Strategies for Managing Risks in the Cloud

Subra Kumaraswamy, Director Intuit Inc.

Professional Strategies – S12

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

2013 Fall Conference – "Sail to Success"

CRISC

CGEIT

CISM

CISA

Executive Summary

Cloud computing goals :

1. Increase business agility and reduce time to market
2. Reduce the infrastructure cost (Data Center footprint reduction)
3. Predictable Opex cost

Public Cloud – Current to Future State

From	To
Slow moving rate of change (limited by provisioning of cloud services)	**Rapid** experimentation (unconstrained by provisioning)
Security protection is provided by **bolt on security** - coarse perimeter and infrastructure controls	Security protection is provided by **built-in security** to control threats specific to cloud
Risk is managed through a **combination of manual security reviews and monitoring for defects**	Risk is managed through **automation to achieve near-zero vulnerabilities**
Governance achieved by **discrete audits, process inspections and manual oversight**	Governance achieved by enterprise wide standards and **baseline security controls**

Why Cloud Security Strategy?

Cloud Security strategy will serve two major functions:

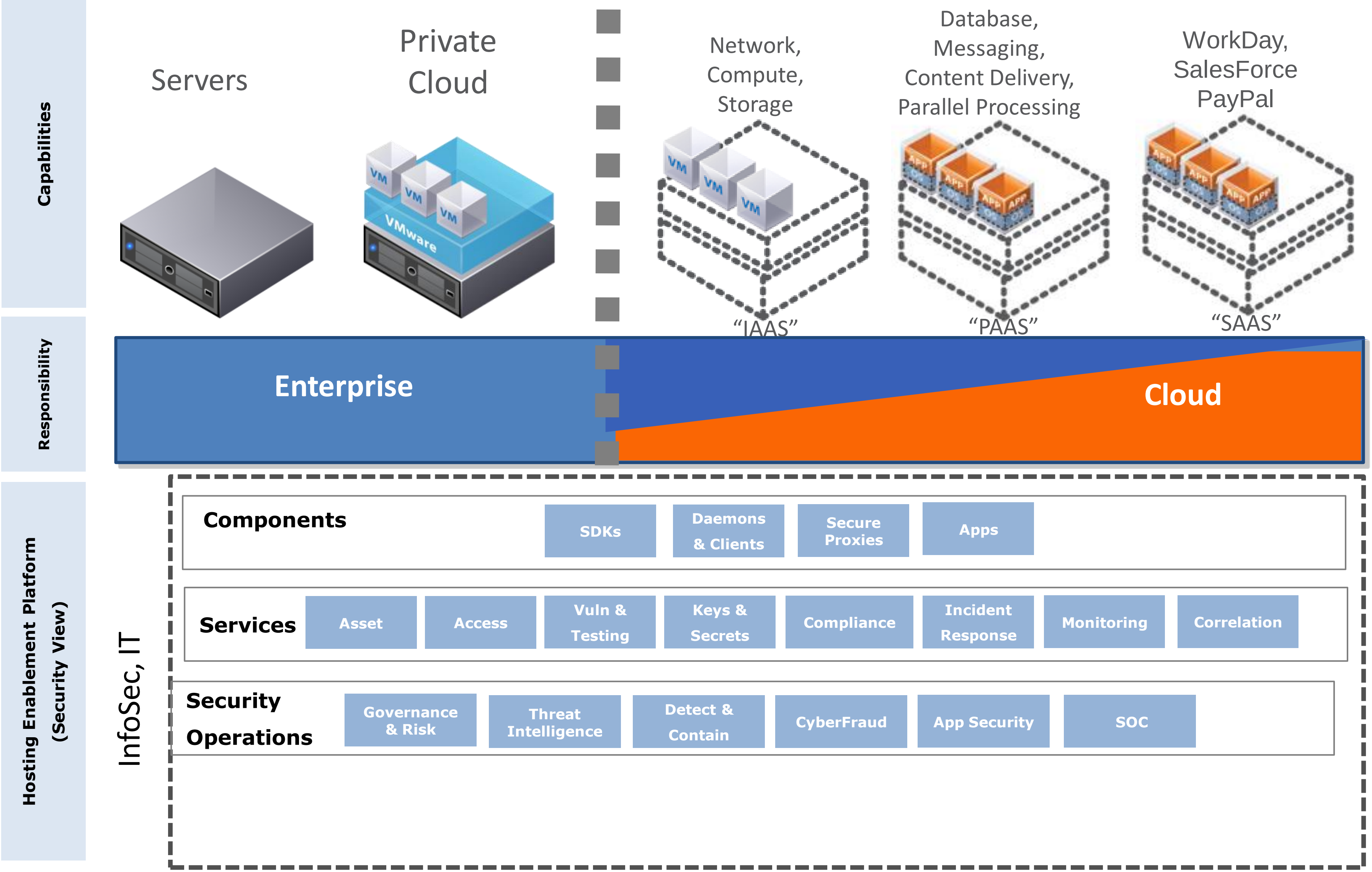
1. To ensure that your cloud solution effectively supports your security and privacy priorities aligned with business strategy.
2. To effectively mitigate risk and protect the confidentiality, integrity and availability of computing resources and data.

