



Implementing an Enterprise Mobility Strategy

Blair Nicodemus

Specialist Leader

Enterprise Mobility Solutions

Deloitte Consulting, LLP

bnicodemus@deloitte.com

+1 215 246 2350

August 23, 2011



The mobility world today

- Mobile computing has been growing at a staggering rate across age groups, income groups industries, geographies and cultures. Sample statistics:
 - 5B mobile subscribers globally as of December 31, 2010 (Gartner)
 - 300M smartphones sold globally in 2010 (Forrester)
 - 20M iPhones sold in Q2 2011 (Strategy Analytics)
 - 15M iPads sold since product launch in 2010 (Apple)
 - 83% of US population owns cellphones; 35% of these are smartphones (Pew Research)
- Mobile computing is widely expected to continue its spectacular growth rate over the next five years. Sample predictions:
 - Smartphone unit sales will surpass laptop unit sales in 2012 (Gartner)
 - Approx. 470M smartphones will be sold globally in 2011 (IDC)
 - Approx. 980M smartphones will be sold globally in 2016 (50% of all handsets sold) (IMS)
 - 2015 global mobile data traffic volume will be approximately 25 times 2010 volume (FCC)

Mobility growth is virtually unprecedented and is likely to continue for the foreseeable future.

Deloitte anticipates the following mobile technology trends over the next few years

Mobile Devices	<ul style="list-style-type: none">• Hardware performance improvements and chipset consolidation is likely to continue, leading to:<ul style="list-style-type: none">– More powerful, thinner, lighter and energy efficient devices with desktop-like performance.– Support for more powerful business applications, consumer applications and games.• Carriers are likely to continue to support several hardware vendors to benefit from supplier competition.• Carriers and device manufacturers are likely to continue to offer devices at different styles and price points to appeal to different market segments and tastes.
Embedded Hardware	<ul style="list-style-type: none">• GPS is likely to be standard, enabling widespread use of location-aware applications.• Cameras are likely to be standard, enabling real-time photo sharing, videoconferencing, image projection, bar code scanning and augmented reality overlay.• Near Field Communications (NFC) are likely to be standard, enabling widespread mobile payment.• Sensors are likely to increasingly be present in devices, creating new data collection opportunities.
Wireless Technology	<ul style="list-style-type: none">• Carriers are likely to continue investing in spectrum, towers and wireless technology, leading to wider high-speed coverage, more reliable connections and faster connection speeds.• Mobile devices are likely to support multiple wireless technologies and transparently transition across indoor, outdoor, urban, suburban and rural locations.<ul style="list-style-type: none">– Embedded Wi-Fi enables indoor coverage, cellular offload and tariff avoidance.
Mobile Operating Systems	<ul style="list-style-type: none">• Rapid release cycles are likely to continue as vendors fight for market share through innovation.• Continuous feature additions are likely to force continuous user interface experimentation.• Mobile applications are likely to increasingly leverage GPS and sensor data provided by the operating system (OS).• OS consolidation is likely to be limited due to carrier desire for competition.

**Mobile devices are likely to become more powerful and sensor rich.
The hardware and mobile OS environment is likely to remain heterogeneous.**

As used in this document, "Deloitte" means Deloitte LLP and its subsidiaries. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Deloitte anticipates the following mobile application trends over the next few years

Social Media	<ul style="list-style-type: none">• Pervasive social networking features in web sites, business applications, games, etc.• Micro blogging on corporate Intranets as unstructured knowledge-sharing vehicle.
Mobile Marketing	<ul style="list-style-type: none">• Location-based services and customer engagement tools, such as couponing, loyalty programs, awards, proximity marketing, geo-tagged purchase history, etc.• Crowd sourcing and consumer apps that provide instant notification of problems.
Mobile Payment	<ul style="list-style-type: none">• Near Field Communications (NFC) and alternative technologies will likely streamline peer-to-peer and conventional retail financial transactions.
Augmented Reality	<ul style="list-style-type: none">• Real-time view of the physical environment overlaid with virtual, computer-generated imagery and information.
Personal Productivity	<ul style="list-style-type: none">• Personal medical data monitoring and analytics, text-to-translated-speech, remote house control, remote car monitoring, etc.
Enterprise Applications	<ul style="list-style-type: none">• Instant access to any business application, workflow or transaction; faster approvals.• Users able to seamlessly roam between devices while accessing cloud-based services.• Increasing use of sensor data (geo-tagged transactions, transaction photos, etc.)
Mobile Analytics	<ul style="list-style-type: none">• Instant access to business dashboard from any location with extensive drill-down capability.

