Security Intelligence.
Think Integrated.

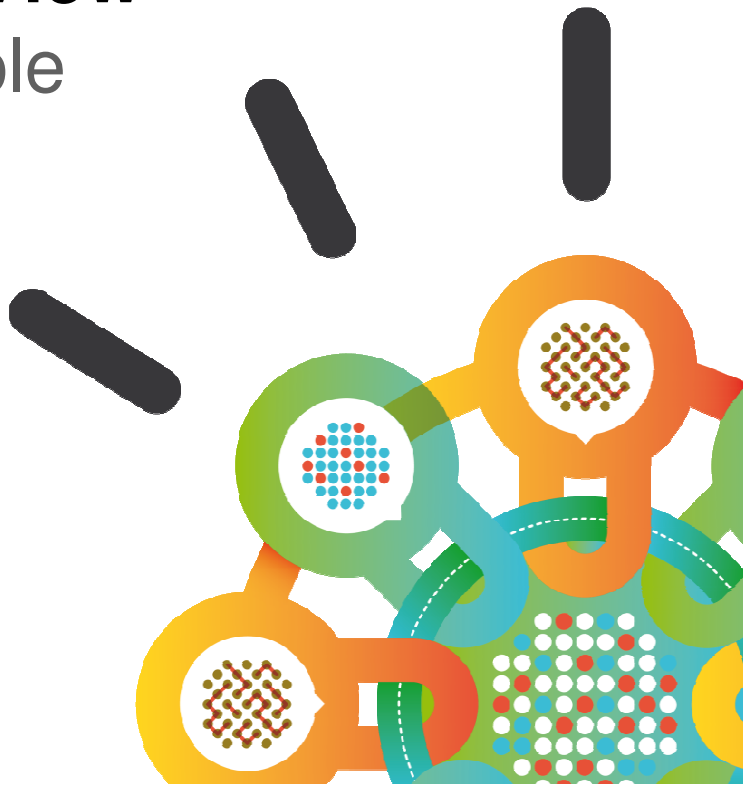
IBM Banking Security Point of View

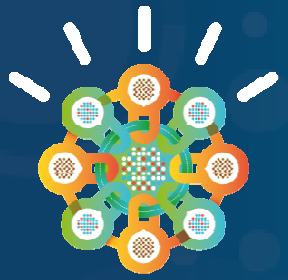
Nepal Banking Security Roundtable

Analysis, Recommendations and Roadmap

Mar 2014

Krishnan Jagannathan
krishnan@sg.ibm.com
+65 90107275
Business Security Advisor.





What we observed

Banks typical designated additional focus areas

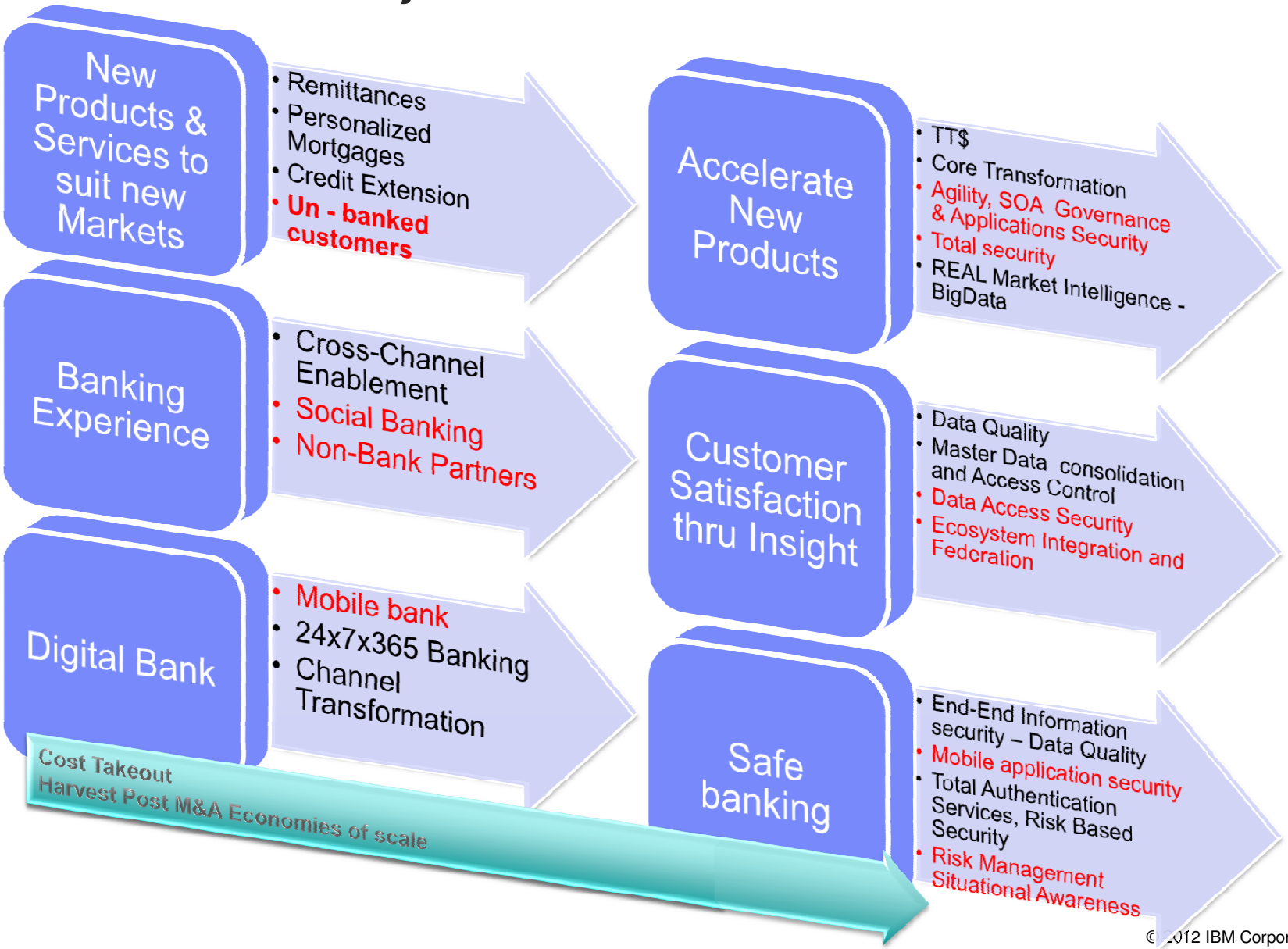
Summary of Banks's Score on Global Banking Imperatives

