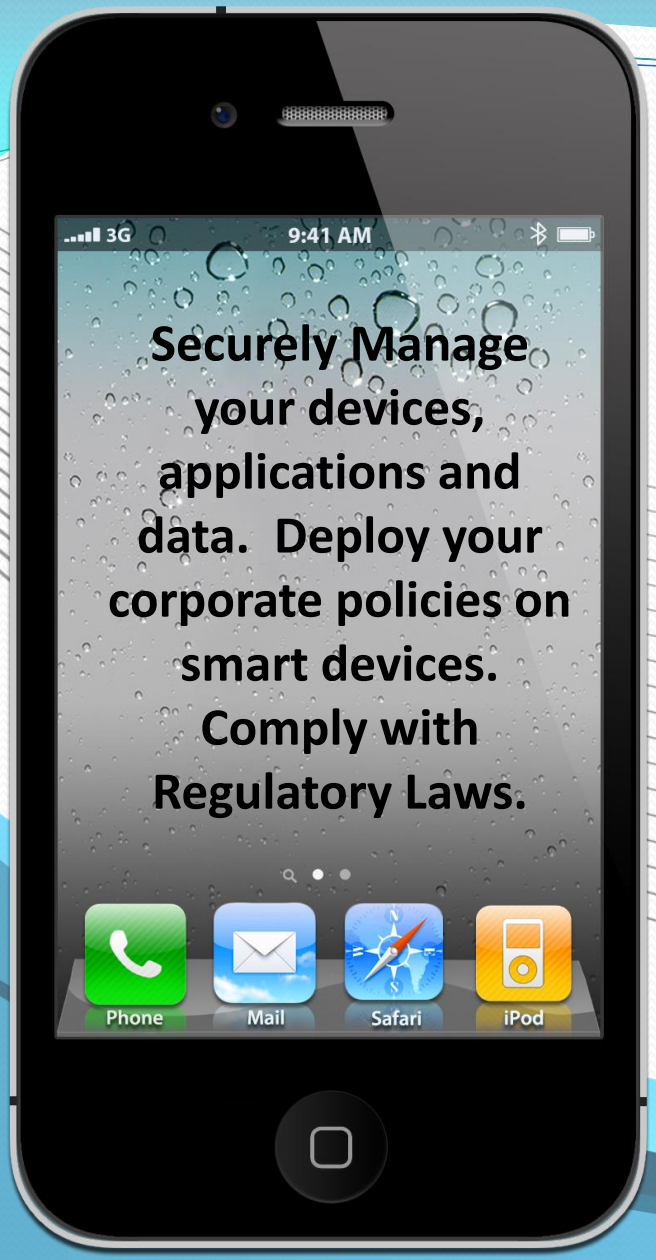


AUDITING SMART DEVICES

Auditing the Security and Management of Smart Devices

ISACA Meeting
February 20, 2013

Securely Mobile

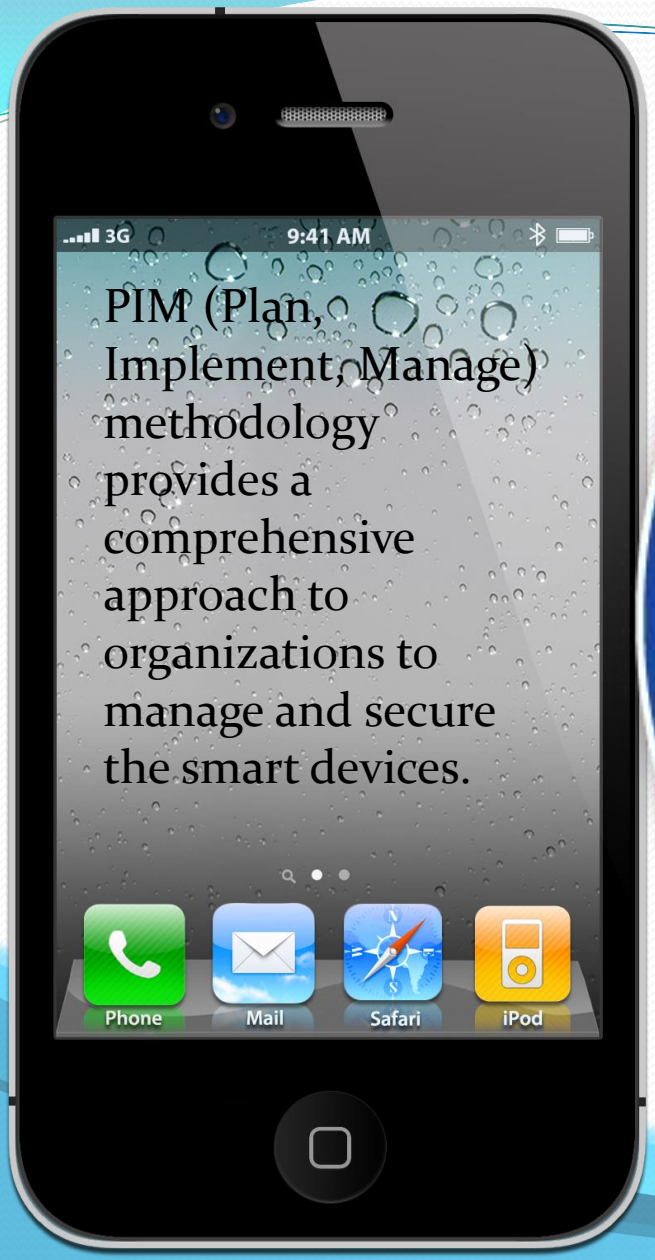
Agenda

- Evolution of Smart Device usage