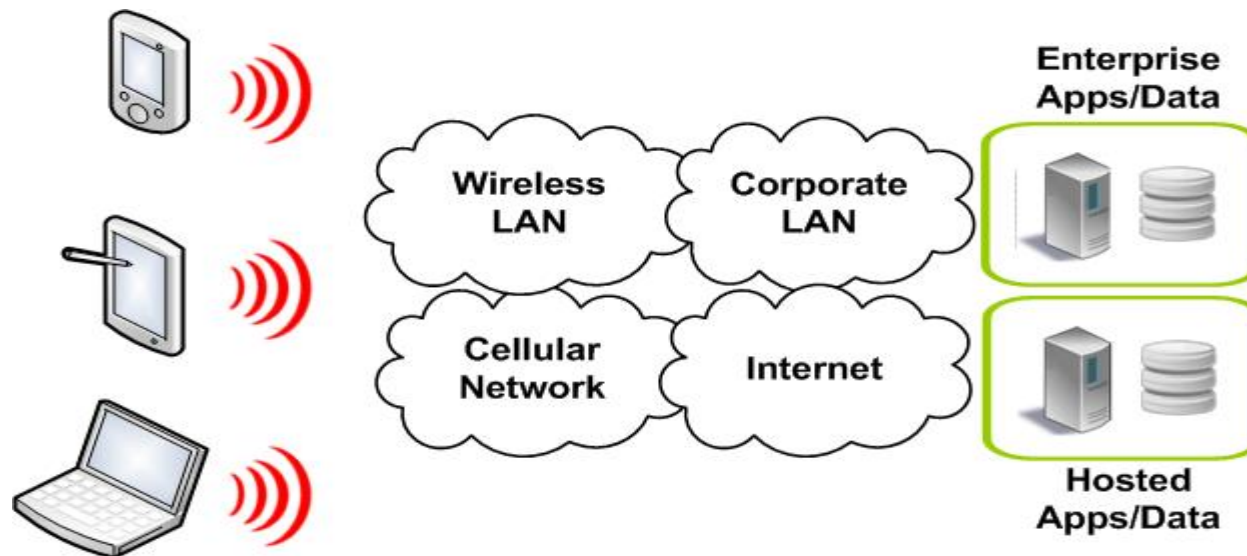
Software innovation is likely to continue and result in new applications that enhance our personal and professional lives.

Why should enterprises go mobile?

- Widespread consumer adoption creates a new communication channel
 - Mobile sales and services
 - Mobile payments and account access
 - Citizen/customer self-service
 - Citizen/customer incident reporting (inbound alerts)
 - Notifications and recalls (outbound alerts)
- Improve staff productivity and efficiency
 - Executive reporting, analytics and dashboards
 - Customer relationship management (CRM)
 - Mobile time and expense entry
 - Workflow review and approval
- Capture data at transaction point
 - Retail/Factory shop floor
 - Field inspections, maintenance, repairs, inventories and investigations
- Remote asset monitoring and control
 - Infrastructure monitoring and alerts (HVAC, bridges, manufacturing equipment, etc.)
 - Real-time security threat monitoring and alerts
 - Remote control/reboot of any asset from any location