Objectives	Priority	Gap	Value	Score
Accelerate New Product Innovation and Development	10	5	10	25
Improve Customer Insight	10	3.5	8.1	21.6
Improve New Customer Acquisition	8.7	3.4	7.7	19.9
Gain a Complete View of Customer Relationship	8.7	4.5	8.3	21.6
Improve Customer Retention	9.1	6.4	7.3	22.8
Improve Core System Information Management	8.8	5.4	9.3	23.4
Cost Take Out From Process Optimization	8.9	5.3	7.8	21.9
Manage Information Over Its Lifecycle	8.2	6.4	7.8	22.4
Paper Elimination & Process Improvement	7.4	5	6.7	19.1
Optimize Customer Facing Lending Processes	7.8	5.4	8.2	21.4
Mitigate Theft & Fraudulent Activity	9.1	5.1	6.6	20.9
Improve Credit Risk Assessment & Decisioning	7.7	3.1	6.1	16.9
Improve Liquidity Monitoring, Assessment & Reporting	8.3	5.7	6.6	20.6
Improved Financial Transparency & Reporting	7.5	5.4	6.5	19.4
Improve Data Quality & Security	8.5	5.6	8.5	22.5

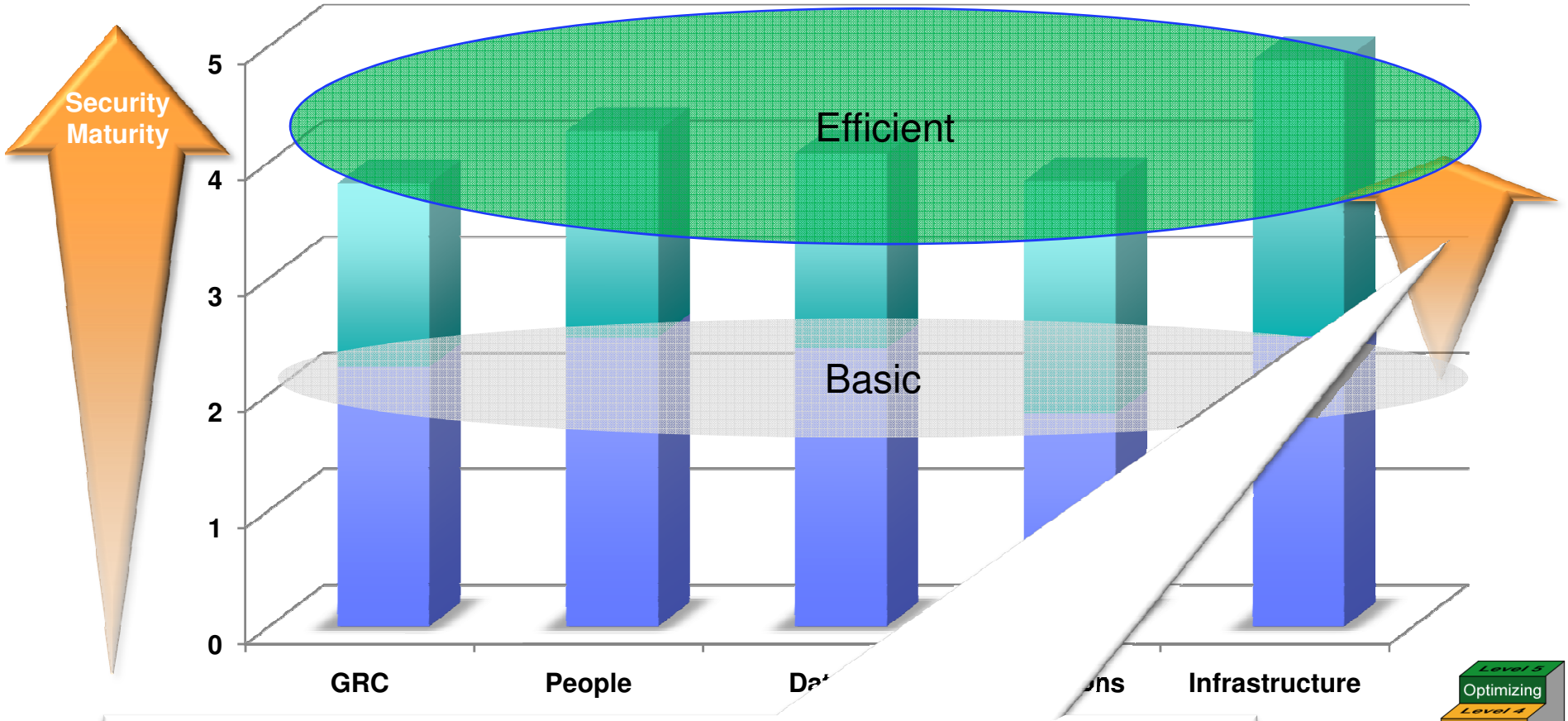
Score => 22 → Red; 21.5<= Score <=21.9 → Blue

Outcome of the Business Security Workshop

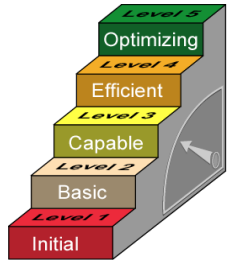
How Banks Business Objectives Translate . . .



