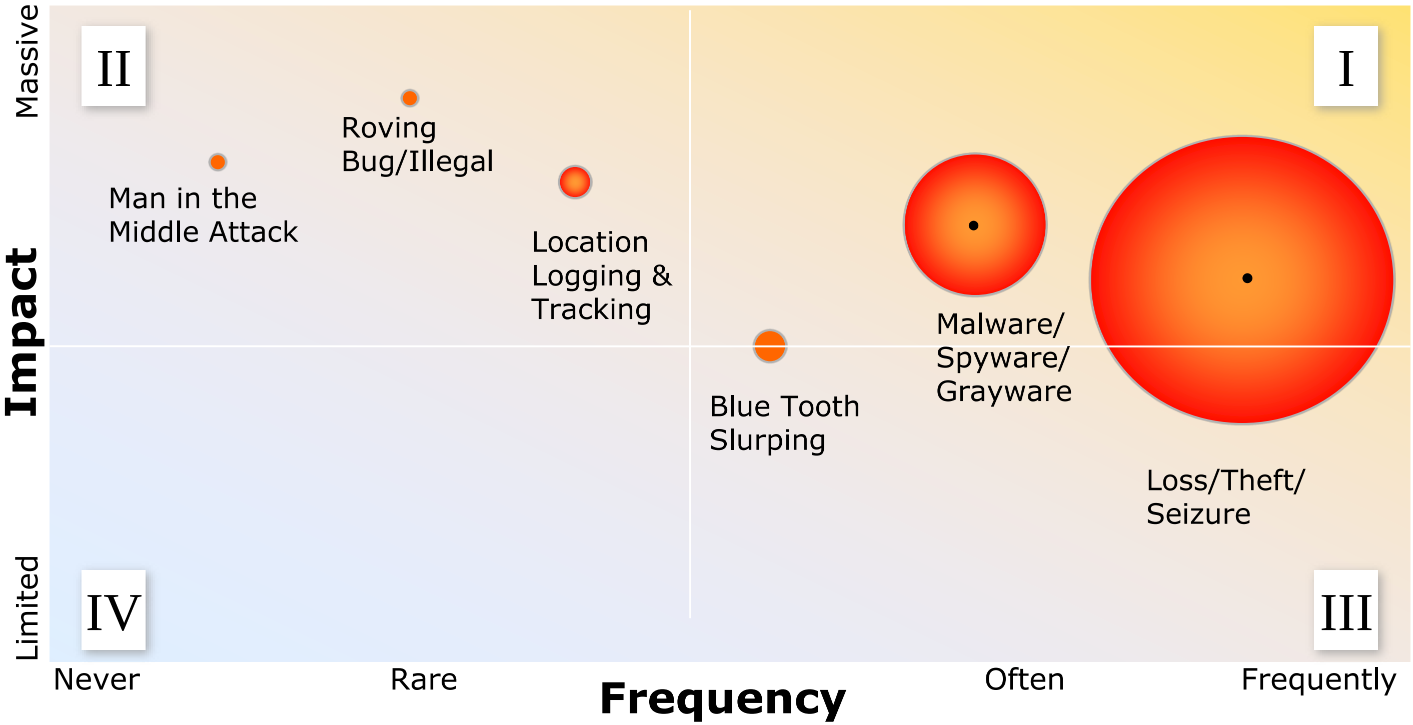
IBM BusinessConnect
Realise the art of the possible.

Delivering Confidence to Seize the Mobile Opportunity

Vijay Dheap
Global Product Manager, Master Inventor
Big Data Security Intelligence & Mobile Security
vdheap@us.ibm.com

