RSA CONFERENCE
ASIA PACIFIC 2013

HOW TO MAKE SECURITY EVERYONES RESPONSIBILITY IN THE MODERN ENTERPRISE

Security in knowledge

Dave Martin
EMC Corporation

Session ID: CLD-W04

Session Classification: General Interest

Agenda

- Understanding the current state
- A new strategy
- Foundational components
- Leverage that foundation
- Govern the environment
- Thinking of a better future

Current state - how did we get here?

From a few to many

The new threats facing enterprises, coupled with business agility, cost pressure and initiatives like cloud and ITaaS predicates a new strategy. Traditionally we relied on a small group of skilled, motivated & passionate individuals to protect the organization, but in this new environment security teams must mobilize and empower the entire enterprise to collectively manage risk

Understanding the cultural gap

Culture of Enablement

Availability
Reliability
Features
Ease of use
Freedom
Choice
Innovation
Reward
Myopic
Entitlement

Service Mindset

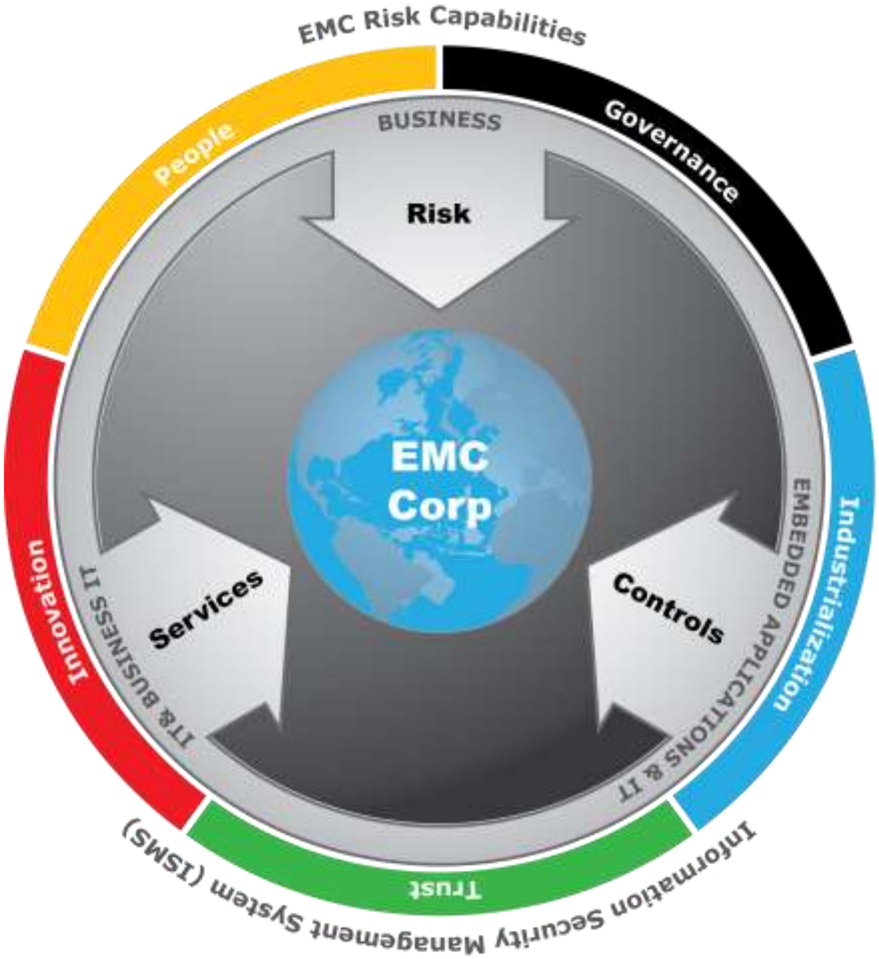
a matter of context

Culture of Protection

Safety
Confidentiality
Loopholes
Missing safeguards
Guidelines
Options
Conforming
Risk
Hyperopic
Privilege