Cloud security strategy when executed with coherent governance, architecture, operating model, compliance and security controls will result in a trusted cloud environment for the business to operate and deliver on their goals

Cloud Computing - Value Proposition

- Self Service
- Pay as you go
- Automated
- Shared Infrastructure

Public Cloud – Deployment Model



Capabilities

Servers

Private Cloud

Network, Compute, Storage

Database, Messaging, Content Delivery, Parallel Processing

WorkDay, SalesForce PayPal

"IAAS"

"PAAS"

"SAAS"

Responsibility

Enterprise

Cloud

Hosting Enablement Platform (Security View)

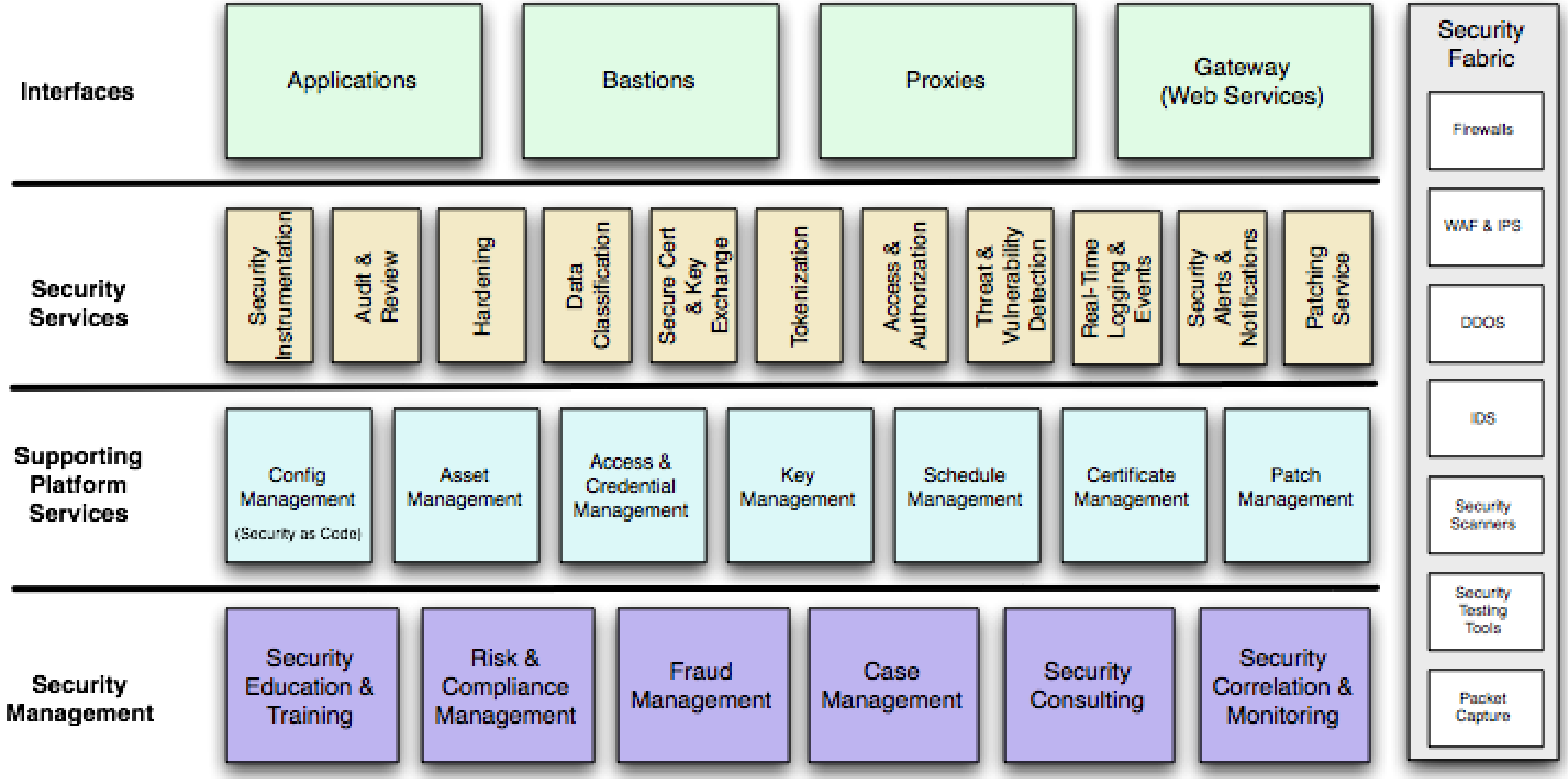
InfoSec, IT

Components: SDKs, Daemons & Clients, Secure Proxies, Apps

Services: Asset, Access, Vuln & Testing, Keys & Secrets, Compliance, Incident Response, Monitoring, Correlation

Security Operations: Governance & Risk, Threat Intelligence, Detect & Contain, CyberFraud, App Security, SOC

Public Cloud – Security Platform Model



Interfaces

Applications

Bastions

Proxies

Gateway (Web Services)

Security Services

Security Instrumentation

Audit & Review

Hardening

Data Classification

Secure Cert & Key Exchange

Tokenization

Access & Authorization

Threat & Vulnerability Detection

Real-Time Logging & Events

Security Alerts & Notifications

Patching Service

Supporting Platform Services

Config Management (Security as Code)