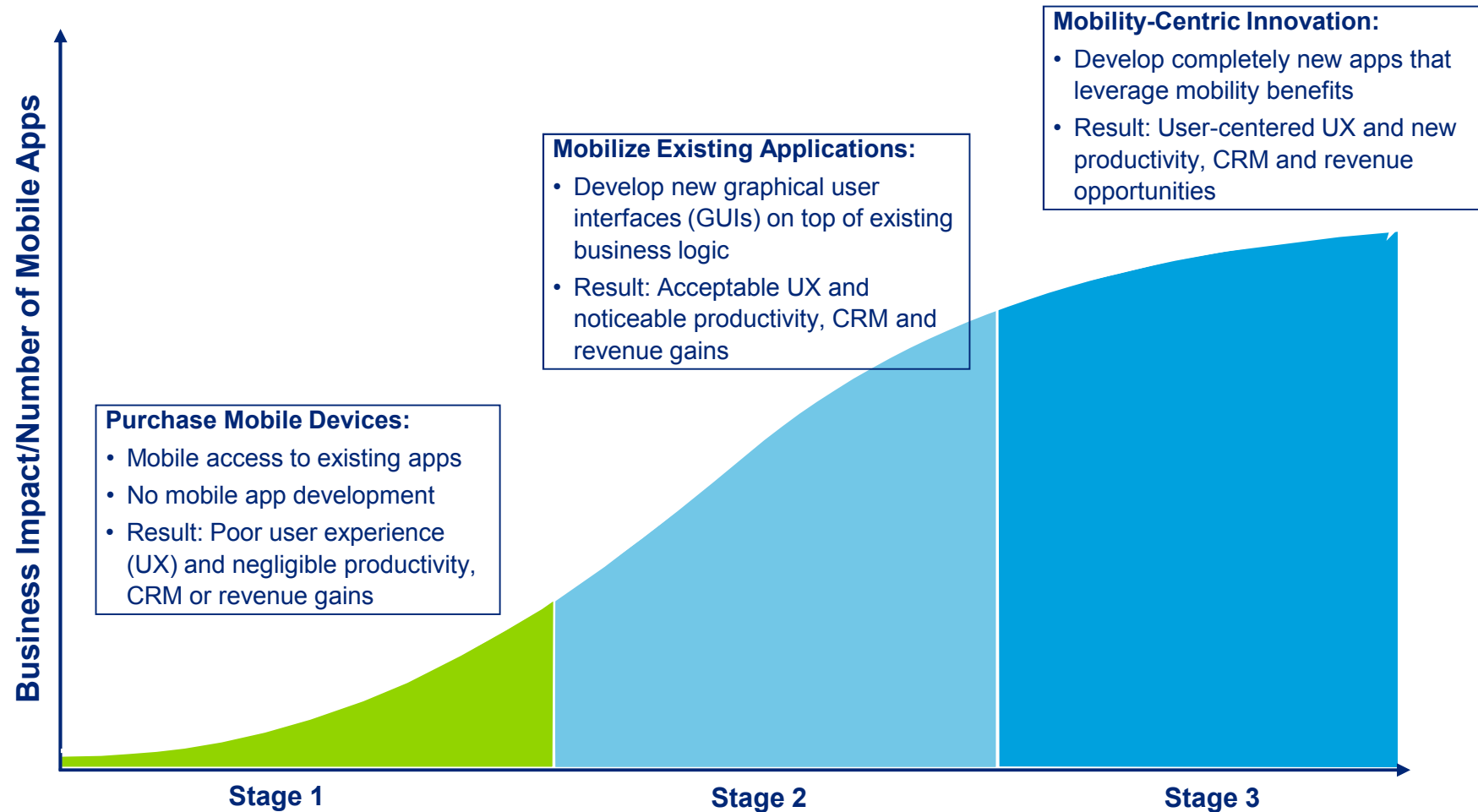
Mobility opportunity for federal agencies

- Mobile E-forms, faster management approvals, customer self-service apps, sensor-tagged transactions, instant access to analytics, remote asset monitoring and control, and other mobile solutions can transform the agency's relationship with employees, contractors, suppliers and customers.
- When combined with cloud computing, workers can seamlessly switch back and forth between desktops, laptops, tablets and smartphones over the course of the day.



Mobility can significantly improve productivity, data quality, operational efficiency, customer responsiveness and customer satisfaction. The mobile cloud can provide rapid access to important business data, customer data and transactions from almost any device and location.