Defensive Mindset

A new strategic approach



Governance			
Standards	Compliance	Policy	Risk
Industrialization			
Rationalize	Security as a Service	Scale	
Trust			
Measure	Controls Assurance	Accountability	
Innovation			
Communication	Technology	Strategy	
People			
Inform	Develop	Partner	Empower

Defining a solid foundation

Back to basics

- Operating principles
  - Define and agree how security work including remediation activities will be prioritized with resource and funding
- Define and support the operating environment
  - Cooperative policy development
  - Controls matrix
  - Architecture standards
  - Control delivery services

Tenets of security governance

The goal of the security governance organization is to provide consistent direction, policies, standards and oversight over security at EMC.

♫ Congruity

Harmonization thinking with the business

- Alignment encourages to conflicting priorities
- Connect security goals to business objectives

⏰ Consistency

Deliver clear and coherent guidelines

- Clear direction results in predictable outcomes
- Measure success with aligned metrics
- Set predictable expectations

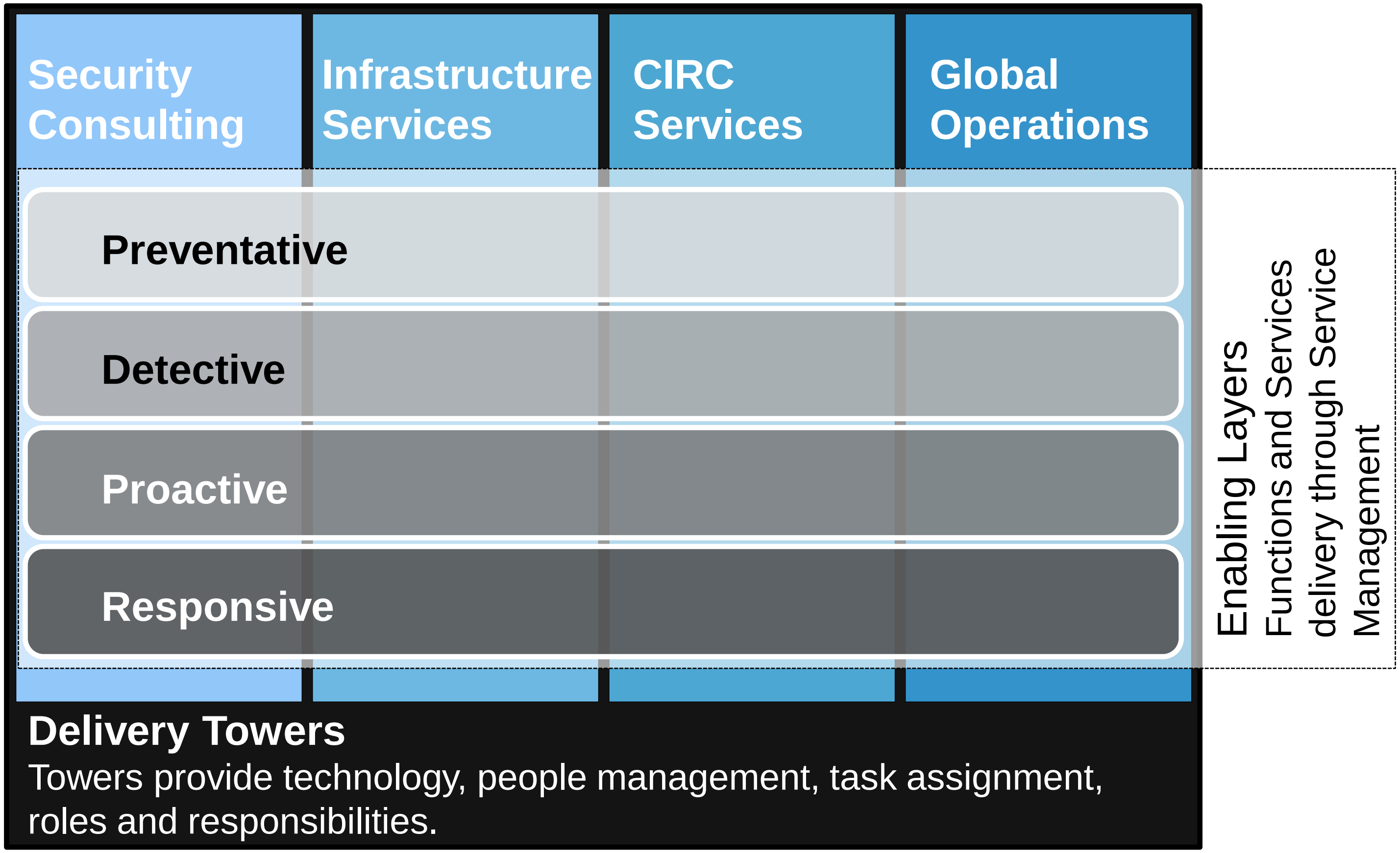
Necessity

Explain why people must do things

- "Because I told you so" doesn't work
- Create buy in to controls
- Justify any infringement on user freedom

Service delivery

Across each security service, resources from different delivery groups are applied by the service manager. Resource requests are based on customer QOS and functional needs.


Security Consulting
Infrastructure Services
CIRC Services
Global Operations
Preventative
Detective
Proactive
Responsive
Enabling Layers
Functions and Services delivery through Service Management
Delivery Towers
Towers provide technology, people management, task assignment, roles and responsibilities.

Leveraging that foundation

Driving change

- Delegate security functions
  - Commoditize security controls
  - Identify control owners, security champions in IT and business functions
- Measure and report

  Ensure architecture compliance, control delivery, control effectiveness, cost of control are measured and managed
- Accountability

  Use goals, rewards and competitive reporting to ensure visibility and ownership at all layers of the teams focus on leadership, control owners and security champions

Commoditize controls

Service enablement of security services will follow a flow of four distinct tasks, focusing on first establishing foundational documentation, qualifying the process, executing or service enabling and providing the service to the market.

Documentation

Document

What is the service?
How to manage it?
Who consumes it?
Who delivers it today?
What skills are necessary?
What should the QOS be?

Build Foundation

Identify controls assurance hooks
Determine Governance communications model

Qualification

Determine

Who should own it
Criticality of the control

Educate

Develop training
Shadowing Services

Authorize

Establish executive support and commitment

Plan

Establish plan for delivery of services

Execution

Train

Teach resources to operate the systems

Transition

Transfer responsibility for assets to appropriate owners.