- Audit Approach
- Q&A

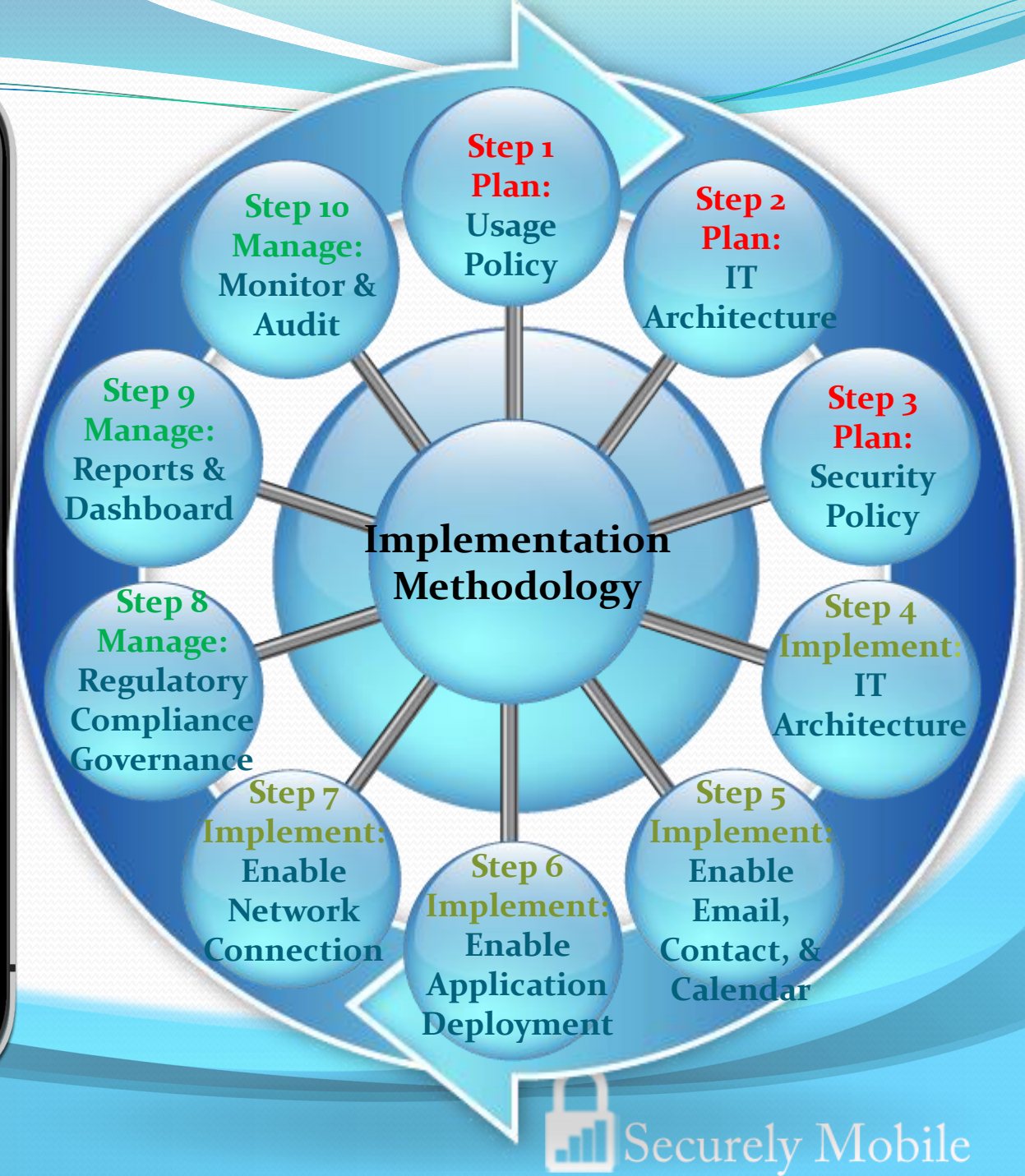
Securely Mobile

Evolution

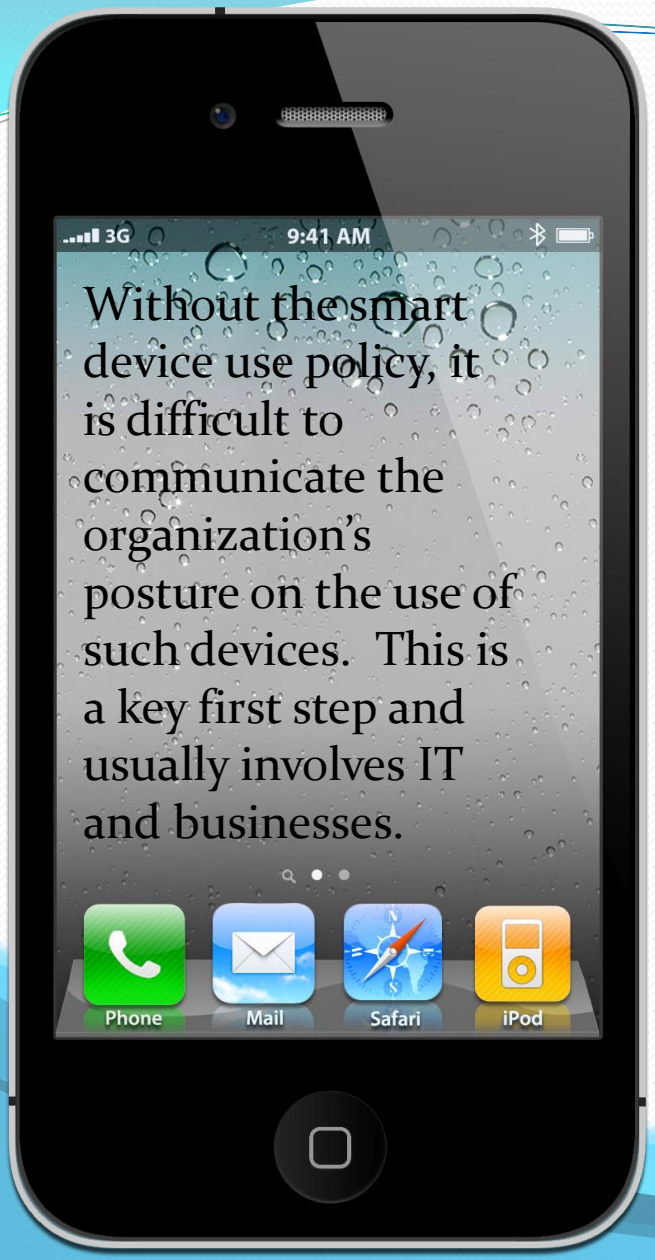
- Most Organizations relied on blackberry
- iPhone and iPad changed the executive landscape
- IT under pressure to also support
  - iOS (Apple)
  - Android (Google)
  - Windows Mobile (Microsoft)



PIM (Plan, Implement, Manage) methodology provides a comprehensive approach to organizations to manage and secure the smart devices.