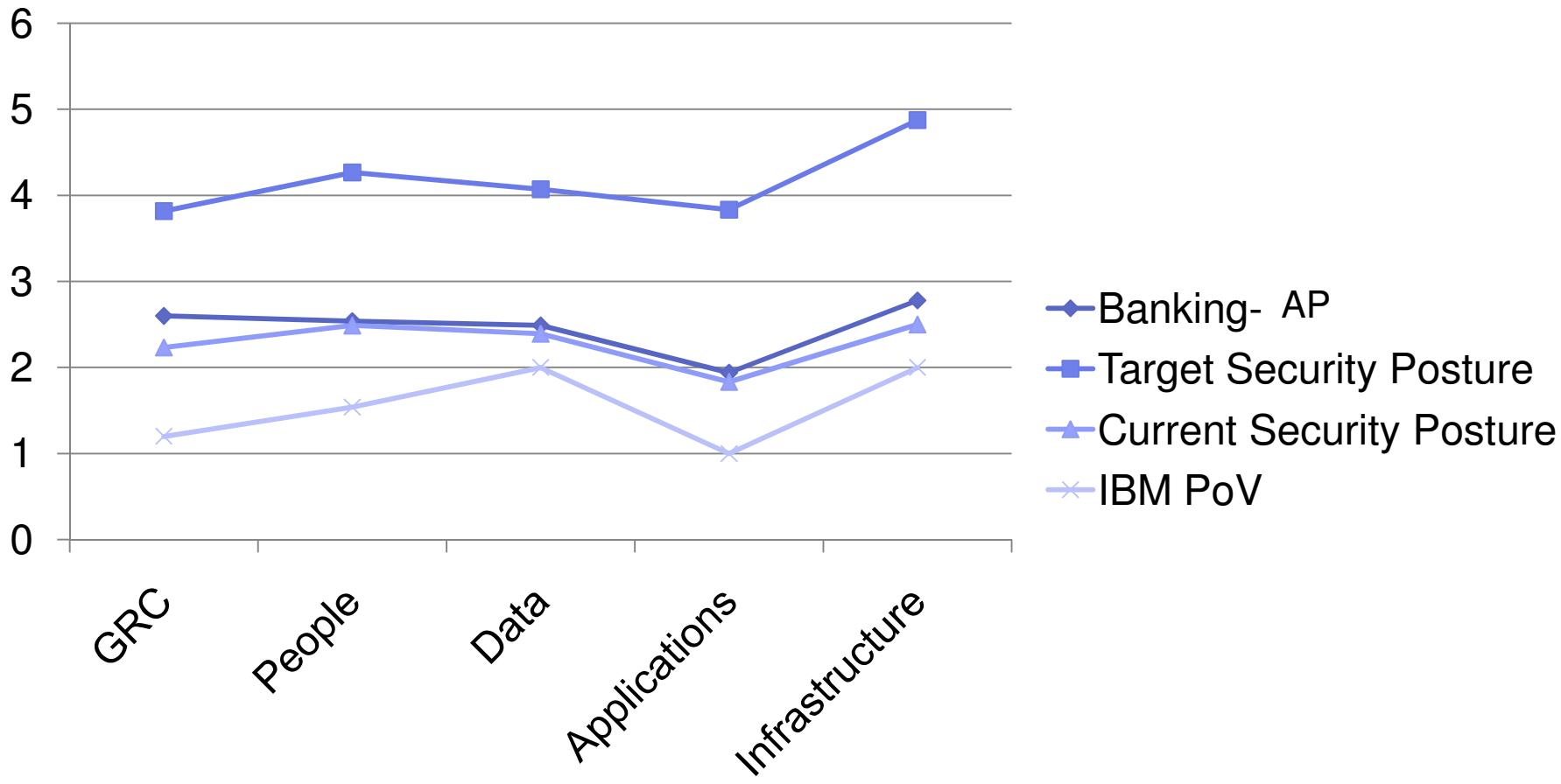
Overall improvement of Banks Security maturity from basic to efficient

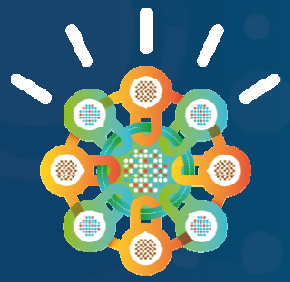


Bridging this gap is not only an aspiration, but an industry imperative with Banks straddling both advanced economies and emergent economies – advanced security postures deployed to meet compliance measures in advanced economies could be tuned and scaled to meet the requirements of emergent economies. As a consequence, it is hoped that this journey will receive the management commitment and investment over the 3 year horizon for timely execution.



