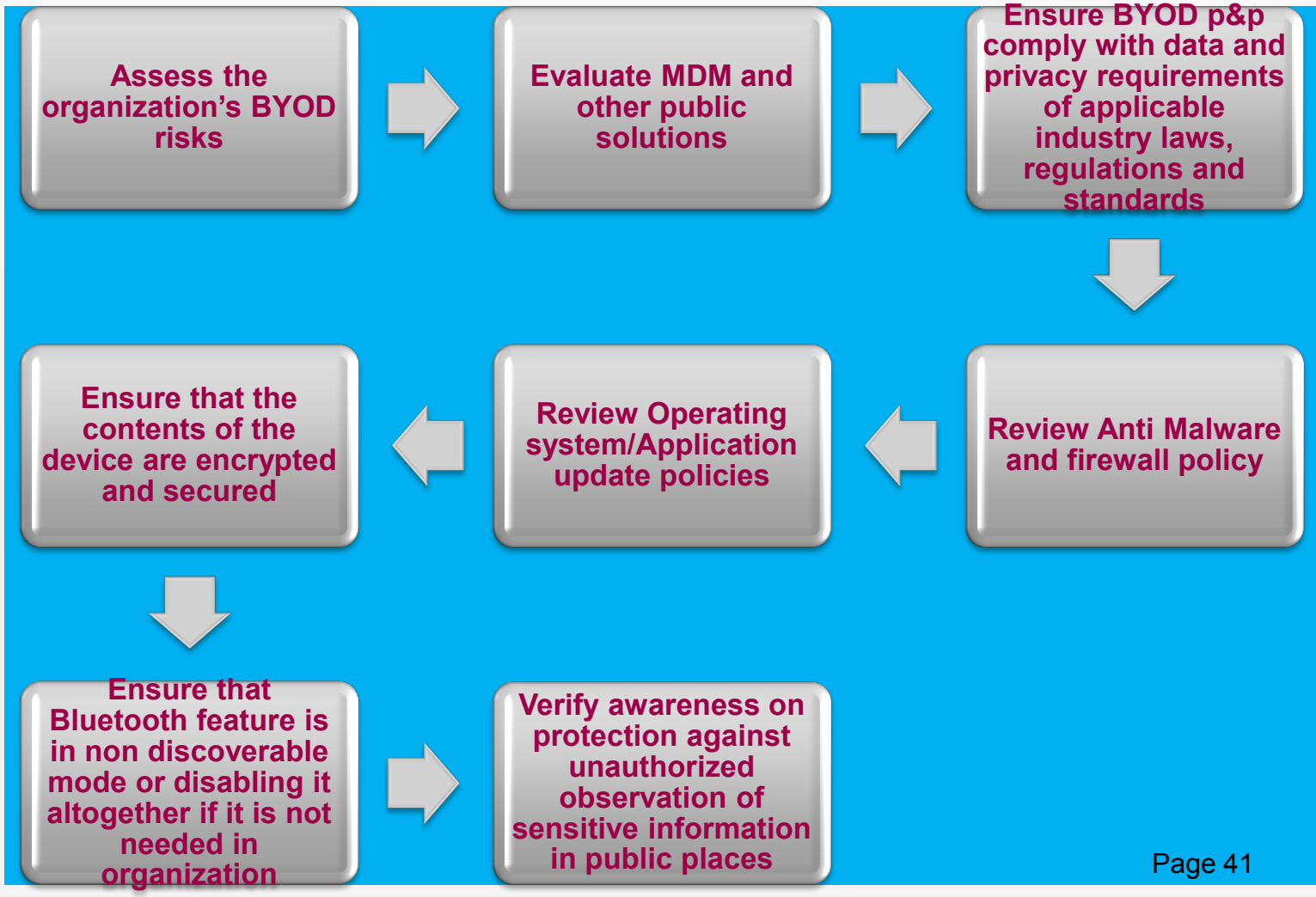
BYOD Policy

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

- 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

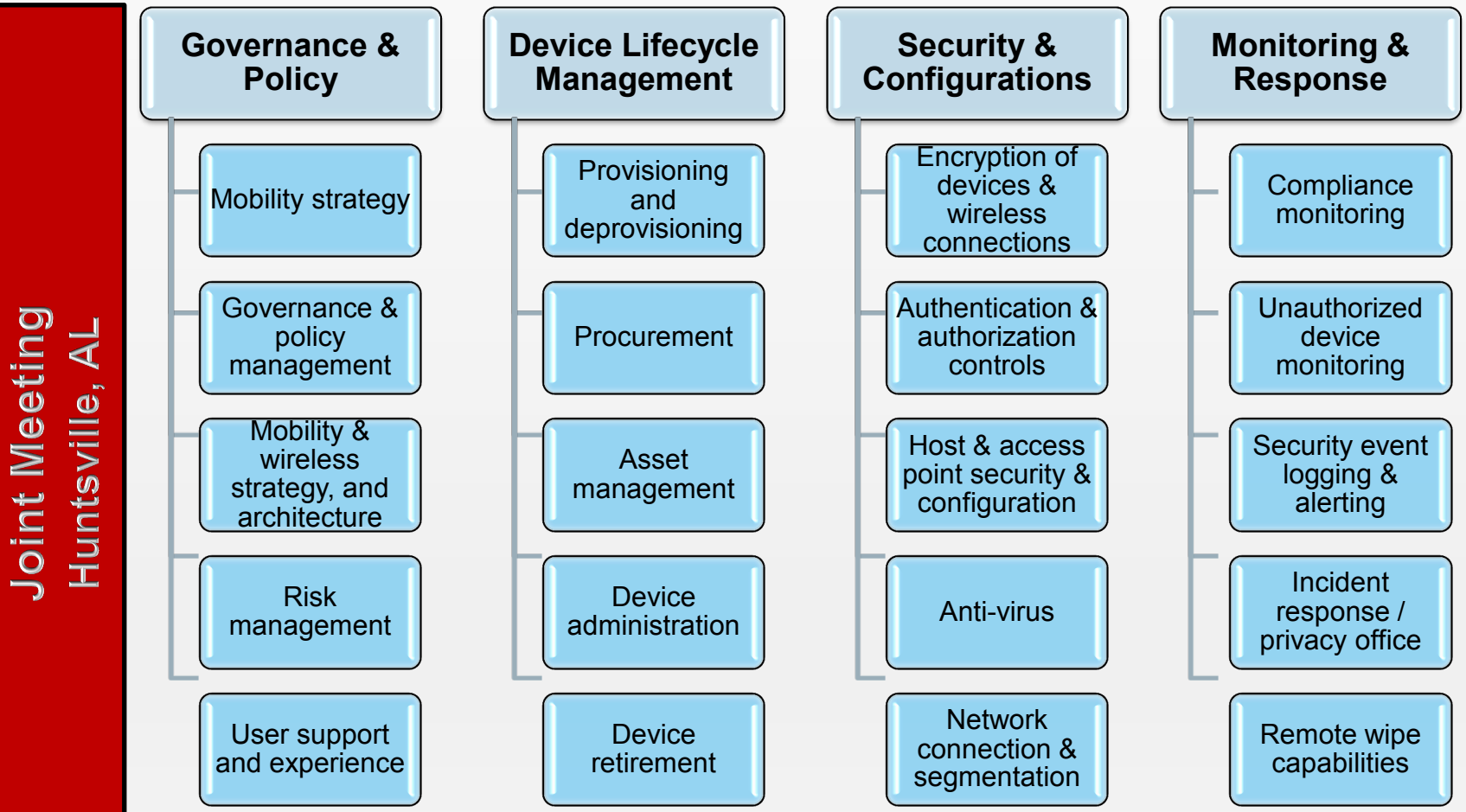
Audit's Role

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL



Audit Domains

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL



Pilot Test

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

	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	

Pilot Test

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

	Tester	
	Carrier	
	Date Tested	
	Environment	DEV
	TEST	
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.	**Inquiry & Observation** 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 procurement. This should include the business need and required approvals necessary for access procurement. **Examination** 1. Obtain a listing of current BYOD users for the period from 6/24/2013 through 7/24/2013. 2. 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). *Note: Where feasible a full population will be tested.* 1. For each sample perform the following test steps: a) Confirm that a formal request including business need has been submitted in CA service desk. b) Confirm that the appropriate approvals have been obtained; User, Manager, Cost Center Manager, and SVP (non-exempt) c) Confirm that each user has accepted the end user license agreement (EULA). 2. 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. Authorisations for special privileged access rights should be reviewed independently at more frequent intervals.	**Inquiry & Observation** 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.	**Inquiry & Observation** 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.

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…).	**Inquiry & Observation** 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. **Examination** 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: a) Confirm that profile enforces access controls that are in-line profile definitions. b) Confirm that controls align with industry best practices: • Lock Settings • Password Settings • Time-out Settings 3. Document any exceptions.

Control Group	Control Number	Control Description	Inquiry and Examination