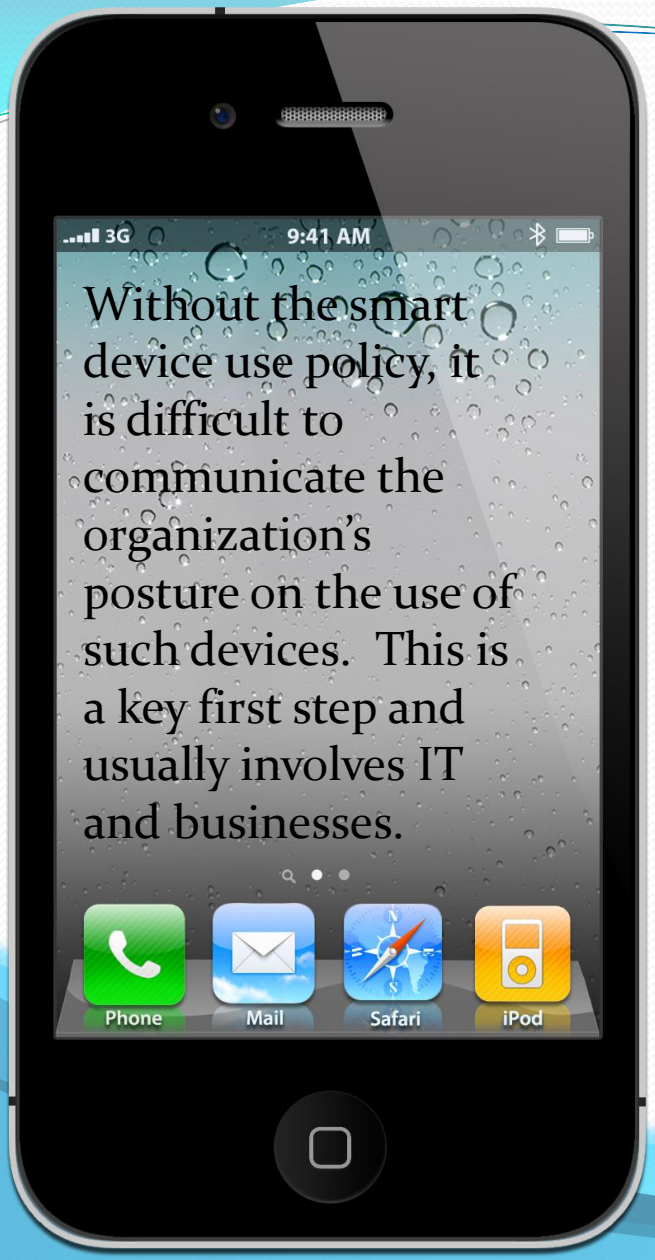


Securely Mobile



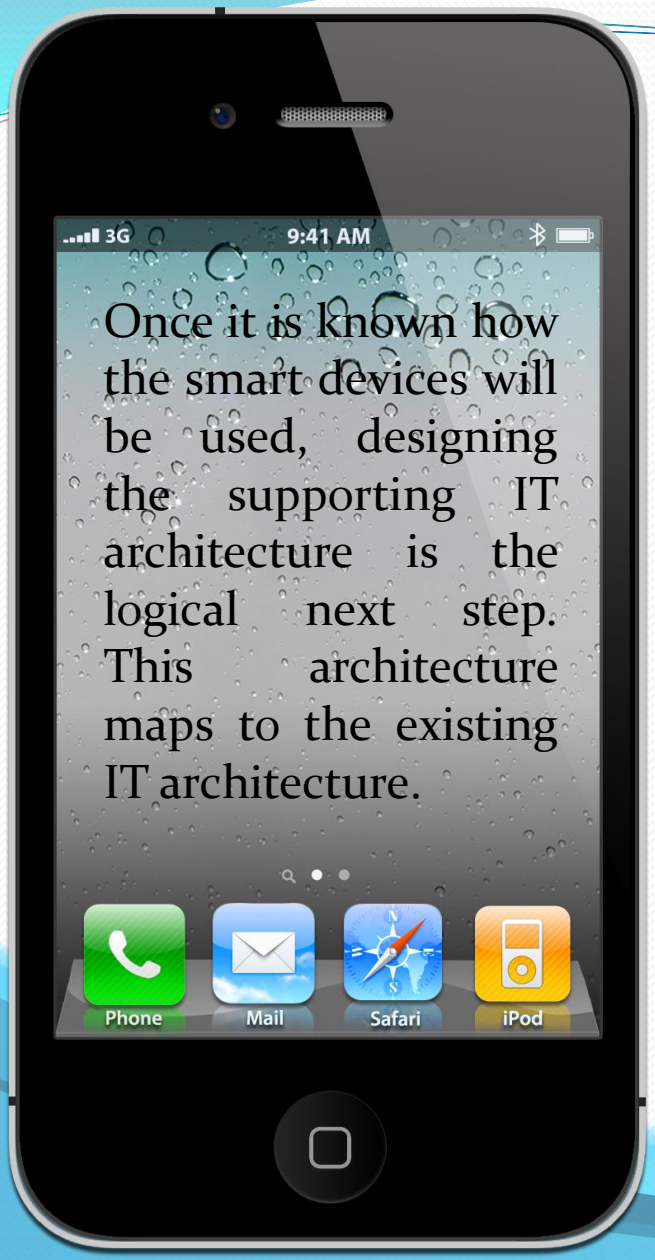
Audit Step 1

- Collect the following documents:
  - Smart Device Use Policy
  - Smart Device security Policy
  - IT Infrastructure architecture documents
  - MDM procedures
  - Reports produced from MDM