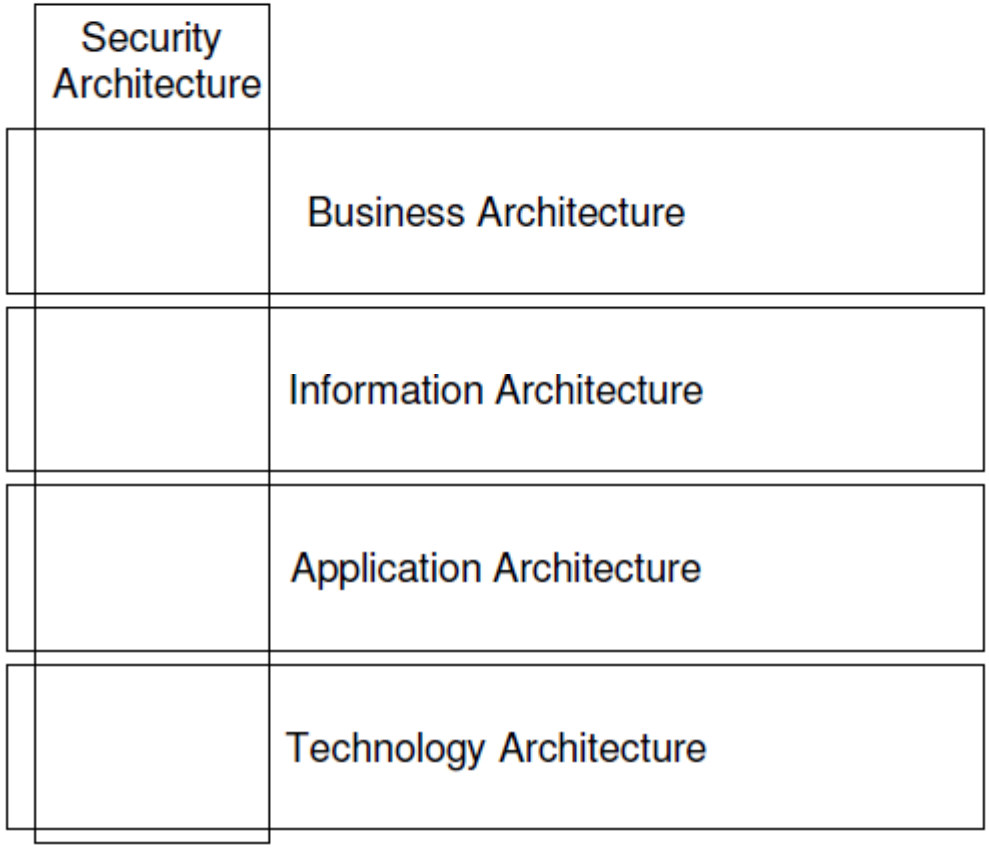
IBMs Assessment



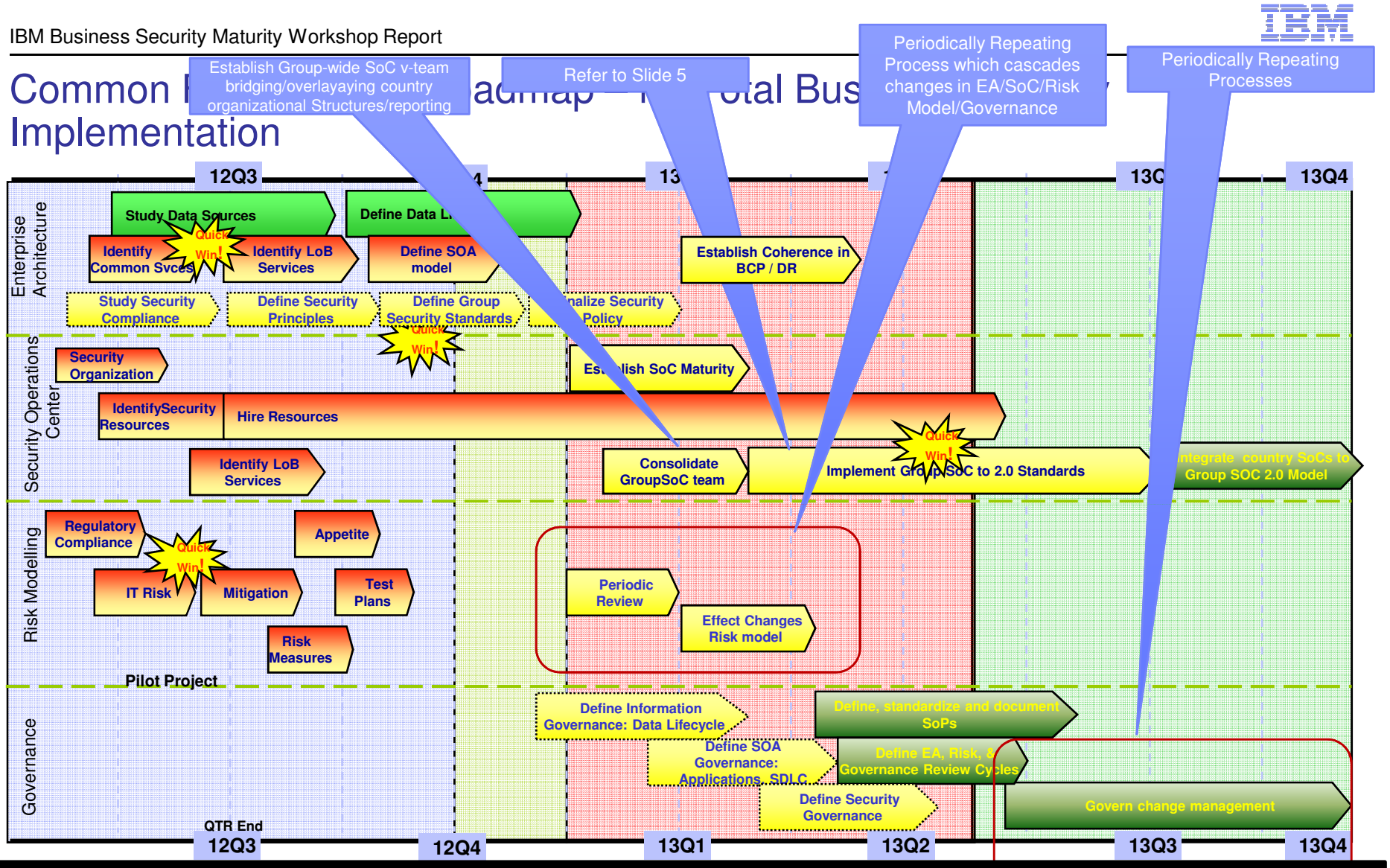


Recommendations – EA & Process

Enterprise Architecture – IBMs PoV

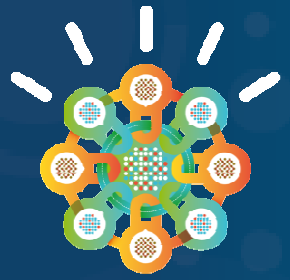


Common I… adMap – …otal Bus… Implementation



This is a recommended sound foundation – it is recognized however that the Banking Group and its Country businesses will already have commenced work in some areas or even reached a state of maturity – however, IBM underscores a Group Standard across all these areas and a sense of *shared responsibility in teams across the group* – achieved through execution of the activities on the slide.

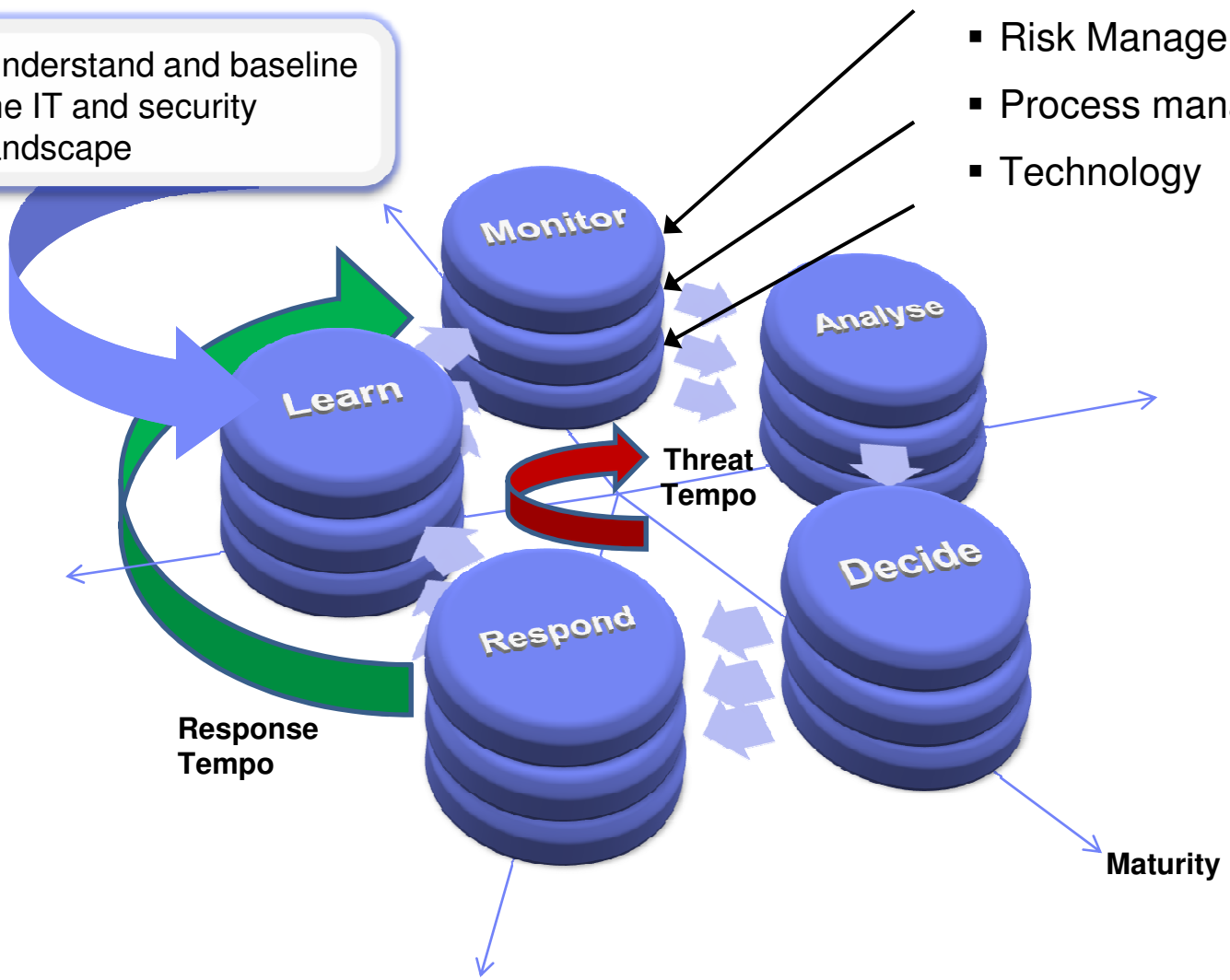
The Security Framework Implementation – in the succeeding slides has to happen concurrently and even preceding the achievement of a maturity state in individual areas on this slide – as they are the **pre-requisite building blocks for security execution**