Typical enterprise mobility adoption trends observed by Deloitte



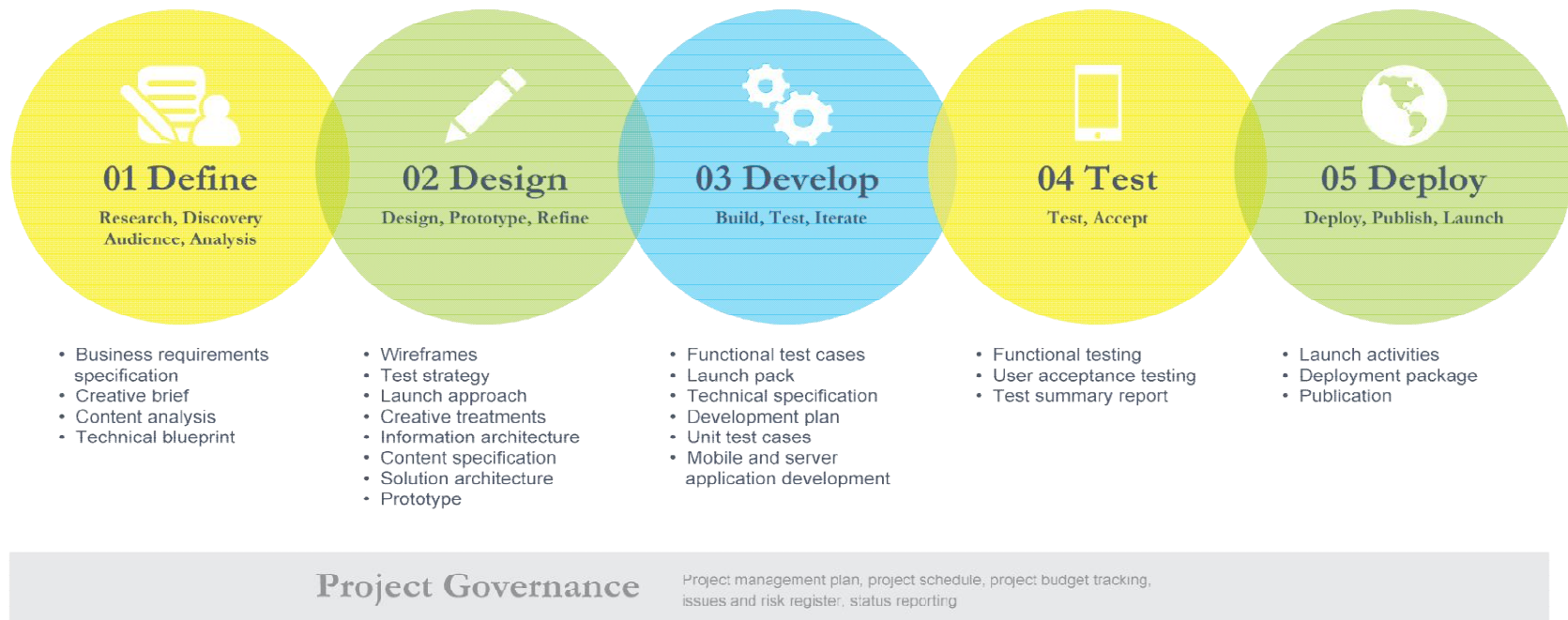
Enterprises often focus on the device and a few priority mobile applications without planning for a long term mobility transformation. As momentum picks up, disparate initiatives duplicate effort and use inconsistent processes and leading to support problems.

Developing a mobility strategy starts with establishing a business mobility roadmap and mobility requirements

Define business mobility goals	Establish a mobility steering committee or program management office (PMO) to coordinate efforts across the enterprise. What are the highest priority business goals? How can mobility help achieve these goals? What user communities are the most mobile or have the most customer interaction? What customer/consumer applications would provide the most value?
Develop business cases and prioritize the roadmap	Convert broad mobility goals into a list of desired mobile applications. For each mobile application create an executive summary that identifies the primary objectives, tangible and intangible business benefits, most important capabilities and features, primary users, primary beneficiaries, etc. Prioritize mobile applications 'wish list' based on business benefit to create a roadmap.
Integrate mobile channel with existing channels	Employees, customers and partners will continue to leverage existing channels (web, call center, face-to-face), but now also want to connect to information using smartphones and tablets. Supporting them requires a multichannel approach with an integrated view of the customer. Define how the mobile application will be distinct from or overlap other channels.
Develop use cases for mobile applications	Drill down into the intended user, situation and transaction. What does the user need? What data entry is required? What data must be available? In what presentation form? At what levels of summary or granularity? Where is the transaction physically taking place? What is the type, availability, performance and reliability of wireless connectivity in that location?
Identify target mobile devices	Map desired functionality and use cases to smartphones and tablets and assess for fitness. Refine use cases as needed. Decide whether the application will be deployed to smartphones, tablets or both. Smartphone have smaller displays than tablets; what functionality will be dropped or adapted to simplify the user interface and provide an enhanced user experience?

Mobile applications should be developed using a methodology tailored for mobile devices

- Tailoring existing software development processes to the specific functionality of mobile devices is important because the mobile hardware, OS, user interface, data security and network connectivity considerations are significantly more complex than the “Wired/Wintel Desktop World.”
- The following shows key activities that should be included in each phase of the mobile application development life cycle:



A mobility strategy should establish a framework for developing mobile applications

Several architectural approaches are possible for developing mobile applications. Examples:

	Full Client	Rich Client	Thin Client
Distinguishing Attribute	All GUI, business logic and data reside on the mobile device.	GUI and logic reside on the device; data is in the cloud	All GUI, business logic and data reside in the cloud.
Strengths	Application accessible even when wireless connectivity is unavailable; highly responsive UI because all logic and data is local and full access to local hardware (e.g. camera and GPS)	Responsive UI since only data is downloaded on demand; no data persistently stored on device; data fresh when wireless available and cloud friendly	No software or data stored on the device; updates applied to server only; no stale data; Permits cross-platform content and cloud friendly
Weaknesses	App must be preinstalled on user devices; patches and data must be pushed to device or retrieved by user; all data stored on the device; risk of stale data; Asynchronous data and software updates and requires OS-specific executable	App must be preinstalled on user devices; patches must be pushed to device or retrieved by user; limited usability when wireless is unavailable; requires OS-specific executable	Application inaccessible if wireless unavailable; temporary wireless disruption may cause session loss; sluggish UI because of server round trip latency and limited access to local hardware
Example	Angry Birds	Weather applet	Mobile web; Virtual desktops

A development framework establishes mobile app design guidelines, can accelerate development and testing, improves usability and helps reduce security vulnerabilities.