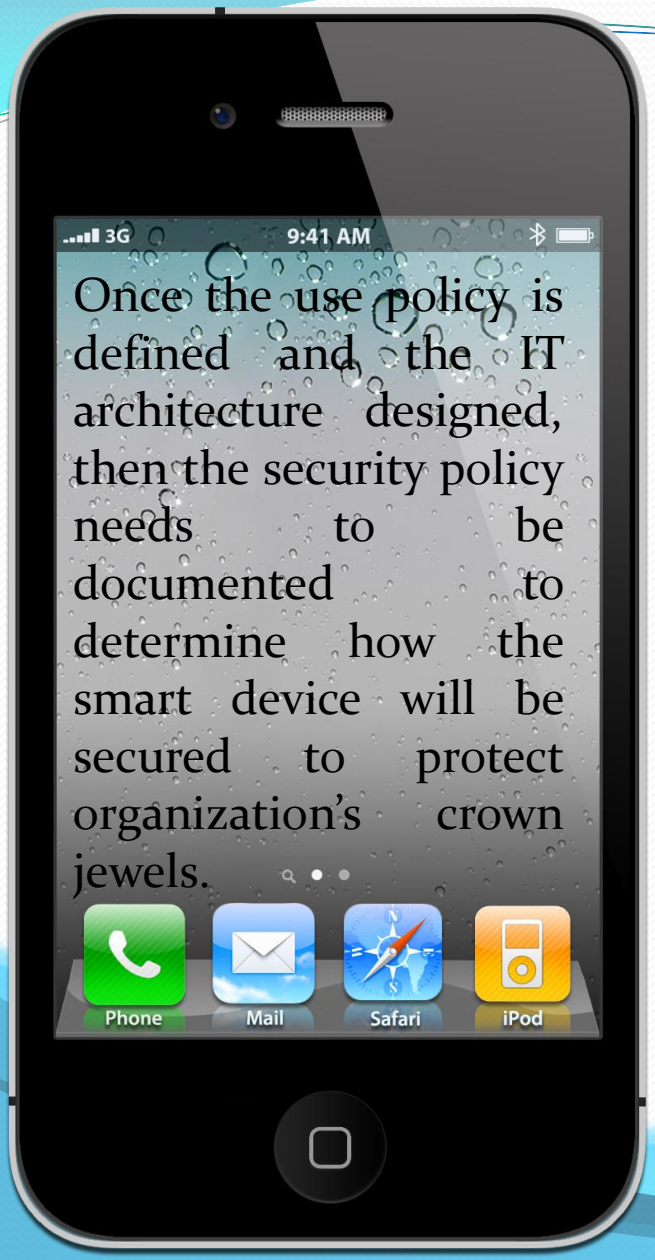
Audit Step 2

- Understand the smart device environment:
  - Is the device a corporate device or is BYOD (Bring Your Own Device) is allowed?
  - Is the corporate data separated from the personal data?
  - Is personal use of the device allowed (Can you play Angry Bird on your device?
  - Is an agreement in place where the employee abides with the corporate security policy?
    - Has the employee agreed to remote wipe of the device
    - Record of their phone calls may be viewed by corporate?
  - Is confidential data residing on the device? If so, what are the procedures in place to monitor and control the confidential data?
  - What type of smart devices are allowed? Apple only? Android only? Others?
  - Is there a backup strategy and procedure in place for smart devices?
  - Is the smart device connecting to the corporate network? How is it being connected?
  - How are applications pushed to the device? Is the corporation developing its own apps? Do they have their own app store? Marketplace?