Asset Management

Access & Credential Management

Key Management

Schedule Management

Certificate Management

Patch Management

Security Management

Security Education & Training

Risk & Compliance Management

Fraud Management

Case Management

Security Consulting

Security Correlation & Monitoring

Security Fabric

Firewalls

WAF & IPS

DDOS

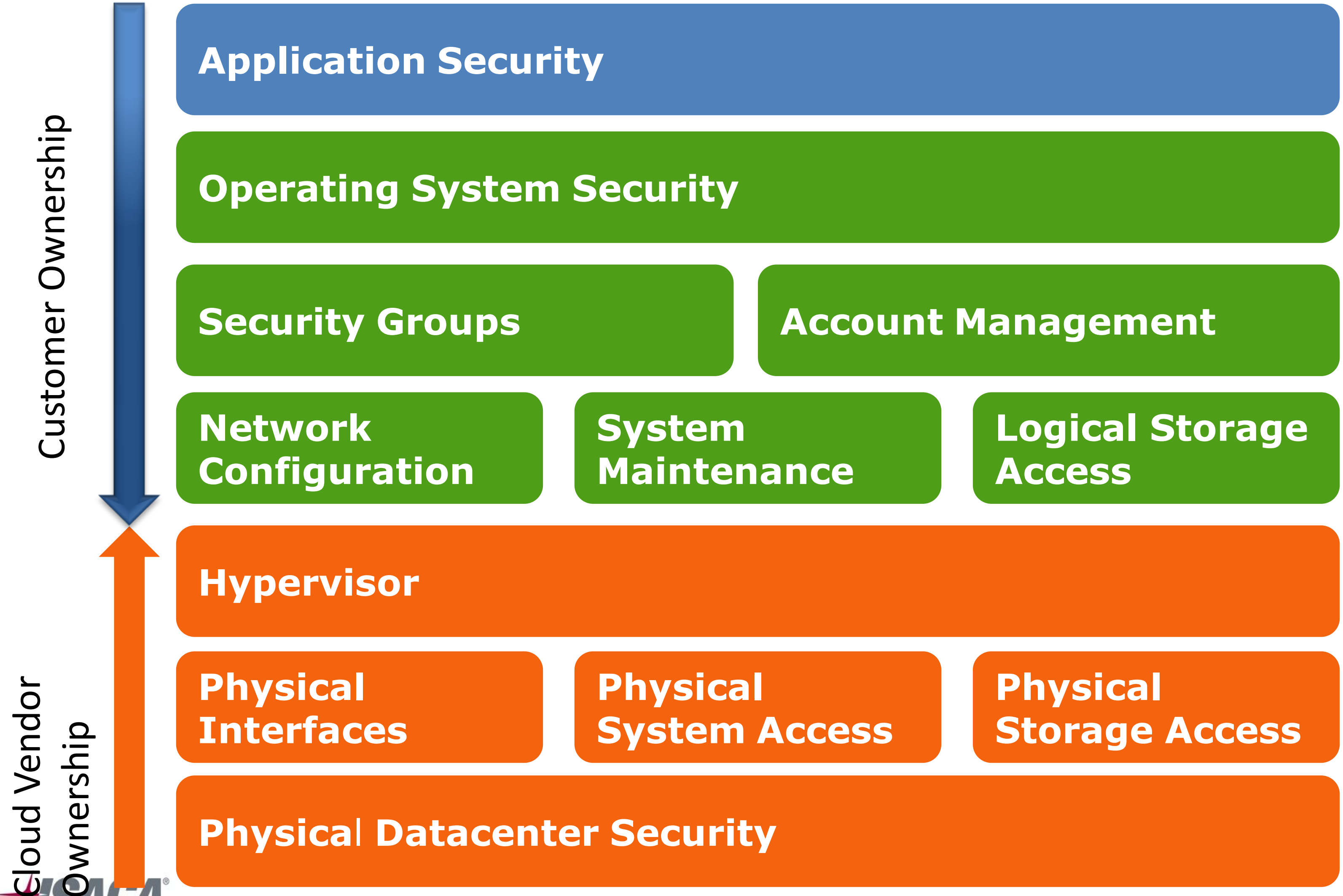
IDS

Security Scanners

Security Testing Tools

Packet Capture

Infrastructure Cloud - Shared Security Model



Customer Ownership