Recommendations – Process, People

IBMs approach to Counter Cyber Defence and Cyber Fraud

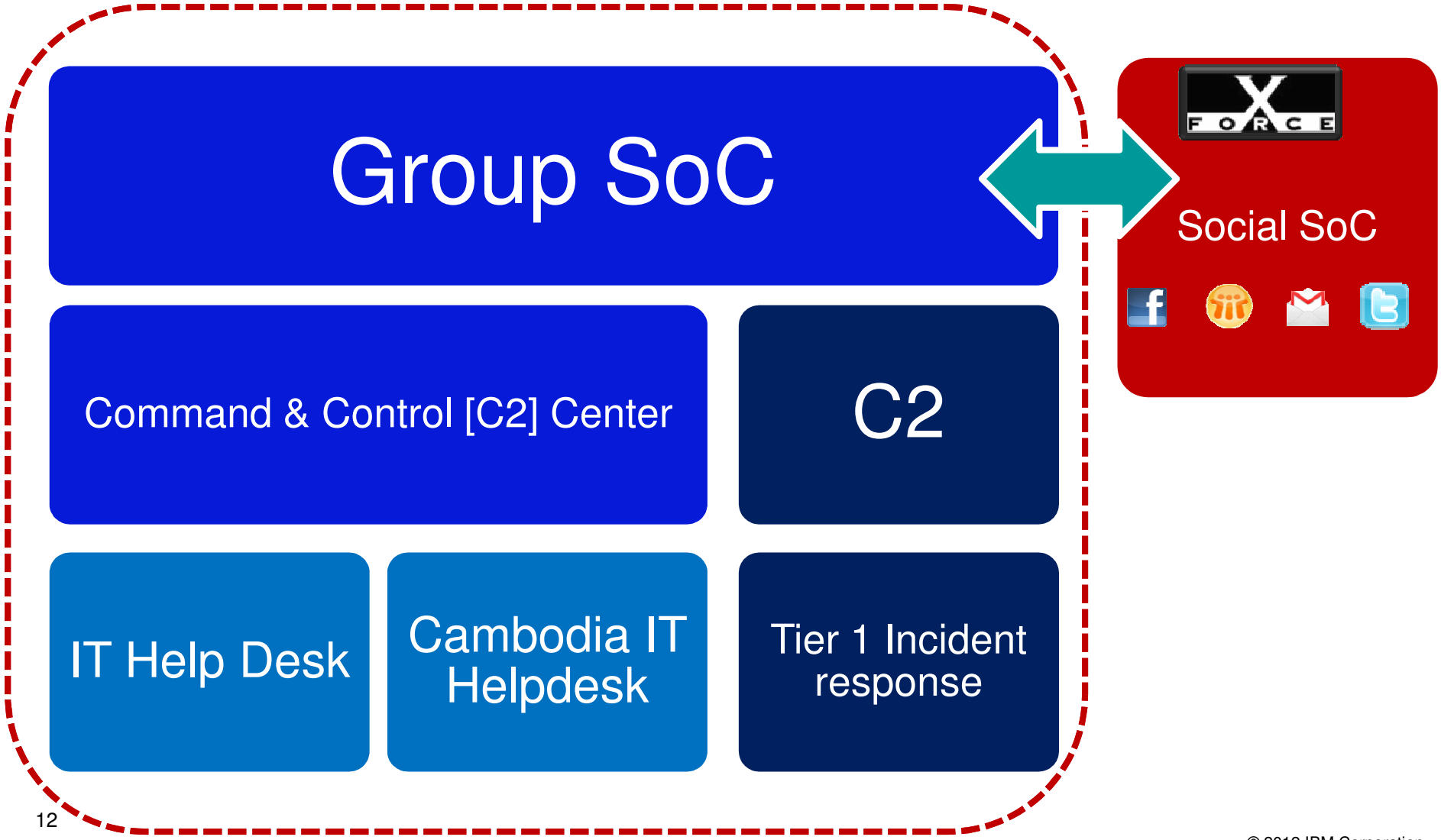
- Understand and baseline the IT and security landscape