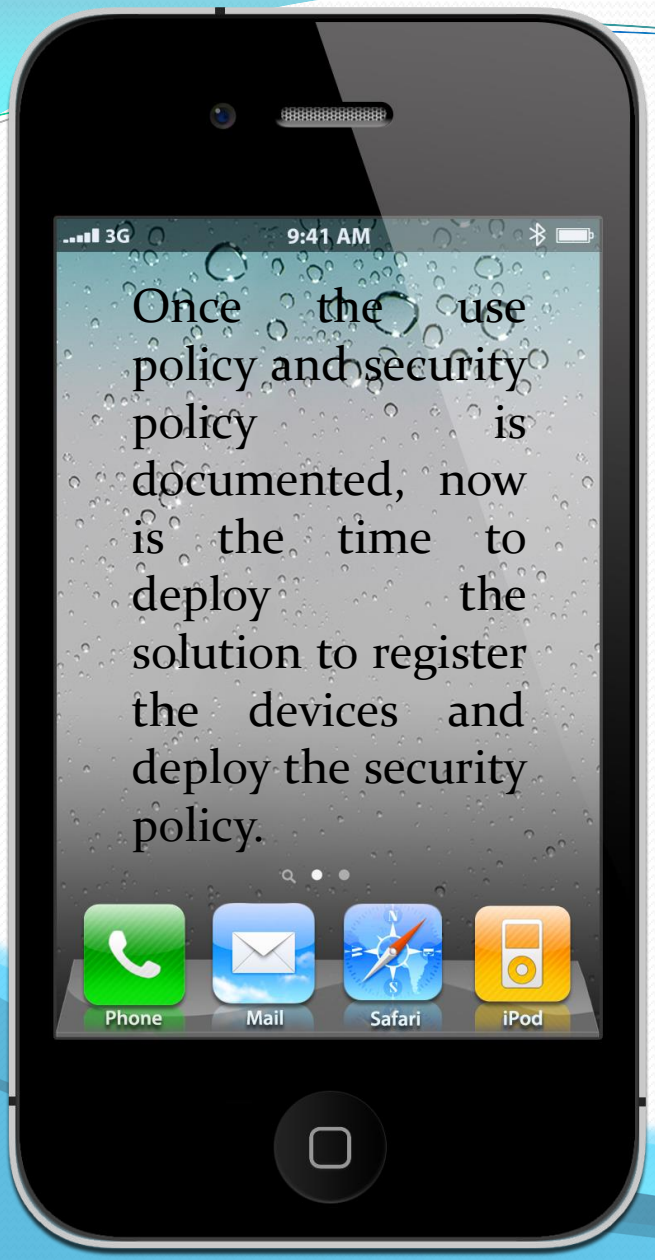
Audit Step 3

- Understand the IT architecture supporting the smart device environment:
  - Is the MDM solution cloud based solution or internally deployed?
  - Is the solution hosted by a third party or self supported?
  - Is there a business associate agreement in place with the vendor?



Audit Step 4

- Understand the smart device security features:
  - Verify that the password policy is meeting industry standards
  - Review the encryption requirements (specially for confidential data) and how encryption is deployed
  - Is there a requirement for port controls on a device (camera usage, bluetooth usage, WiFi controls)?
  - What procedure is in place for remote wipe/locking and unlocking of device
  - What procedure is in place for reporting of lost devices
  - How the devices are tracked and monitored
  - What device configuration is pushed as profile to the device (VPN? Email? Etc.)
  - How are the delivery of applications controlled to the device? Does the corporation use blacklisting? Whitelisting? How are the features implemented?
  - What audit and monitoring features are turned on? What reports are being generated?



Audit Step 5

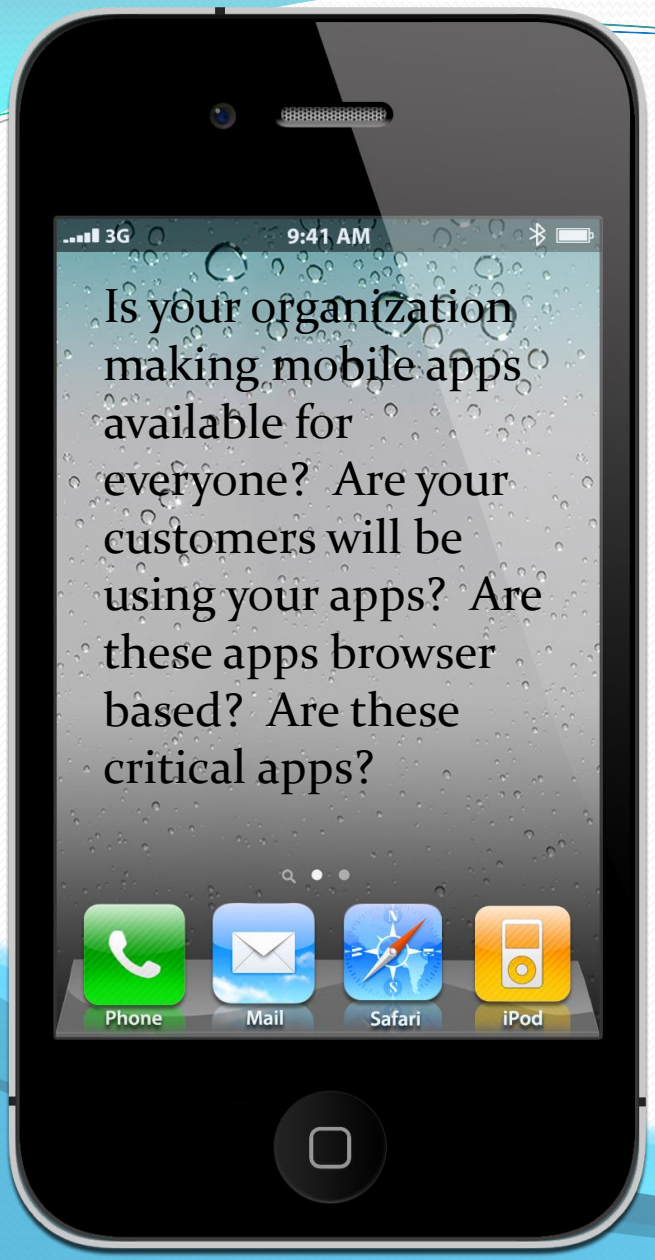
- Understand how the devices are enrolled into the MDM software
  - Does the organization use self-registry? How do users register their device?
  - How do users re-register when they purchase new device or replace an existing device? What happens to the old device? Is the data wiped off the device?
  - How is it verified that the appropriate security policy has been pushed to the device?