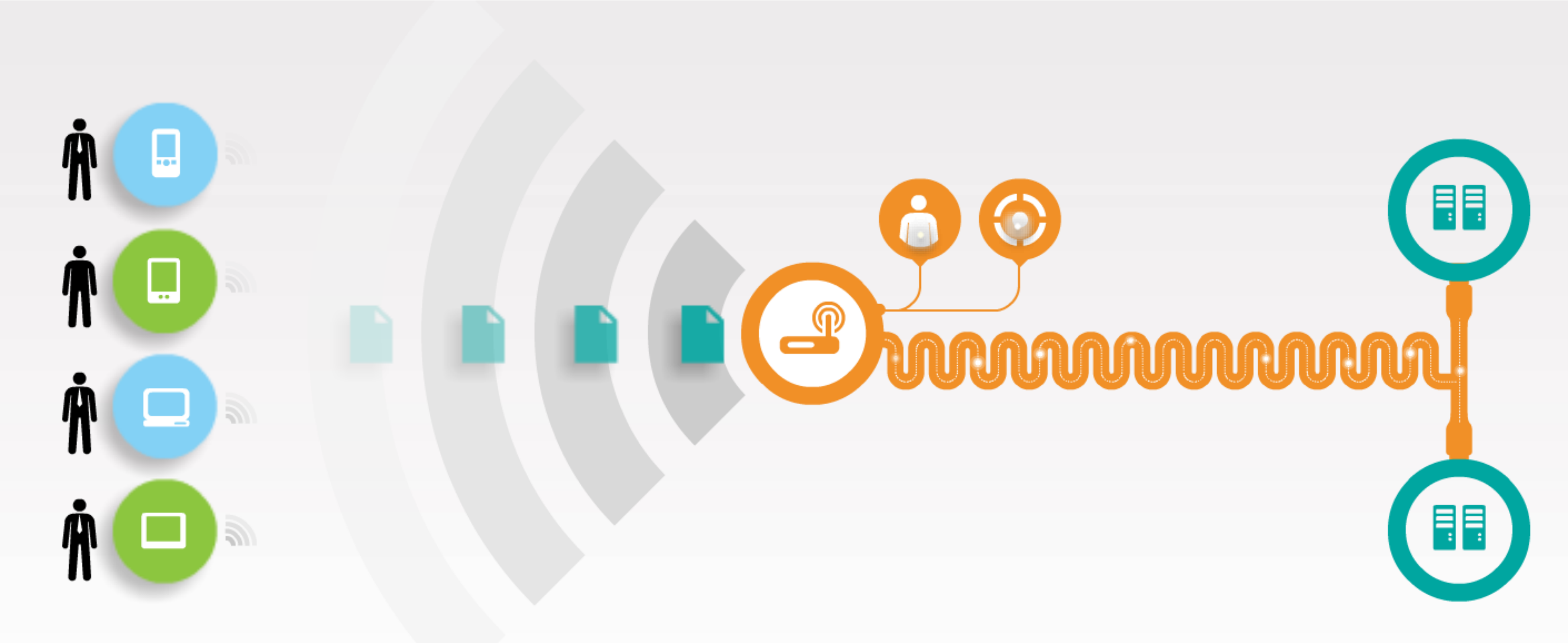
What Are Mobile Security Concerns?

Based on Gartner, Mobile Security Risks, interviews with members of ISS xForce, and Corporate Executive Board. e.g. Industry (not IBM only) view



Control Category I: Focus on risks for all mobile devices used by IBMers for IBM business purposes
Control Category II: Focus on risks for targeted populations of IBMers (ex. SVPs)

A Structured Approach to Designing Your Mobile Security Strategy



Device Management

Security for endpoint device and data

Network, Data, and Access Security

Achieve visibility and adaptive security policies

Application Layer Security

Develop and test applications

Device Security & Management

Where to begin? Develop a greater understanding of BYOD Programs

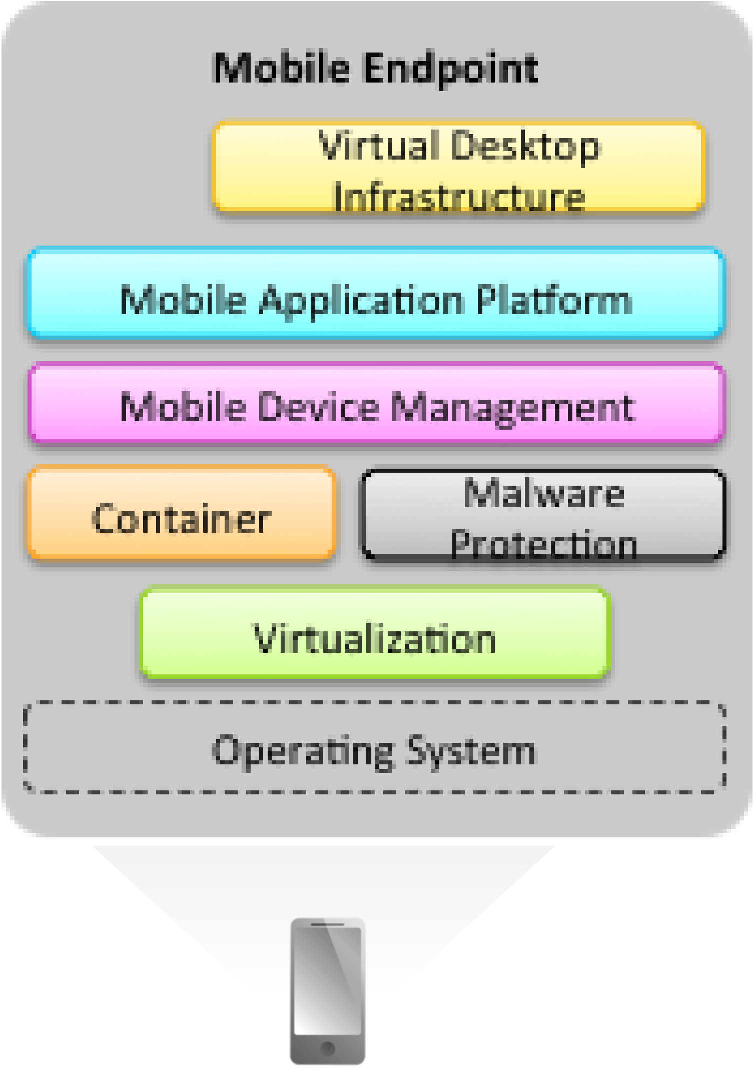
Degree of Platform & Device Choice: Organizations can determine the degree of choice they afford their employees in selecting their mobile devices.