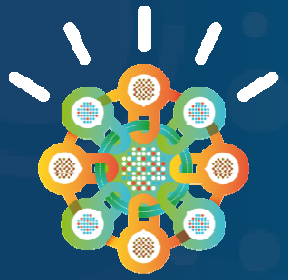


Layers

- Risk Management
- Process management
- Technology

Recommendation - SoC 2.0 Model

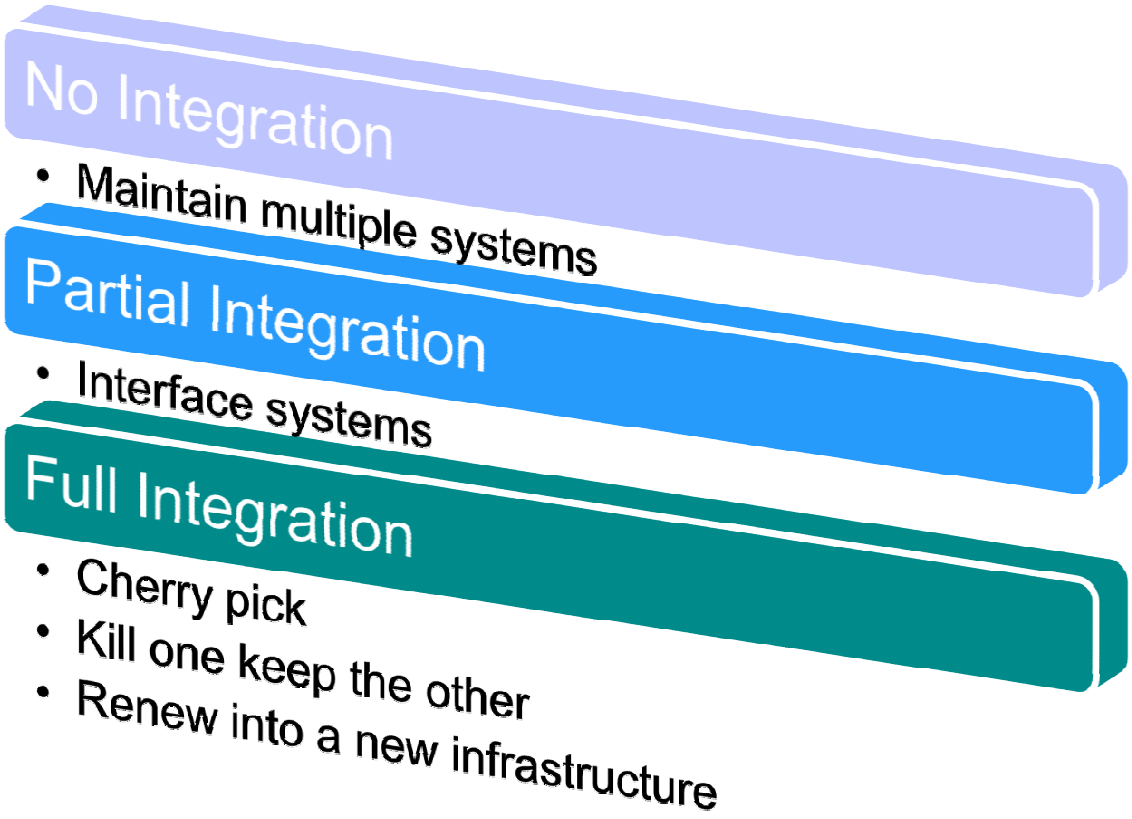




Post Merger Integration

Business Security Integration

The options

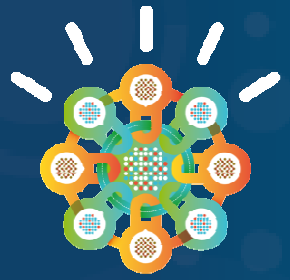


Key to success in a Multinational context

synergize fast

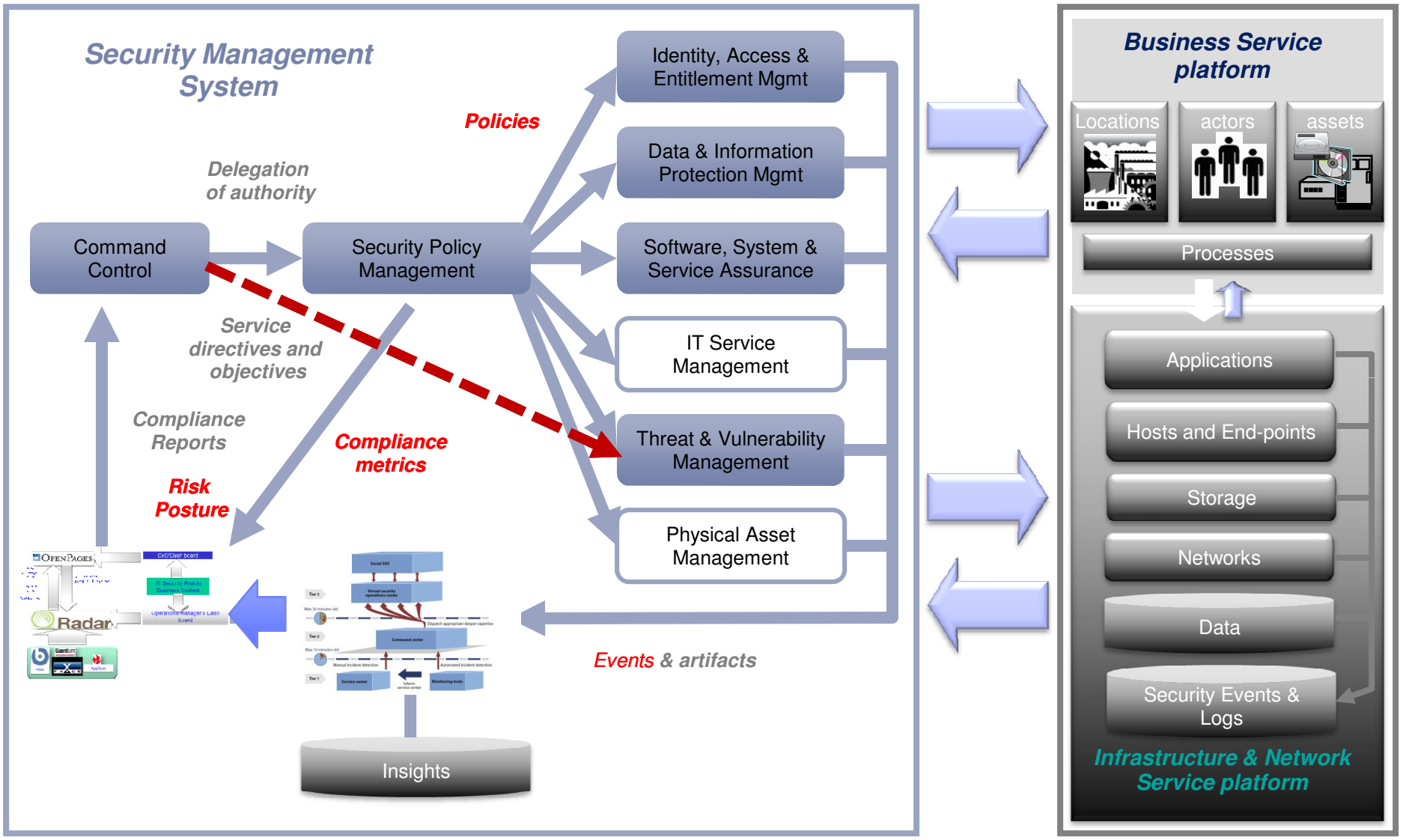
- Multi-national banks need to standardize on business security while supporting regional requirements and processes.
- Regulatory requirements in every Geography in the region define how the processes and the supporting architecture are disposed.
- That said, the success of Security Integration is through establishing a common standard of security controls and
- maintaining multiple degrees of depth in implementation decreed by local regulatory injunctions.
- The bank may look to raise the security posture across the group to a common implemented model far exceeding regulatory expectations – but that is a business call.

This calls for a security approach which enforces a Group standard - while Integrating existing local operations



The recommended target security model

IBM Security Model



GRC Recommendations

Predictive Risk Control = Situational Awareness + Operationalization

Predictive Risk Control = SoC + Connected Security Architecture

- Enterprise Architecture assessment which is underway at Banks. This activity has management attention, which is laudable. However we recommend that the activity extends its scope specifically to address Data Architecture & Enterprise Security Architecture (ESA) as well.