Audit Step 6

- Review the email, calendar and contact information
  - How is email synced with the corporate servers? Is the email encrypted?
  - Where and how is virus checking performed?

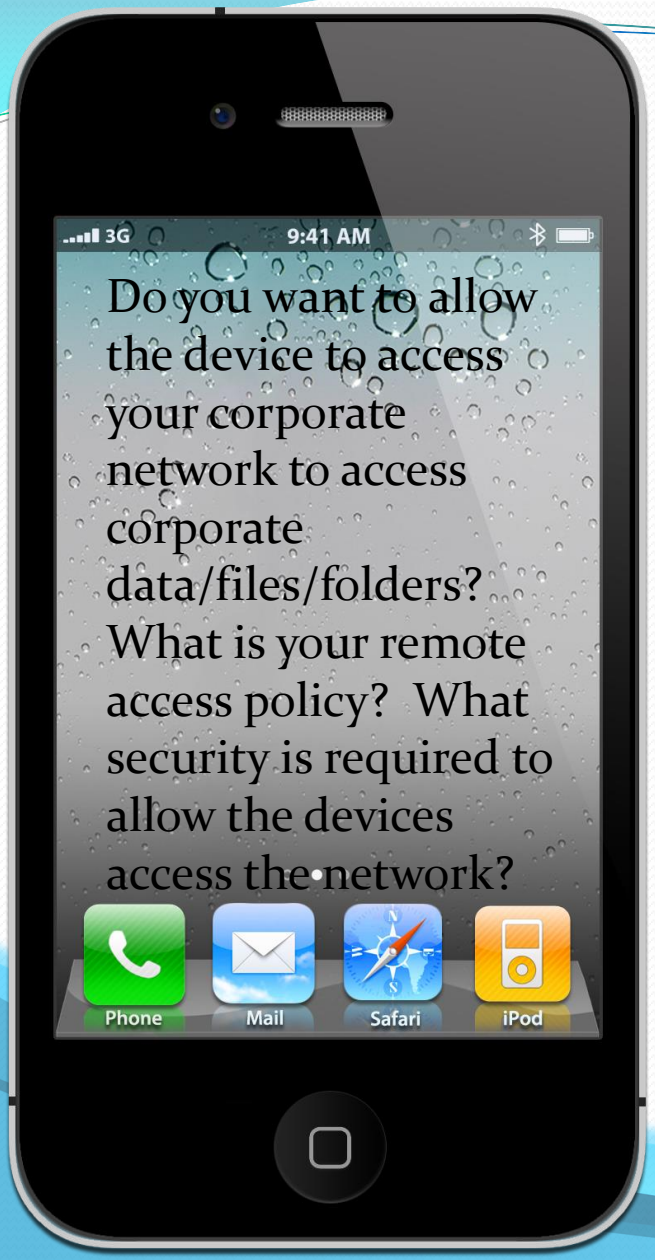
Securely Mobile

Audit Step 7



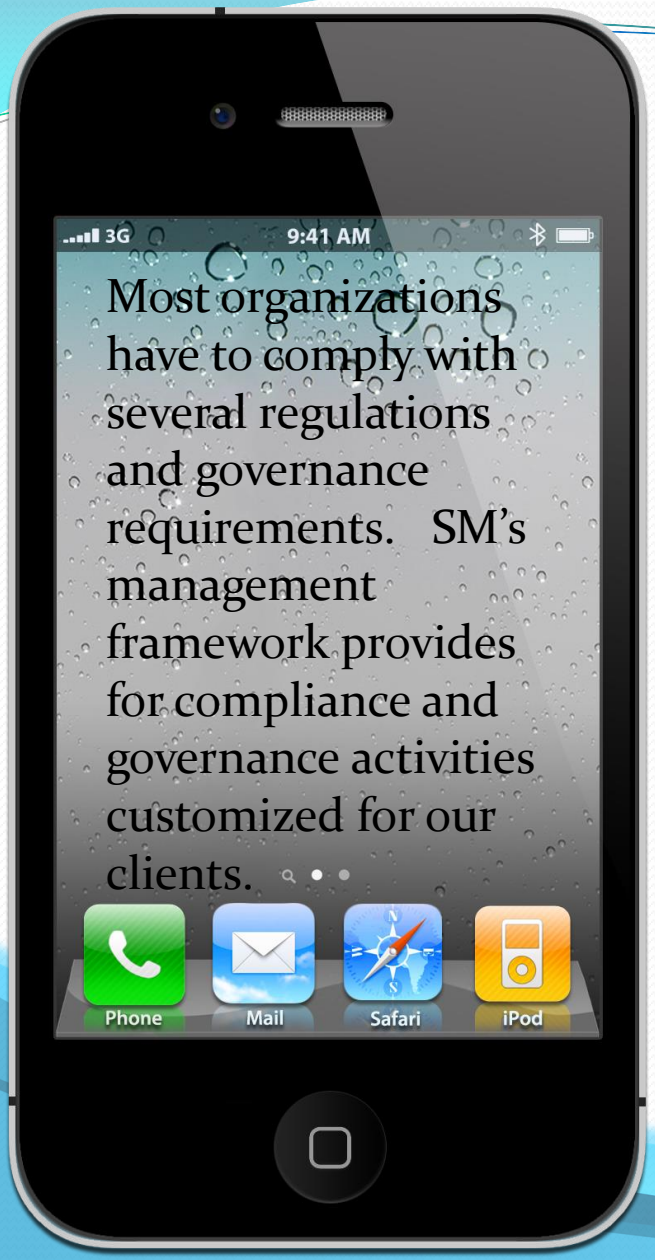
- Review the corporate apps running on the device
  - Review the homegrown applications and how the data is stored and encrypted on the device?
  - Review the whitelisting and blacklisting deployment
  - Review the authentication procedure for the applications – passwords? How are they authenticated? Is there an authorization process with corporate data?