Device Usage	DU.3	GOOD application and server activity will be logged at a device/user level. This includes, but is not limited to: • Amount of data the device is requesting from the server • Downloading (files) from the server • Usage statistics	**Inquiry & Observation** 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. **Examination** 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: a) Ensure that all required metrics are being recorded for the device/user. 4. Document any exceptions.

Control Group	Control Number	Control Description	Inquiry and Examination
Termination of BYOD Usage	T.1	Upon termination (voluntary or involuntary) access to GOOD application will be requested and removed in a timely manner in accordance with corporate policies.	**Inquiry & Observation** 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: a) FMLA b) Voluntary end of usage c) Involuntary end of usage d) Lost/Stolen device end of usage **Examination** 1. If possible, AS will execute each of the following scenarios: 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: 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.

Control Group	Control Number	Control Description	Inquiry and Examination
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.	**Inquiry & Observation** 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.	**Inquiry & Observation** 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.

Control Group	Control Number	Control Description	Inquiry and Examination
Application Security	AS.2	GOOD application and devices will only use secure channels to connect devices to associated technologies.	**Inquiry & Observation** 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.	**Inquiry & Observation** 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.	**Inquiry & Observation** 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 actives that are being logged and reported on and ensure that devices are recording data appropriately.

Conclusion

Southeastern and Southwest Intergovernmental Audit Forums
Joint Meeting
Huntsville, AL

- Request & Authorization Process
- Mobile Device Management (MDM) Solution
- Monitoring
- Asset Management (inventory)
- Security Awareness & Training
- Patch Management
- User Agreement
- Incident Response
- Help Desk Procedures

Southeastern and Southwest Intergovernmental Audit Forums

Joint Meeting

Huntsville, AL

Southeastern and Southwest Intergovernmental Audit Forums

Joint Meeting

Huntsville, AL

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