- **Banks have a professed goal of real-time risk management and are focussing security efforts to deter APTs and cyber attack vectors while strengthening fraud detection through security analytics. IBM recommend Banks prioritize the following:**
  - **Invest in a centralized SOC model as described in slide 13.**
  - **Put in place a distributed Security Console that could be shared by SOCs across the group.**
  - **Put in place a GRC dashboard that reflects risk posture**
  - **Automate compliance by Linking the Security Intelligence and IT GRC platforms.**
  - **Develop a correlation engine between security intelligence and other information to develop all points insight.**

- Enterprise Security Principles deriving from the ESA need to be standardized across group. Some Country Security Specific controls will vary based on regulatory requirements – but the bank will benefit through a coherent set of controls:
  - Perform an assessment of the current security policies and their effectiveness. In order to understand the following
    - How are the policies enforced
    - How is compliance of the policies measured
    - How is non-compliance (remediation) managed and acted upon

- **ESA forms the bedrock of secure ubiquitous (mobile) banking . Mobile banking is predicated on secure core systems as well as their client footprints on edge devices . Security cannnot be a bolt-on strategy once the mobile clients are deployed.**

- The development of a policy driven ESA to realize an effective security program management
  - This will develop the standards that apply to the adoption of security controls across Banks and validate the business / security policies driving their adoption

Enterprise Architecture = Business Process Model + **Security Architecture** + Data Architecture + Technology Standards

- Focus on technical standards for asset management, compliance, vulnerability management, event and incident management for enterprise wide endorsement and adoption in Banks .

- As security needs an all party buy-in we recommend Banks build a risk aware culture within Banks business and develop further security awareness across the Banks organization (education).

Identity and Access Management Recommendation

- Asses the current identity and provisioning tools in the environment
  - Understand the applications and systems in scope
  - Value of integration and effectiveness of the identity lifecycle management
- Implement an IAM platform for privileged and shared user control
  - Get control on their usage (e.g. through check-in/check-out -- shared discretionary access credentials)
  - Obtain traceability and accountability
  - Monitor privileged and shared user account activity and baseline patterns of usage for anomaly detection

Coherent Access = Risk based Authentication + Federation + Privilege control + Repository agnostic

- Standardize the IAM model
  - Select a new candidate IAM platform that possesses:
    - Expanded risk management capability
    - Extensibility to cover WebSSO, Enterprise SSO, Risk Based Access Management
    - Federated Identity management
    - Privileged Identity Management
    - Integrates with existing identity repositories

- Perform an audit to identify the functional accounts (non person entities) in existence in the environment.
  - Review current policies for lifecycle management of functional accounts and improve the policies where needed to assure the lifecycle is fully managed & abnormal usage is not possible.

Data and Information Security Recommendations

- Identify and document where sensitive data lies in Banks and ensure it has appropriate security controls to protect it.
- Develop policies & enforce controls for information classification within the business.
- Ensure assets have been classified based upon Banks information policy framework and that this is centrally tracked in the asset profile registry.
- Identify where production data exists in non-production environments.
  - Develop a plan to remove / redact this data from non-production environments
  - Ensure there are clear 3rd party vendor guidelines around the handling of information assets in the organization.

Data Security = Critical Data Inventory + Distributed DAM + SoE

- It is recommended that Banks make investments in implementing:
  - A coherent privileged Data Access control mechanism across the group to protect sensitive user data as well as sensitive business information.
  - Build in Security into the existing Business Continuity Plans.
    - Conduct security audits to establish the state of security controls as far as business continuance concerned.
  - Ensure SoEs are put in place for hardening Systems & Database instances being newly commissioned.

Application Security Management Recommendations

EAS →Application Inventory →DAST → vulnerabilities → IPS >> Security Intel

- Incorporate security into the SDLC lifecycle process.
  - Build security awareness in the developers
  - Build successful security audit as a condition of acceptance of code
  - Build a security developer practice and library of secure coding practices and models.
- Provide enterprise wide SLDC security testing methodology and tools to identify application vulnerabilities
  - Perform regular application security scanning (pen-testing) to identify risks
  - Identify key application vulnerability risks and start remediation project

- **Rapidly invest and implement tooling to cover :**
  - **Static code testing**
  - **Dynamic/Web applications code testing**
- **Implement Test Data Management through process and tooling**
- **Ensure the Application security tool is able to inform secure application gateways and the IPS of application vulnerabilities – this is a key dimension to safeguard a bullet-proof virtually patched security model**

Infrastructure Recommendations

- Implement Next Generation IPS technology for threat detection at the network layer to protect Banks
  - Extend this to all networks
  - In case varying IPS technology pieces are in place – define an integration or retirement/refresh plan.
  - Ensure the IPS is capable of Anomaly detection, superior attack prevention through Virtual patching, fine grained control of traffic such as:
    - Allow Web2.0 [Youtube, facebook traffic] only to specific destinations in the organization
    - Is able to integrate with the Advanced SIEM platform at the Group SoC.
- Ensure consistency of remote access policy across Banks business units.
- Be able to enforce Security controls on all devices connecting to the Bank network [nomadic devices] especially those that are owned by employees.
  - and secure bank information by being wiped off on loss of device.
  - Extend the control footprint onto mobile applications to execute in a secure sandbox on customer device.
- Complete the Patch Management project to cover operating systems and applications.
- Implement Security Information and Event Management (SIEM) to provide insight into the effectiveness of the security control implementation across Banks
  - Provide visibility into threat landscape
  - Provide centralized repository of log data
  - Provide single dashboard for view of assets and log collection
  - Support the foundation of a SOC
    - Enable better IT Security risk identification and management, thus improving the organizations IT Risk posture
    - Link incidents across the business and understand if they are related.
    - Provide situational awareness for Banks .
- Consolidate the existing and fragmented CMDB's into a centralized CMDB service for Banks .

•Operationalize Security – Implement Next Generation IPS with Vulnerability Management and SIEM integration.
•Implement Endpoint Management

Key takeaways

- From the business prioritization activity, we are glad to note that the key corporate business goals are borne out. Those being:
  - Accelerating new services to market – **Mobile delivery and therefore mobile security being key thrust #1.** The roadmaps prepare the Information Systems stack to deliver mobile apps in a secure manner.
    - Some of these services need to be delivered as part of Social Banking with new kinds of fee-based services like remittance and also micro-finance. This requires re-thinking processes and getting banking closer to the rural or under-banked client demography over both smart phones , conventional phones and other devices.
    - The Web 2.0 model of Banking is the happening new channel. Again, it calls for embracing this pervasive channel for feedback and providing banking services. Most of the activity here happens on mobile devices – underscoring mobile as an imperative.
  - Total banking security being a non-negotiable goal – which translates to a whole set of system and dependent goals embodied in the 3 roadmaps specifically detailed out.
  - Delivering operational excellence and evolving a model to deliver a sum which is greater than the parts – this is best delivered through the Distributed Security Operations model which we have described in the Advise note (delivered separately earlier – the 1-slide #13 describes this model).
  - Real-time Risk Management and Fraud Detection – This is delivered through collecting all internal information the bank possesses – security intelligence, events, KYC, unstructured info etc into a BigData repository and using the resulting correlation model generate insights which potentially pick up patterns such as fraud history and particular demographies with higher propensity, certain internal attack and how this connects to events in the public domain. This helps getting ahead of the attacker. This has been described in the BigData correlation Advise we have provided separately.
  - New IS models such as cloud are being tried out in the banking domain . This is still in a nascent stage with private cloud deployments around common services and also in extending core systems. Vitualization security is at the core to make cloud – based delivery secure. IBM being at the very leading edge of cloud security could provide the cloud security framework to support this – should the bank decide to embrace this model.