Securely Mobile



Audit Step 8

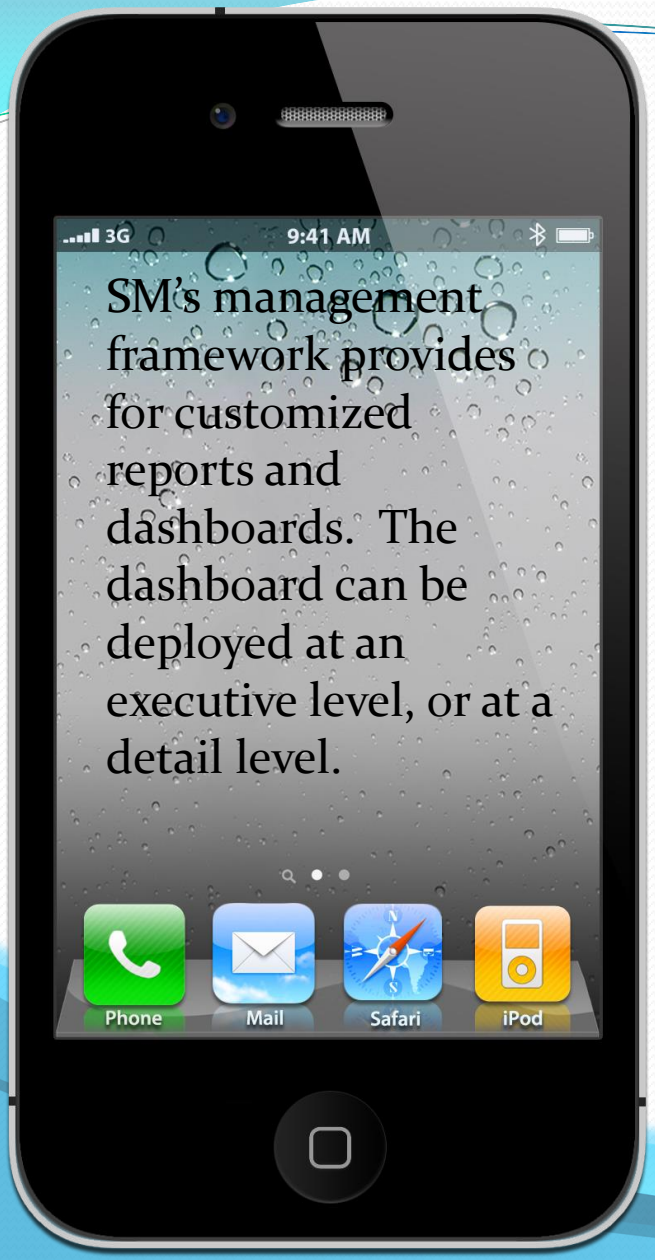
- Review the device connection to the corporate network
  - What type of remote connection is used?
  - What authentication is used prior to allowing access to corporate network?
  - What encryption protocols are in place for the remote connection?



Audit Step 9

- Review the regulatory and compliance requirements
  - What reports and controls are in place to support the HIPAA, SOX, PCI and other regulatory and compliance requirements

Securely Mobile



Audit Step 10

- Review management reports
  - What reports are reviewed by management?
  - What key statistics are monitored and reviewed?

Securely Mobile

Audit Step 11

- Review other device support services like eDiscovery, litigation hold etc.

Audit Step 12

- Document the risks and draft a report

Securely Mobile