Documenting Usage Scenarios: To gain a better understanding of the risk profile of a BYOD program, a detailed understanding of how employees wish to employ their personal devices for work tasks is essential. This will also influences the degree of oversight necessary to mitigate the risk.

Identification of Sensitive Data/Content: To assist in prioritization when designing an organization's BYOD security posture it is necessary to enumerate what data or content needs to be accessed and if that content will need to be stored on devices.

Building the Business Case – Cost/Benefit Analysis: BYOD programs can have many hidden costs that erode the cost savings gained from not having to purchase the device themselves. There is an imperative to define metrics that help quantify the business value gained from the program and to mitigate cost increases.

Options for Securing Mobile Endpoints…



Protecting Mobile Access to Data over the Network

Where to begin? Achieve visibility and adaptive security policies

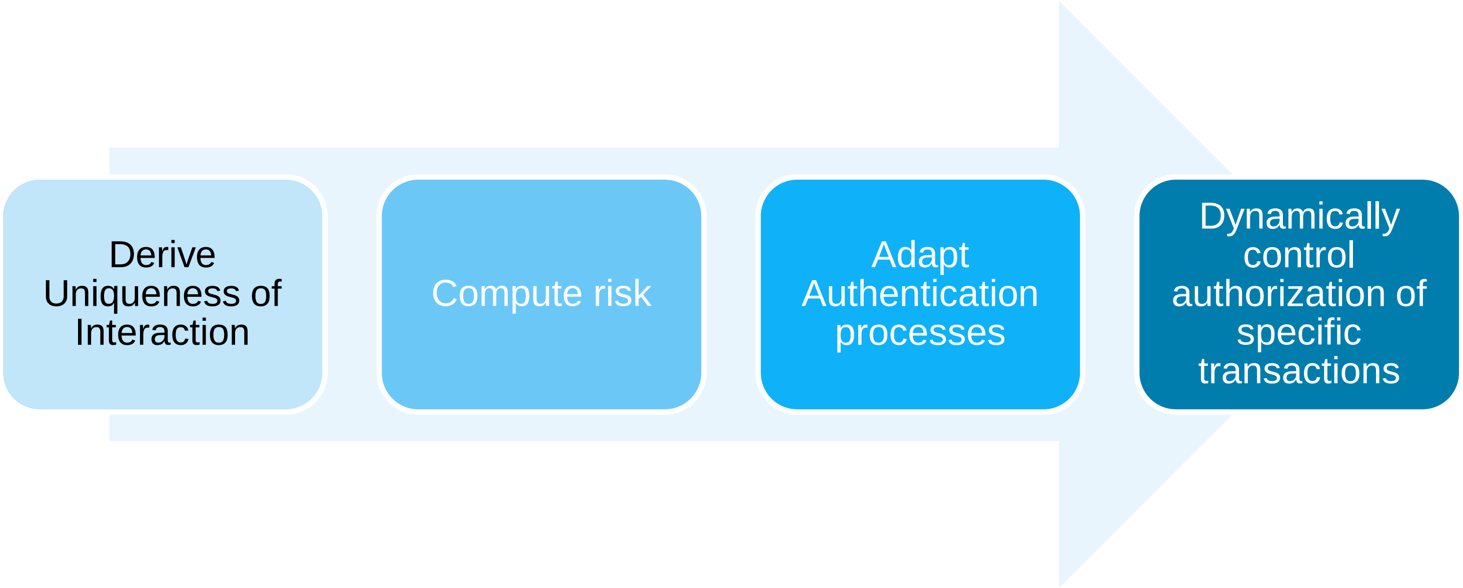
Centralized User Management: Assembling singular view of all the mobile users across one or more mobile apps enables for consistent user governance and reduces redundancy and complexity of access control embedded in each app.