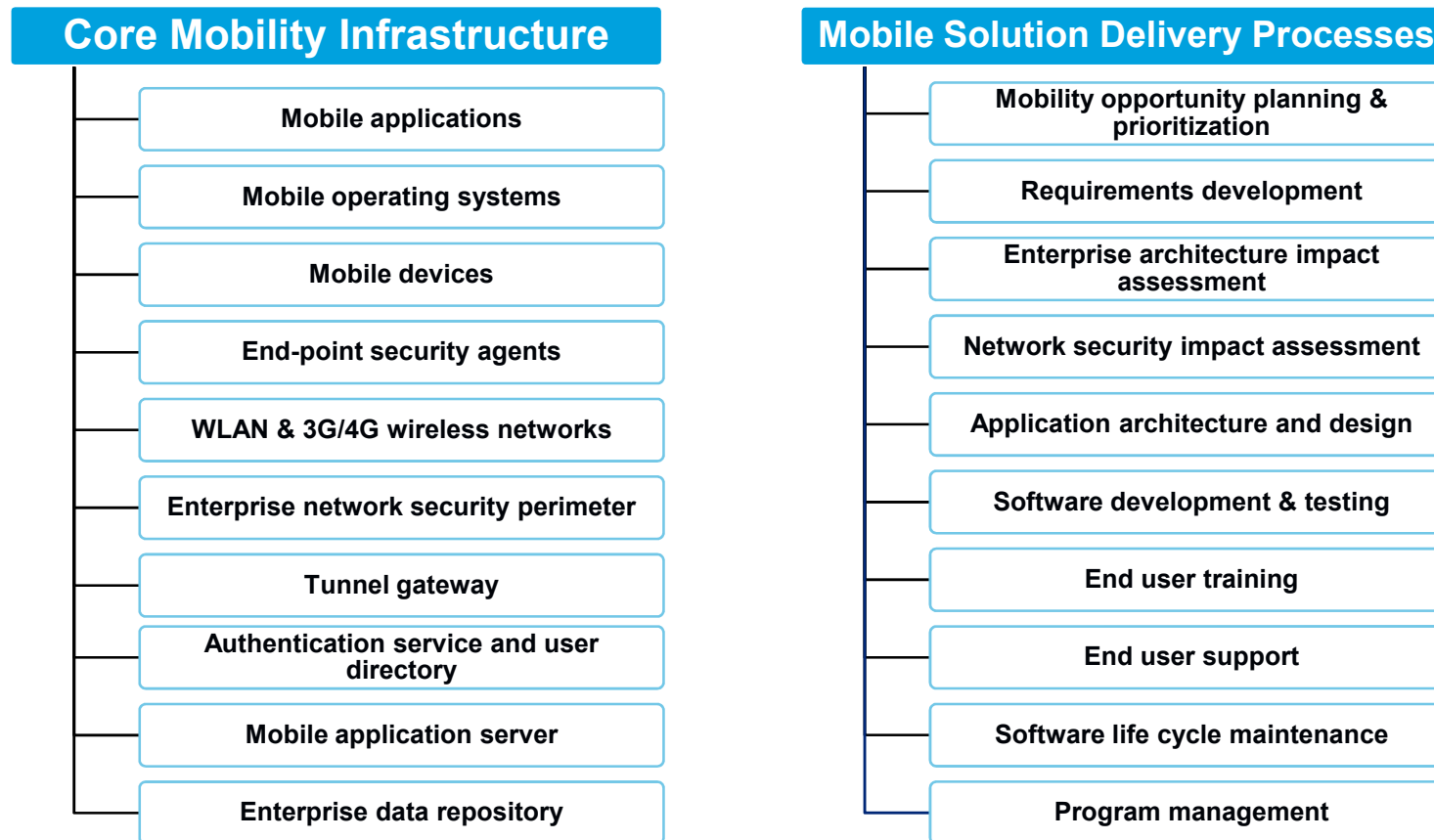
A mobility strategy should tailor security policies and controls for mobile applications, user authentication, data protection and exposed server applications

When developing mobile applications, security considerations should be factored in at each stage of the mobile application development life cycle in order to minimize security vulnerabilities.