Monitor

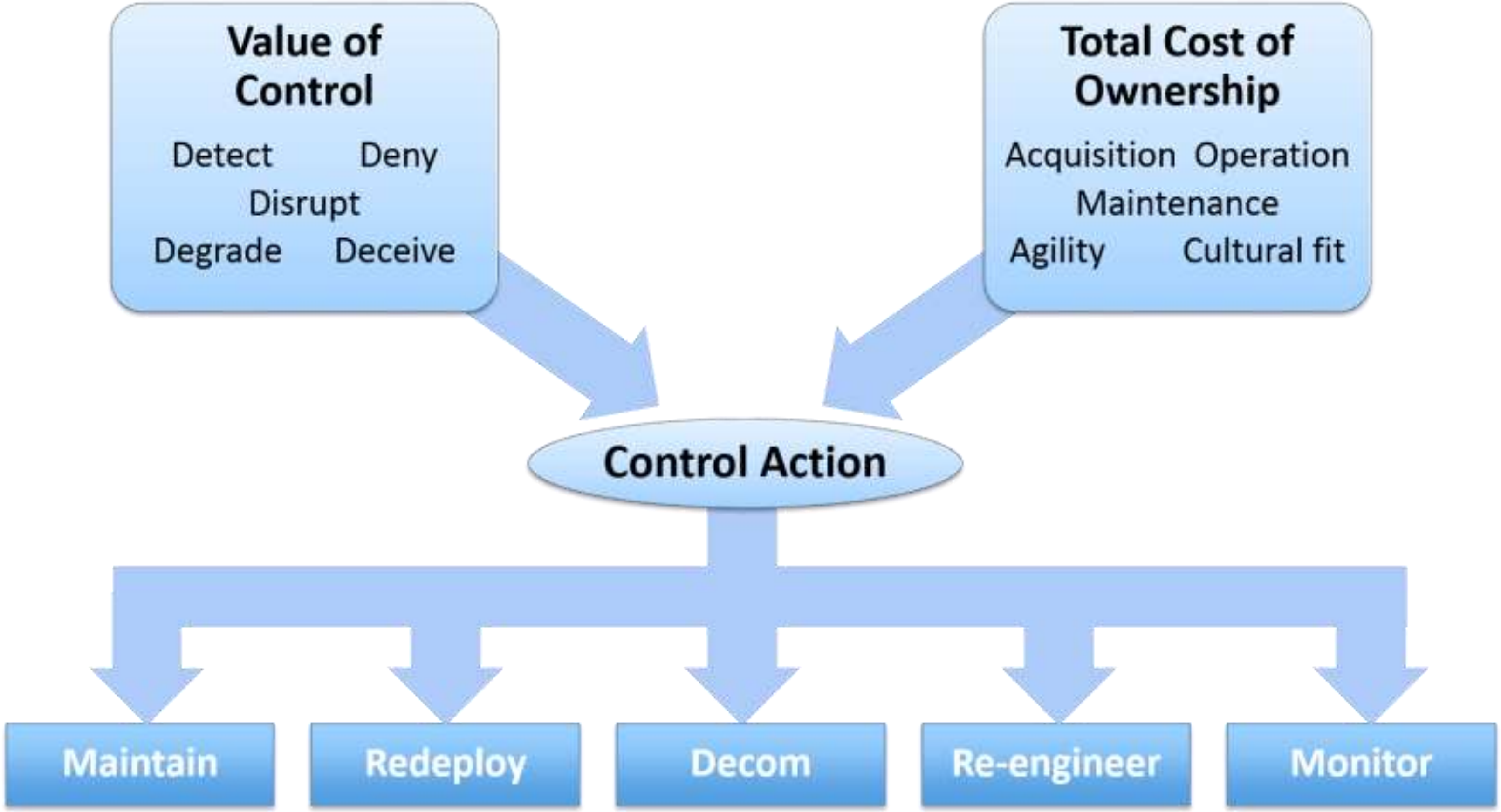
Provide monitoring and guidance to solution implementation