Segmenting Mobile Users: Segmenting mobile users based on access privileges allows for better management through tiered access. This practice assists in anomaly detection.

Enumerating Context Attributes: Selection of the contextual attributes that can influence risk when accessing applications and content will facilitate a granular risk assessment of each user interaction.

Defining Access Policies to Govern Risk: Codification of access policies for applications and content allows for greater consistency and logic testing. Externalizing these policies from applications improves the flexibility of the security posture.

User Context Influences Risk…In Mobile the Context is Dynamic



Derive Uniqueness of Interaction
Compute risk
Adapt Authentication processes
Dynamically control authorization of specific transactions

- Mobile affords many attributes that pertain to the user's context allowing for unique identification of a specific interaction (i.e. location, network, time, device properties etc)
- Risk of the unique interaction can be computed based on established policies
- The risk score can be utilized to select the authentication processes best suited for that interaction
- The risk score can also be employed to control authorization for specific transactions during that interaction and deliver education to the user on security best practices in context

App Security...Securing by Design

Where to begin? Instituting a Safe Mobile App Development Culture

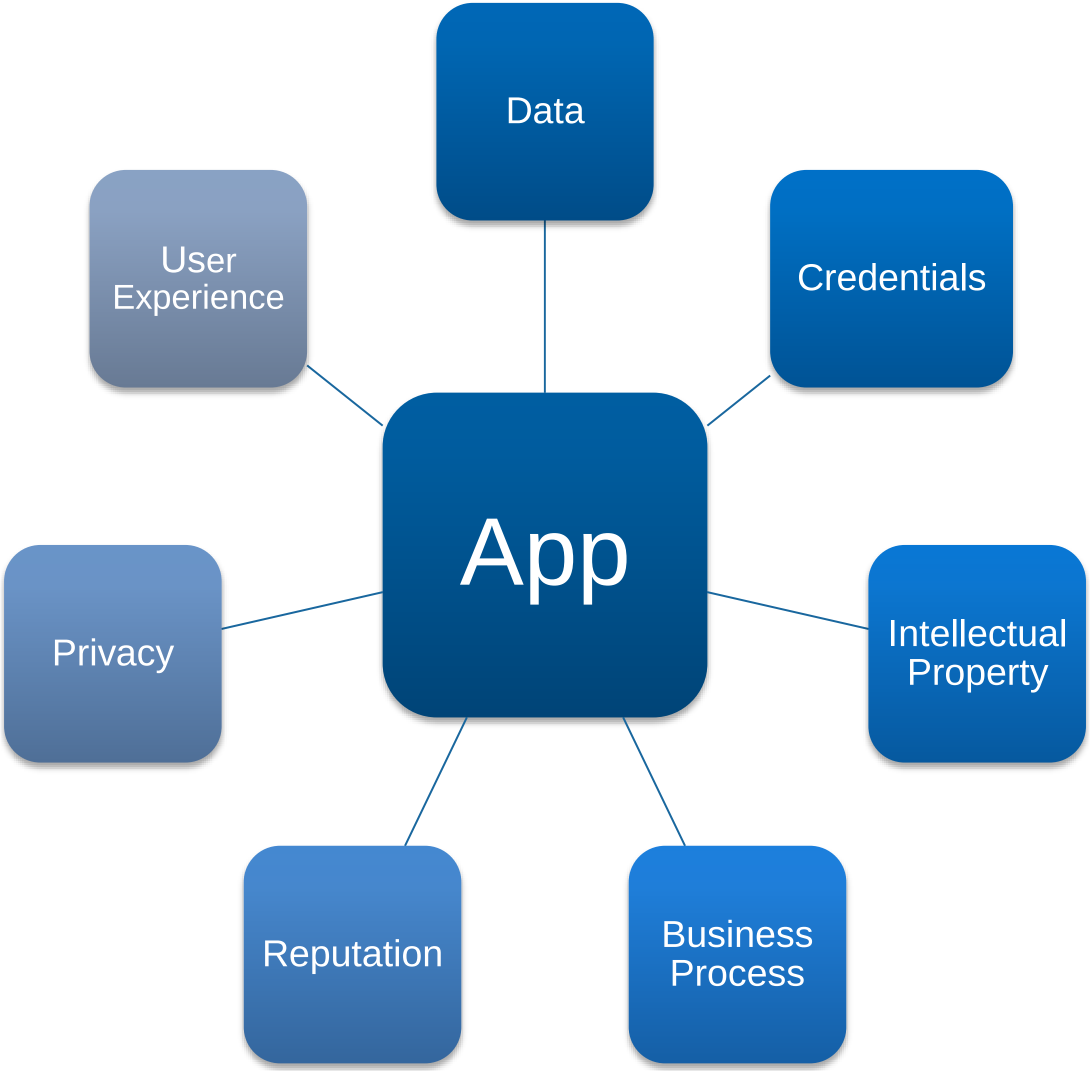
Establish a Security Standard: Mobile app development can be undertaken by different parts of the organization or even outsourced, therefore a security quality standard has to be defined which all development efforts can adhere to.