Planning and Definition	Secure planning establishes the security requirements for the application.
Design and Architecture	Secure design identifies security issues and provides mitigation solutions for the architecture and design aspects of the software
Development	Secure development pertains to allowing software development processes with methodologies and tools to produce secure code.
Testing	Secure testing leverages various toolkits, emerging threat intelligence information and appropriate methodologies to perform anonymous as well as user-level software security testing.
Deployment	Secure deployment provides the conformance of software development process to other information security processes and monitors the occurrence of intended periodical software security tasks.

A mobility strategy should address security from an end-to-end perspective

Mobile applications intersect with numerous IT systems and IT processes. Examples:



A mobile enterprise security framework assesses each intersection with systems and processes to reduce known risks and new risks.

A mobility strategy should define supported devices, establish a framework for managing supported devices, and a framework for supporting future devices

- Mobile device management provides full life cycle support for mobile devices, mobile applications and associated data stores to help ensure:
 - Applications, patches, security agents, etc. are properly provisioned
 - Data is automatically backed up and protected at all times (at rest and in transit)
 - Devices are configured correctly and protected from threats
 - IT can remotely correct problems, wipe data and disable the device
- This requires systems, defined processes and skilled resources in multiple areas. Examples:

Provisioning

- Initial mobile device & mobile apps request
- Map user & device to a user group & mobile applications
- Wireless service provisioning
- Network access controls provisioning
- Image the mobile device (apps, settings and security agents)
- Enrollment in device monitoring platform
- On-device isolation of user apps/data from enterprise apps/data

Asset & Configuration Management

- Physical asset tracking & accounting
- Software license accounting & management
- Hardware repair/replace & warranty issues
- End user data backup
- OS & application patch testing
- Device configuration management
- Over-the-air updates

Security

- User authentication (including PIV card)
- Device, mobile app and enterprise app access control
- Stored data encryption and end-to-end encryption
- Application whitelist/blacklist
- Content filtering and malware protection
- Security event monitoring, logging and response
- Data leak protection & removable storage control

User Support

- Password reset
- Remote troubleshooting
- Device/app/data restore
- Device support roadmap
- Trouble ticketing and support knowledge database
- Trend analysis
- Help desk training on devices and apps

The bring your own device (BYOD) trend and the consumerization of IT

- Powerful and connected smartphones and tablets have penetrated every facet of our personal and professional lives and are used continuously over the course of the day.
- Employees increasingly want to use their favorite mobile device for personal and professional use. They want to store personal data and install Internet games on devices used to access enterprise applications and data.

BYO Rationale

- User Perspective:
 - Desire for one device and phone number, not two
 - Desire to fully own the decision process when selecting a personal device
 - Desire for the latest and greatest gadget
- Company Perspective:
 - Increased staff productivity due to better morale & hardware
 - Potential to reduce hardware, monthly service, provisioning and ongoing support costs
- IT Department Perspective:
 - Potential for reduced IT staff workload as users move off employer provided devices and onto BYO devices

BYO Challenges

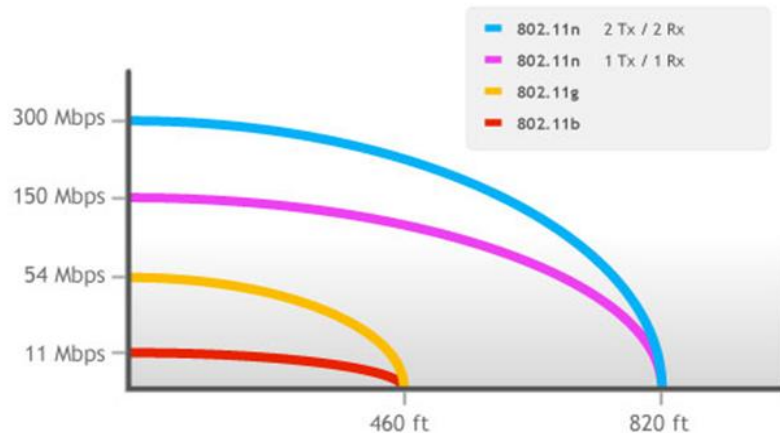
- Security
 - Enterprise data confidentiality, integrity and availability
 - Liability for personal data (wipe, central storage)
 - Defining the security perimeter
- Applications
 - Impact of heterogeneous device environment on application development and support requirements
- Support
 - Device certification, provisioning and management
- Cost
 - Potential loss of corporate-level volume discounts because of personal purchase.

Enterprises should align user mobility expectations, IT capabilities and the needs of the business. Failure to act may increase security risk as unmanaged mobile devices continue to connect to the enterprise network.