Application Security

Operating System Security

Security Groups

Account Management

Network Configuration

System Maintenance

Logical Storage Access

Cloud Vendor Ownership

Hypervisor

Physical Interfaces

Physical System Access

Physical Storage Access

Physical Datacenter Security

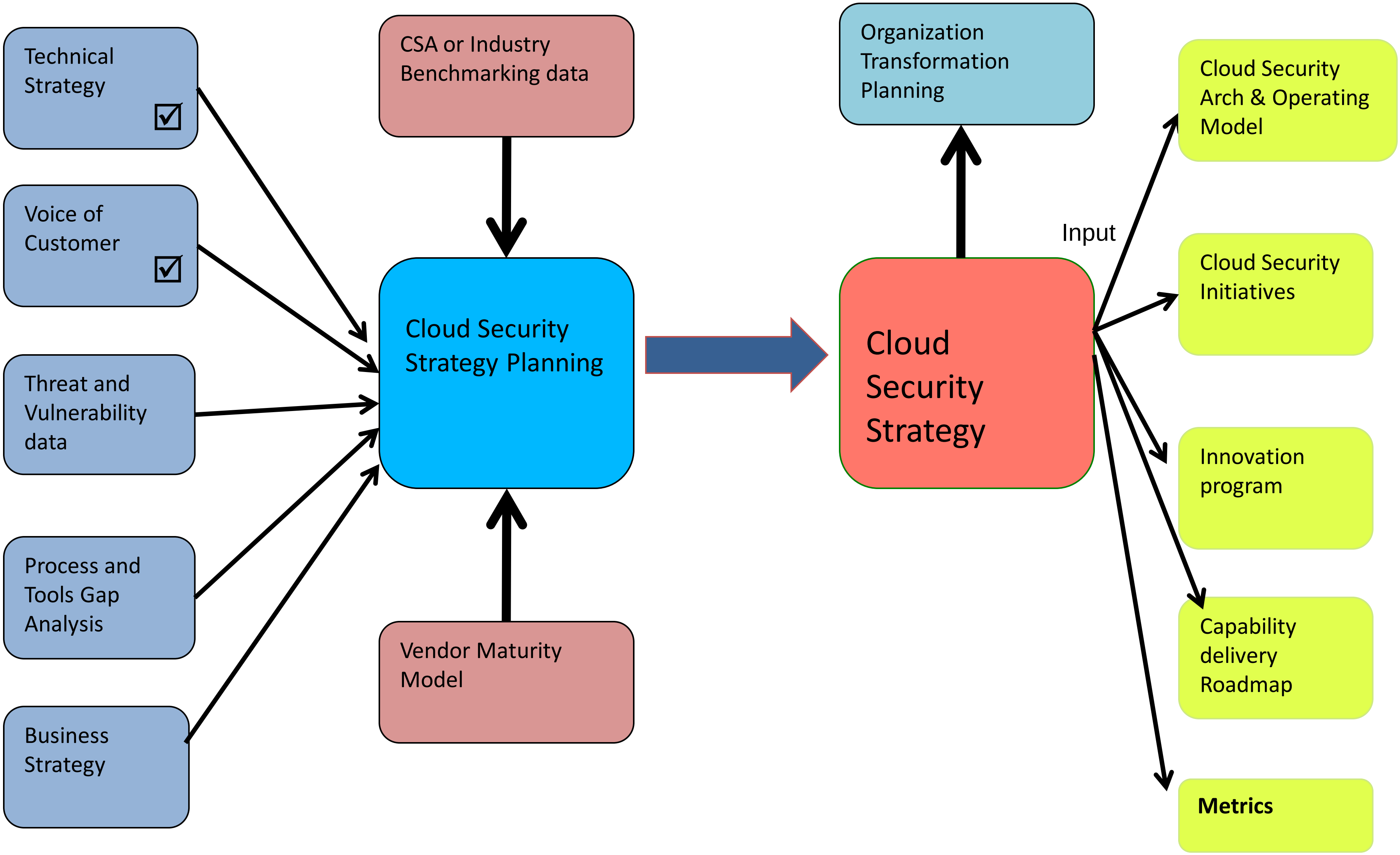
Cloud Computing – Control Vs Accountability

”Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties. ”

From the CSA’s Security Guidance for Critical Areas of Focus in Cloud Computing

How Do We Get There?