Commitment

Maintain

Service Acceptance
Controls Assurance

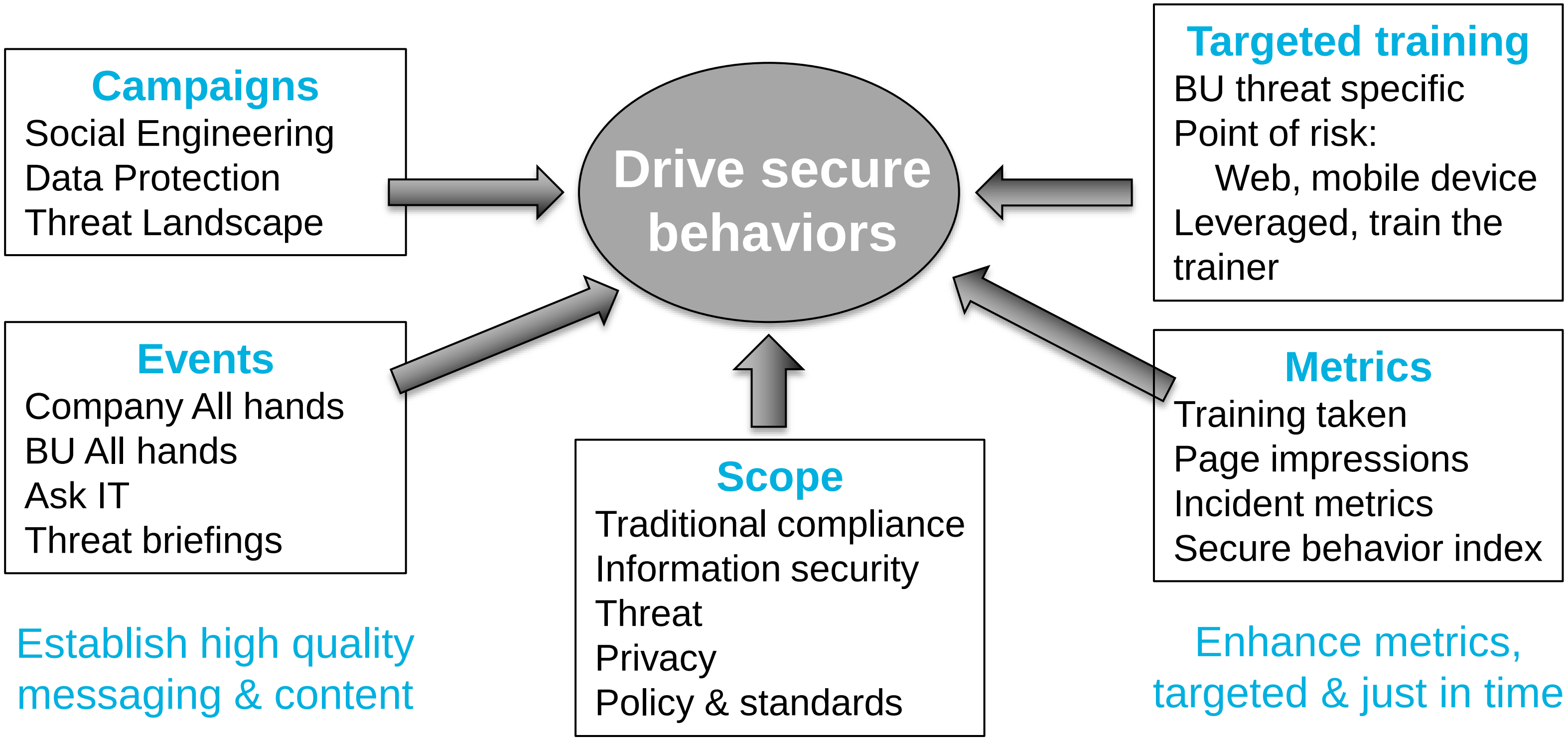
The value of controls vs. TCO



Manage the control portfolio via a constant review of control effectiveness vs. operational cost. Driving decisions of effective use of resources, under performing controls may be moved, managed at a lower cost or scheduled for decommission and/or replacement.

Spreading the word

End user awareness is not enough, drive a multi-faceted dynamic program to drive behavioral change through defined objectives and measurement of effectiveness.



Drive secure behaviors

Campaigns
Social Engineering
Data Protection
Threat Landscape

Events
Company All hands
BU All hands
Ask IT
Threat briefings

Scope
Traditional compliance
Information security
Threat
Privacy
Policy & standards

Targeted training
BU threat specific
Point of risk:
Web, mobile device
Leveraged, train the trainer