A mobility strategy should address wireless connectivity to leverage the power of the mobile device

Wireless LANs (Wi-Fi)

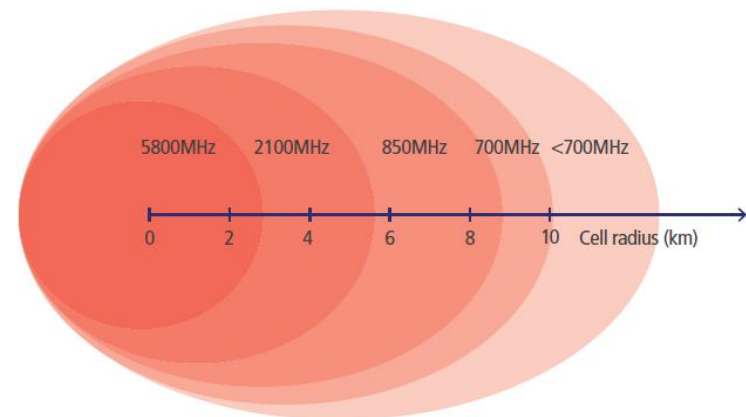
- Wireless LANs (WLANs) connect **local** wireless devices to one another (peer-to-peer) or to a local wireless access point (AP)
- The enterprise provides their own APs
- Main WLAN standards are:
 - 802.11b: 10Mbps, 2.4Gz
 - 802.11g: 54Mbps, 2.4GHz
 - 802.11a: 54Mbps, 5GHz
 - 802.11n: MIMO multi-antenna technology
- Range is a few hundred feet



Graphic Source: Amped Wireless

Cellular Wireless (3G/4G)

- Cellular/mobile data networks connect roaming wireless devices to a **cellular** network tower
- Service is purchased from a wireless carrier
- Main cellular wireless standards are:
 - GSM (GPRS, EDGE, UMTS, HSPDA, HSPA)
 - CDMA (1XRTT, EVDO, LTE)
 - WiMax
- Range is a few miles

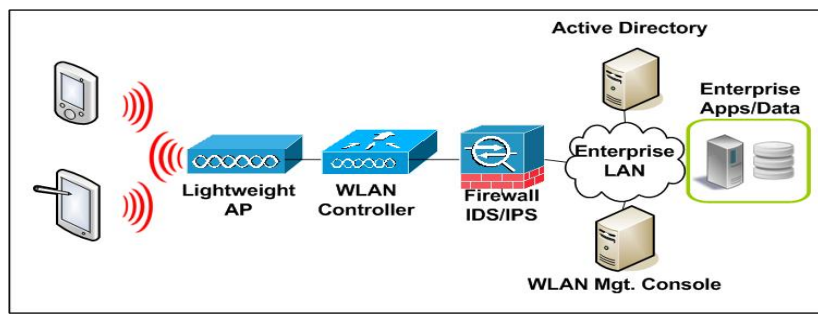


Graphic Source: GSM Association

A mobility strategy should address wireless security to protect the mobile device and applications servers

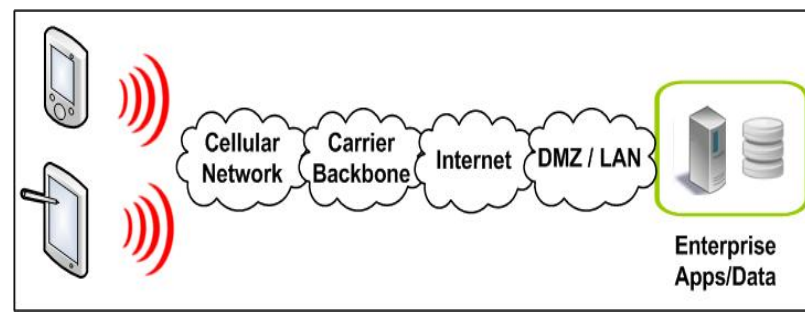
Wireless LANs (Wi-Fi)

- NIST 800-97 provides guidance on how to secure WLANs
- Security requires as a minimum:
 - FIPS 140-2-compliant wireless link encryption
 - Strong device and user authentication
 - Security boundary between WLAN and wired LAN
- WLAN cautions:
 - Certificate-based authentication needed to prevent connections to unauthorized APs
 - Device lockdown essential to enforcing wireless security policy
 - RF environment monitoring essential to detect intrusion attempts, misconfigured & unauthorized devices and WEP/WPA use



Cellular Wireless (3G/4G)