Segregate Security Logic from Business Logic: Security requirements will have less variation than business logic and requires different set of skills. Security features can be developed and leveraged across multiple apps.

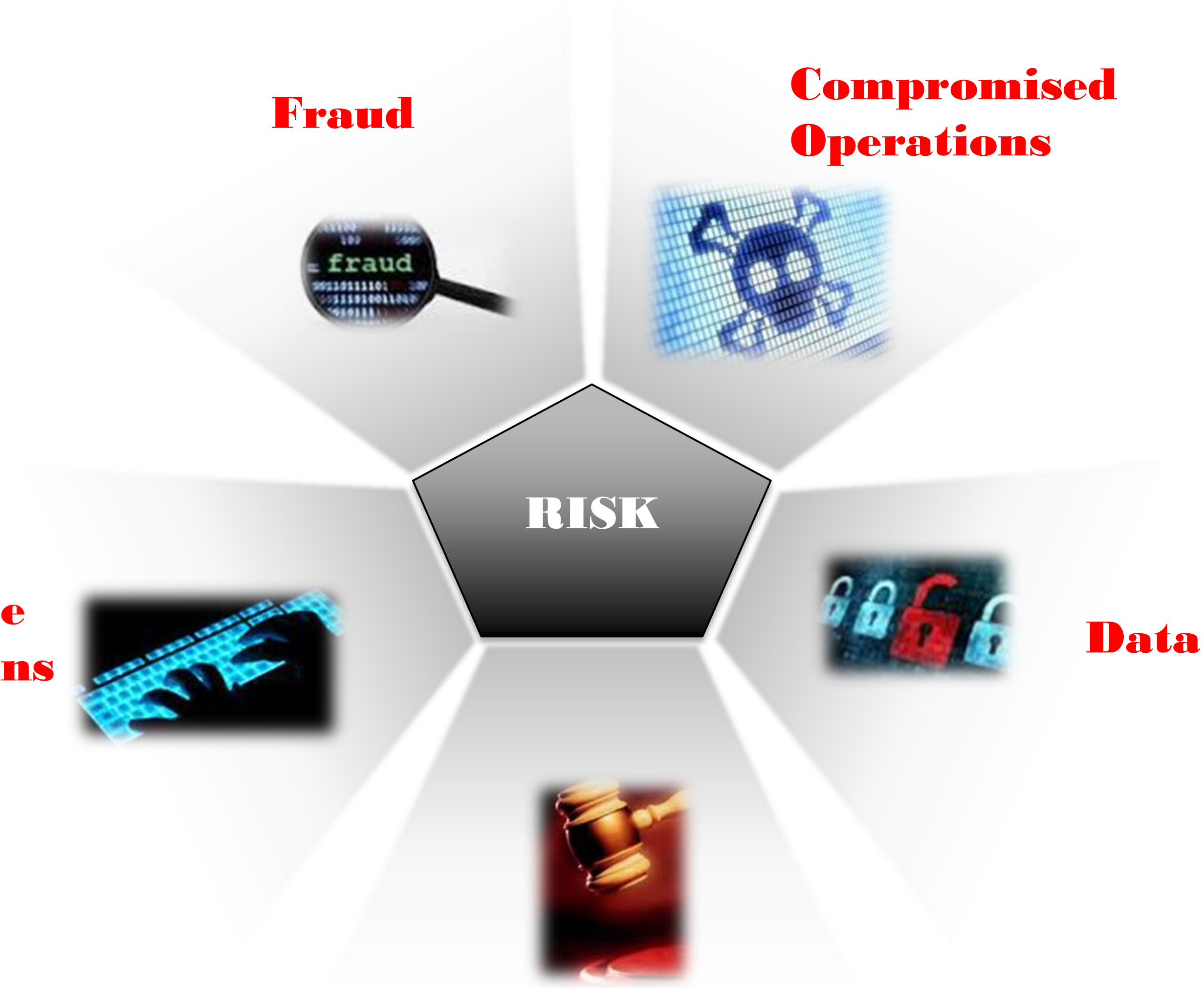
Analyze Security Applications: Mobile apps need to be assessed for their risk exposure – sensitivity of data, usage scenarios etc. This aids in prioritizing and investment of security rigor employed in safeguarding it.