Metrics
Training taken
Page impressions
Incident metrics
Secure behavior index

Establish high quality messaging & content

Enhance metrics, targeted & just in time

Govern the environment

The case for controls assurance

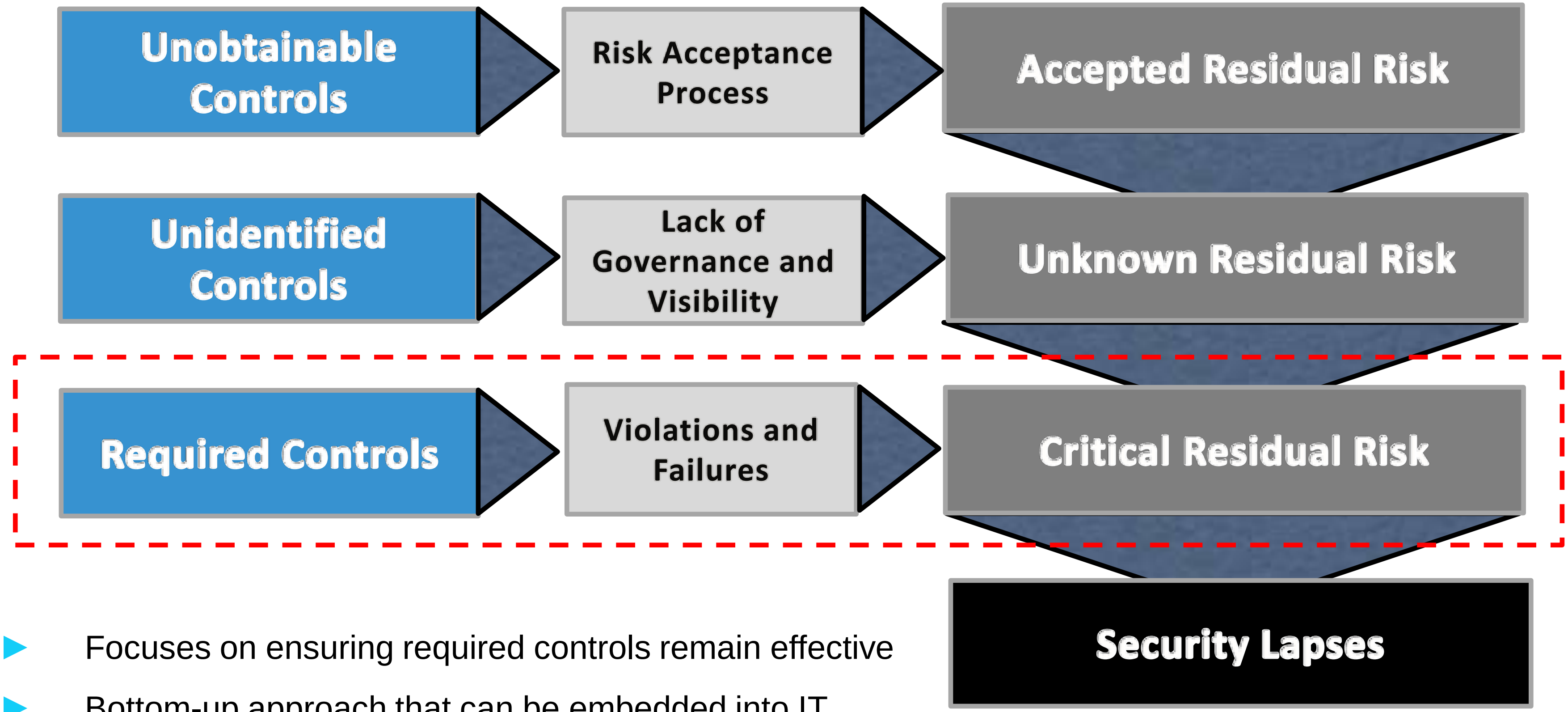
If controls are …..

1	**Justified**	Business units, users, and those who run their systems, agree on the necessity of the controls
2	**Owned**	Ownership of security controls by those who operate the services with assurance provided by security / audit
3	**Embedded**	Embed controls reporting into functional reporting

Controls assurance will …..