- Cellular/mobile data networks provide strong link encryption and device authentication, but enterprise data traverses the Internet
- Security requires as a minimum:
 - FIPS 140-2-compliant end-to-end encryption
 - Strong device & user authentication
 - Access controls to protect exposed servers
- Cellular wireless cautions:
 - Unpredictable outdoor coverage
 - Rural/international coverage holes
 - Unpredictable in-building performance
 - Silent cutover to Wi-Fi

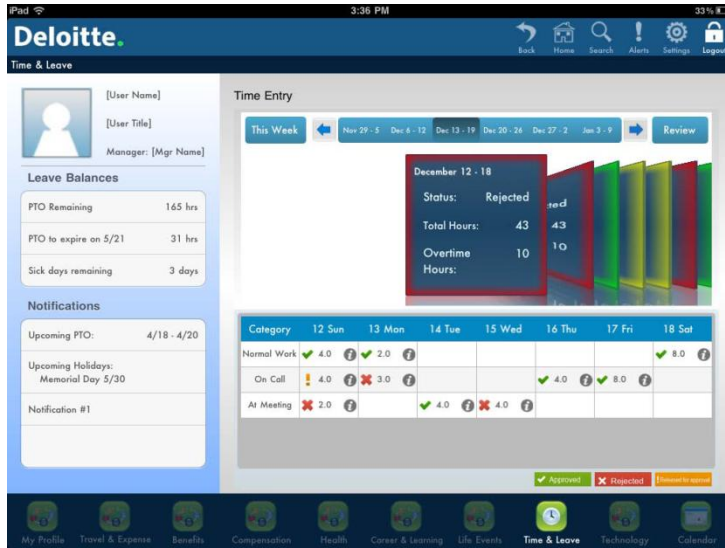


Summary: Jumpstarting your enterprise mobility strategy

Application Roadmap	Establish a mobility leadership team. Identify, justify and prioritize mobile applications for each business unit (e.g. sales force enablement, customer relationship management (CRM) analytics, personal productivity, etc.). This becomes your mobility roadmap.
Application Requirements	Develop mobile application use cases, requirements, wireless connectivity requirements and wireframes. Confirm the planned feature set aligns with the planned device and complements other connectivity channels.
Application Architecture	Understand tradeoffs of alternative mobile application architectures and develop a decision framework for when to use a given architecture. Develop a cloud-friendly architecture that allows seamless roaming between smartphone, tablet and laptop over the course of the day.
Application Development	Decide whether you intend to support multiple mobile operating systems (OS) and develop a multi-OS development strategy. Evaluate and shortlist SDKs. Develop proof of concepts.
Application Deployment	Develop a mobile application rollout framework that addresses QA testing, user training, user documentation, help desk readiness, pilot testing, etc.
Security	Evaluate security risks and develop a response plan at each point in the end-to-end mobile transaction flow and mobile application life cycle support processes.
Device Management	Develop mobile device procurement, security and management standards. Define mobile device management & data protection requirements & solution. Develop an agile process for evaluating and slipstreaming future mobile devices into the IT support process.
Wireless Connectivity	Ensure you have pervasive, reliable, high-speed wireless connectivity everywhere mobile users are. Ensure wireless networks are properly secured (authentication, encryption, perimeter inspection) and monitored.

An enterprise mobility strategy establishes a framework to guide technology, design, process and resource decisions made while rolling out mobile applications. It provides a roadmap for success.

Federal Mobility Relevant Applications - Examples



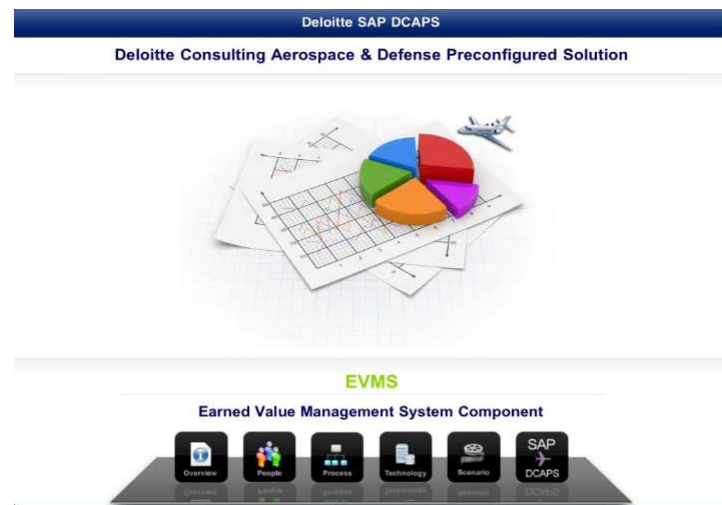
Mobile Time keeping



Utilities Green Monitoring



ArcSight Security Monitoring



EVM Reporting/Monitoring

Deloitte.