App Management Policies: Active management of applications is required to respond when mobile apps are compromised. This includes defining the update process, conditions when the app will be locked and situations when data stored locally by an app are wiped.

Protect the Integrity of the Mobile App



Key Security Considerations for Safeguarding Mobile Transactions



RISK

Fraud

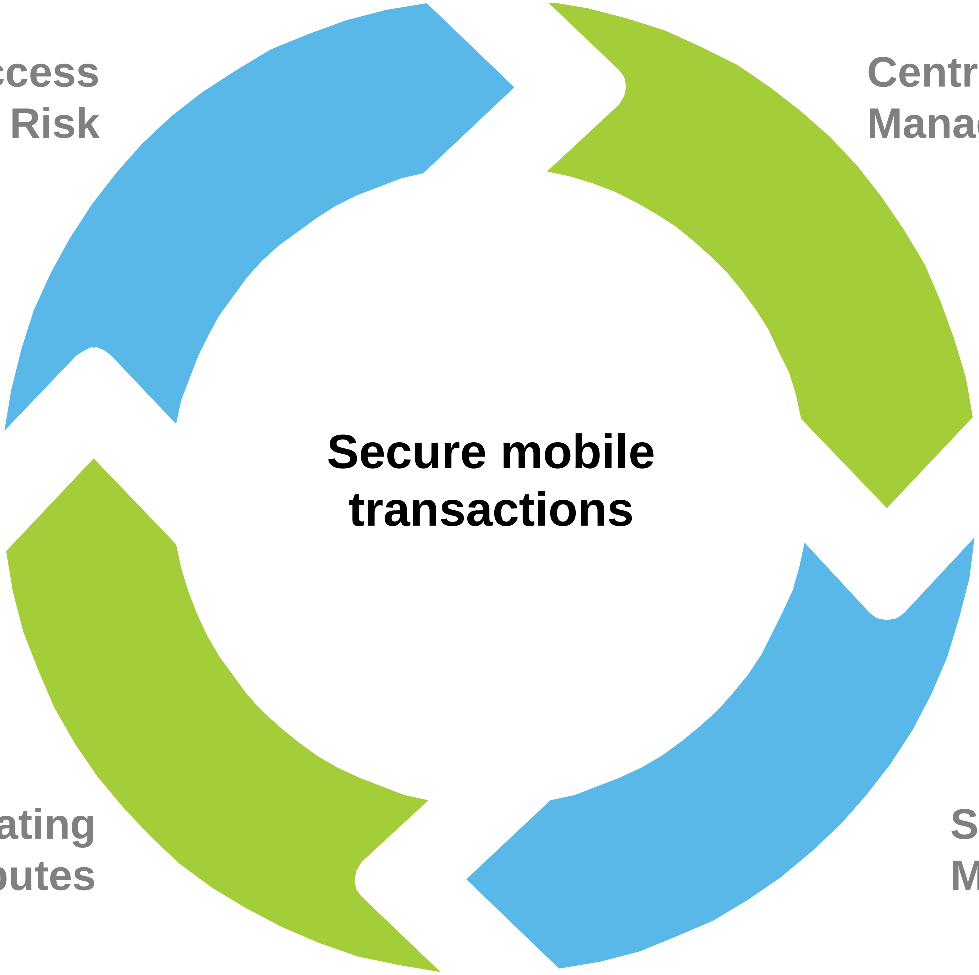
Compromised Operations

Data Loss

Non-Compliance

Illegitimate Transactions

Delivering Trust in Mobile Transactions…



Defining Access Policies to Govern Risk

Centralized User Management

Secure mobile transactions

Segmenting Mobile Users

Enumerating Context Attributes

Thank You!