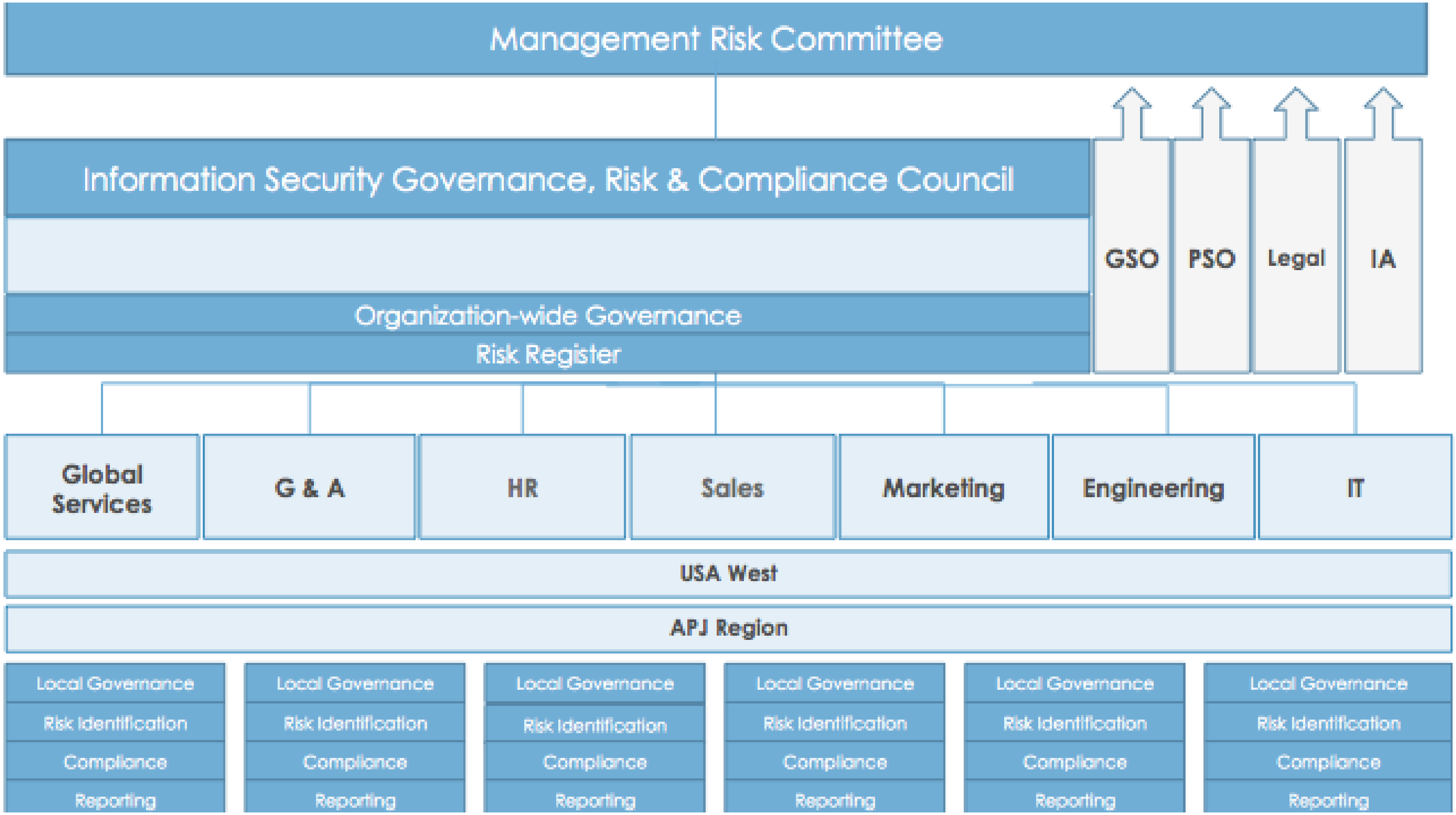
Drive measurement & accountability	Give requirements, trust but verify
Improve operational maturity	Parallel approach to total quality management (build in not bolt on)
Foster consistency & agility	Create a process to define controls, follow it and get out the way

Controls assurance



- Focuses on ensuring required controls remain effective
- Bottom-up approach that can be embedded into IT
- Reporting can be embedded within operational reporting
- Allows other security staff to move up the chain into governance and risk management