- In sum, the happy outcome of the workshop has been in defining steps to ready the bank to achieve success in its trans-regional operations – attaining the goal of becoming a **strong regional universal** bank while:
  - **Simplifying operations** and delivering **maximum operational excellence in post M&A integration** phase**.**

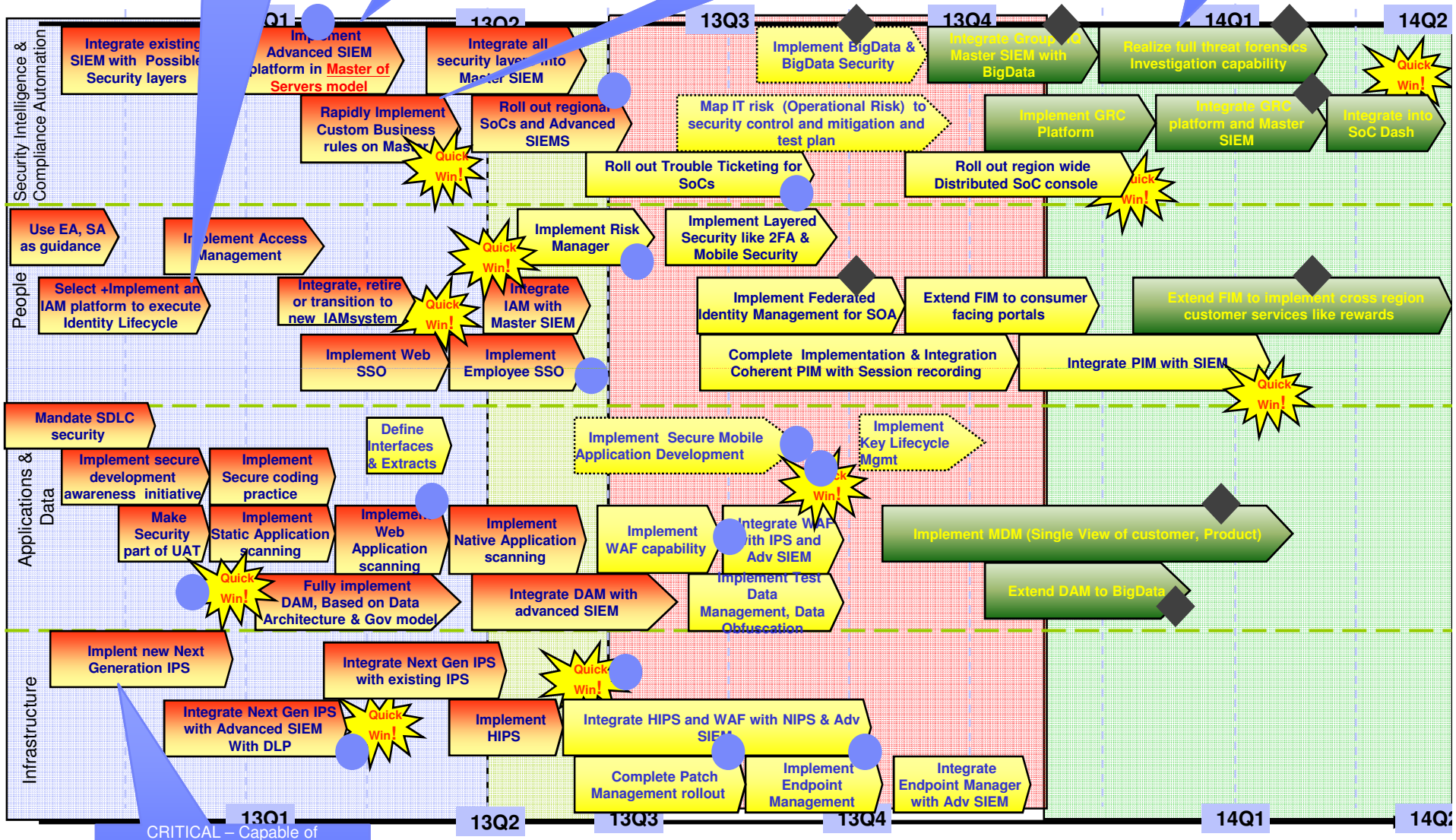
CRITICAL –Capable of supporting SSO for employees and customer: Federation, RBAC, Risk Management,

CRITICAL – a very rapidly deployable platform with minimum services involvement and with RM features integrating automated Vulnerability mapping

CRITICAL – Business rules corresponding to most threat vectors/indicators should be available out-of-the-box as well as compliance reports. Other rules shd be easily customizable.

CRITICAL – Essential for Social SoC –security KM, advanced threat sense-making and Fraud prediction as well as APT defense

Suggeste[d] [r]oadm[a]p for operations i[n] Advanced Econo[mies]



Next Steps

- Imperative Enterprise Architecture Actions
  - Establish Data Architecture as a key work-stream
  - Establish Security Architecture as a key work-stream
  - Establish Business Modeling as a fundamental step of the Enterprise Architecture exercise.
- Imperative Risk Modeling and Governance Actions
  - Establish the OR IT Security Risk Model
  - Define a Governance model, Enterprise Security Principles, and Security Policy
  - Ensure the Security Technology supports security policy

- Imperative Security Organization Actions
  - Harvest and consolidate security organization – cross group
  - Identify cross business security components and take ownership [based on Security Architecture]
  - Establish a Security Operations Center 2.0 model cross group [separate from IT Operations Center]
  - Define coherent SoPs and Response teams
- Imperative Security projects to achieve base operational security posture
  - Real – time Situational Awareness and Actionability
  - Vulnerability Intelligence
  - Risk Management at each security layer
  - Dynamic Security and Virtual Patching
- Imperative Security Projects to achieve future state and support key business imperatives
  - Advanced Correlation for fraud detection
  - BigData correlation
  - Compliance automation
  - Social Banking
  - Branch rationalization

ibm.com/security