Enterprise GRC framework



Management Risk Committee

Information Security Governance, Risk & Compliance Council

Organization-wide Governance

Risk Register

GSO

PSO

Legal

IA

Global Services

G & A

HR

Sales

Marketing

Engineering

IT

USA West

APJ Region

Local Governance

Risk Identification

Compliance

Reporting

Local Governance

Risk Identification

Compliance

Reporting

Local Governance

Risk Identification

Compliance

Reporting

Local Governance

Risk Identification

Compliance

Reporting

Local Governance

Risk Identification

Compliance

Reporting

Local Governance

Risk Identification

Compliance

Reporting

RSA CONFERENCE ASIA PACIFIC 2013

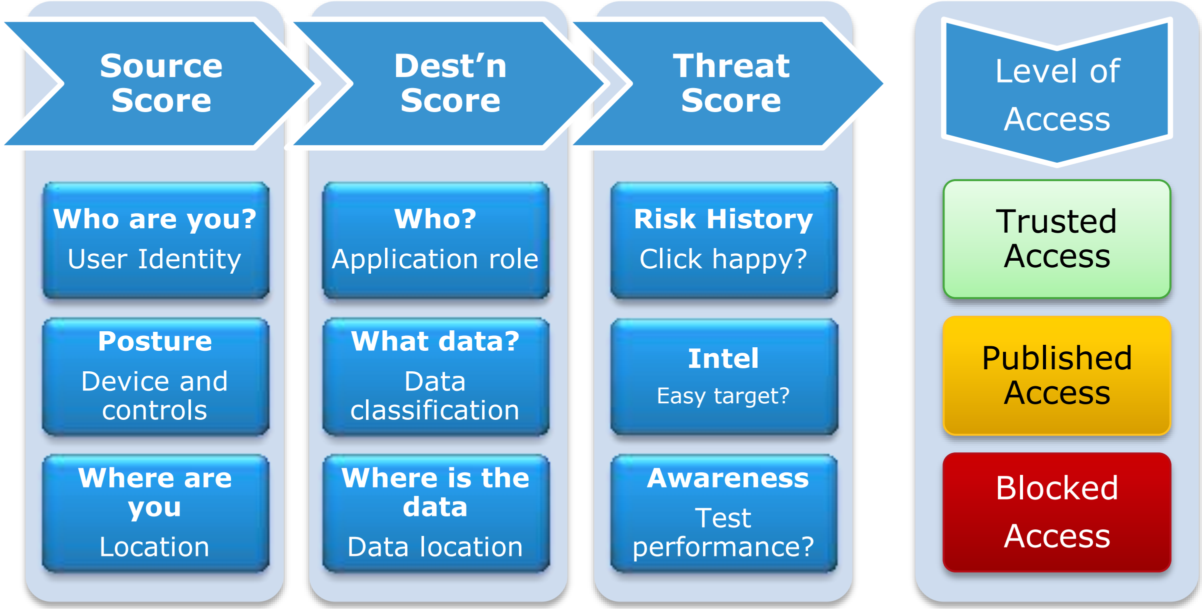
Building a better future

Embedding controls

- Getting close to the data
- Security controls applied as business rules
- Proving risk context and reputation to the application ecosystem
- The beginnings of adaptive security controls

Dynamic & adaptive controls

As the ability to determine dynamic risk improves, for high certainty events we will use the end user machine posture, role, normalcy of request, user compliance history, requested data sensitivity and transaction type to determine (re)authentication level, adapt control requirements and ultimately the success or failure of the transaction.



Source Score
Dest'n Score
Threat Score
Level of Access
Who are you? User Identity
Posture Device and controls
Where are you Location
Who? Application role
What data? Data classification
Where is the data Data location
Risk History Click happy?
Intel Easy target?
Awareness Test performance?
Trusted Access
Published Access
Blocked Access

RSACONFERENCE
ASIA PACIFIC 2013

Next Steps

Taking Action

- Review your program
- Identify opportunities
- Close foundational gaps
- Kick off targeted programs
- Leverage other teams
- Mature programs
- Identify additional transformations

Thank you