Cloud Risk Management - Process


Technical Strategy ☑
Voice of Customer ☑
Threat and Vulnerability data
Process and Tools Gap Analysis
Business Strategy
CSA or Industry Benchmarking data
Cloud Security Strategy Planning
Vendor Maturity Model
Organization Transformation Planning
Cloud Security Strategy
Input
Cloud Security Arch & Operating Model
Cloud Security Initiatives
Innovation program
Capability delivery Roadmap
Metrics

Establish Public Cloud Security Principles

Managing Risk, not Zero Risk [Sample]

1. Do not extend the regulatory or industry compliance footprint into the systems of the public Cloud providers.
2. No data classified as SENSITIVE (or above) can be stored or processed by a service operating in a Public cloud.
3. Applications and Systems that are not cloud ready should not be considered for public cloud deployment.
4. All data at rest in cloud should be encrypted and encryption keys will be always under Enterprise control.
5. All cloud processing must have explicit onboarding and ongoing governance

Establish Clear Vision and Mission

- Sample Vision: “Build Security into Cloud Services to enable Innovation”
- Sample Mission: “Remove security and compliance barriers to use public cloud services”
- Establish Guard Rails and Guidelines for use of cloud within Enterprise
  - E.g. Until we have the right capabilities in place to ensure we can manage risk and meet compliance, our approach is to limit the use of confidential data in cloud until Fy14.
- Be transparent on the scope of applications and services that qualify for cloud use and periodically revisit the scope
  - New controls can accelerate new use cases for cloud adoption

Public Cloud Operating Model

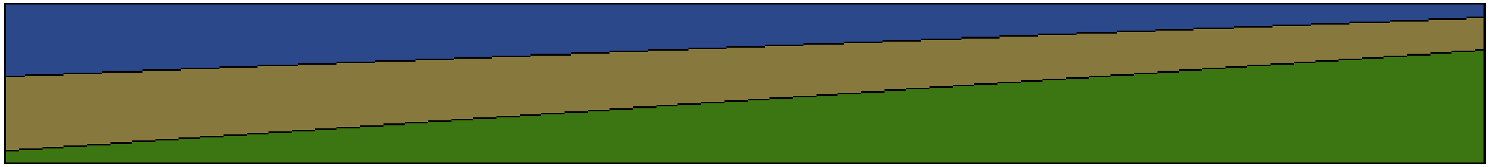
	BU Consumers	**Risk** Consultants & Enablers	**IT** Architects & Builders
Build *Support Cloud usage With security and compliance at scale*	• Identify requirements and Cloud services needed	• Architect security services that scale • Identify controls and guidelines for Public Cloud use	• Builders of capabilities identified in cloud Enabling Services roadmap
Automate *Enable Product and biz Teams by automating controls to Reduce Risk*	• Engage with infosec to plan for controls automation at the design time	• Provide guidance to BUs during deployment	• Provide guidance to BUs during deployment
Operate *Ensure quick response to reduce risk of operating in the cloud*	• Conform to risk management plan for reduced attack surface.	• Operate security services enabling security controls • Help BUs consume services and alerts to protect offerings in the cloud	• Maintain underlying technology for security services

Enable Public Cloud -Three Year Roadmap

Year 1 Year 2 Year 3

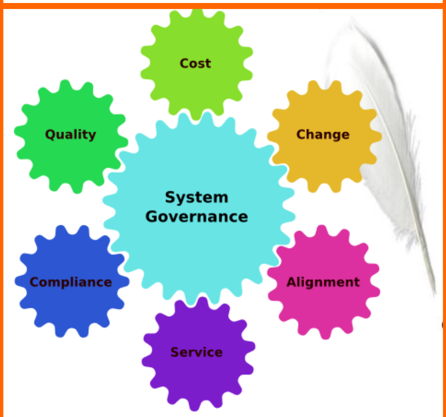
BUILD	Basic Services	Enhanced Services	Operational	Self-Service
AUTOMATE	White Glove	Reduced Consulting	Targeted Consulting	High Risk Consulting
OPERATE	Custom	Run the Business	Scaling	Mature

RESOURCE ALLOCATION



Cloud Risk Management - Pillars

Governance



- Cloud Governance and controls framework (CSA, 27002, etc)
- Business Continuity templates, guidance
- Vendor maturity models

Awareness & Training

- Develop training
- User awareness
- Brown bags
- Cloud security news letter

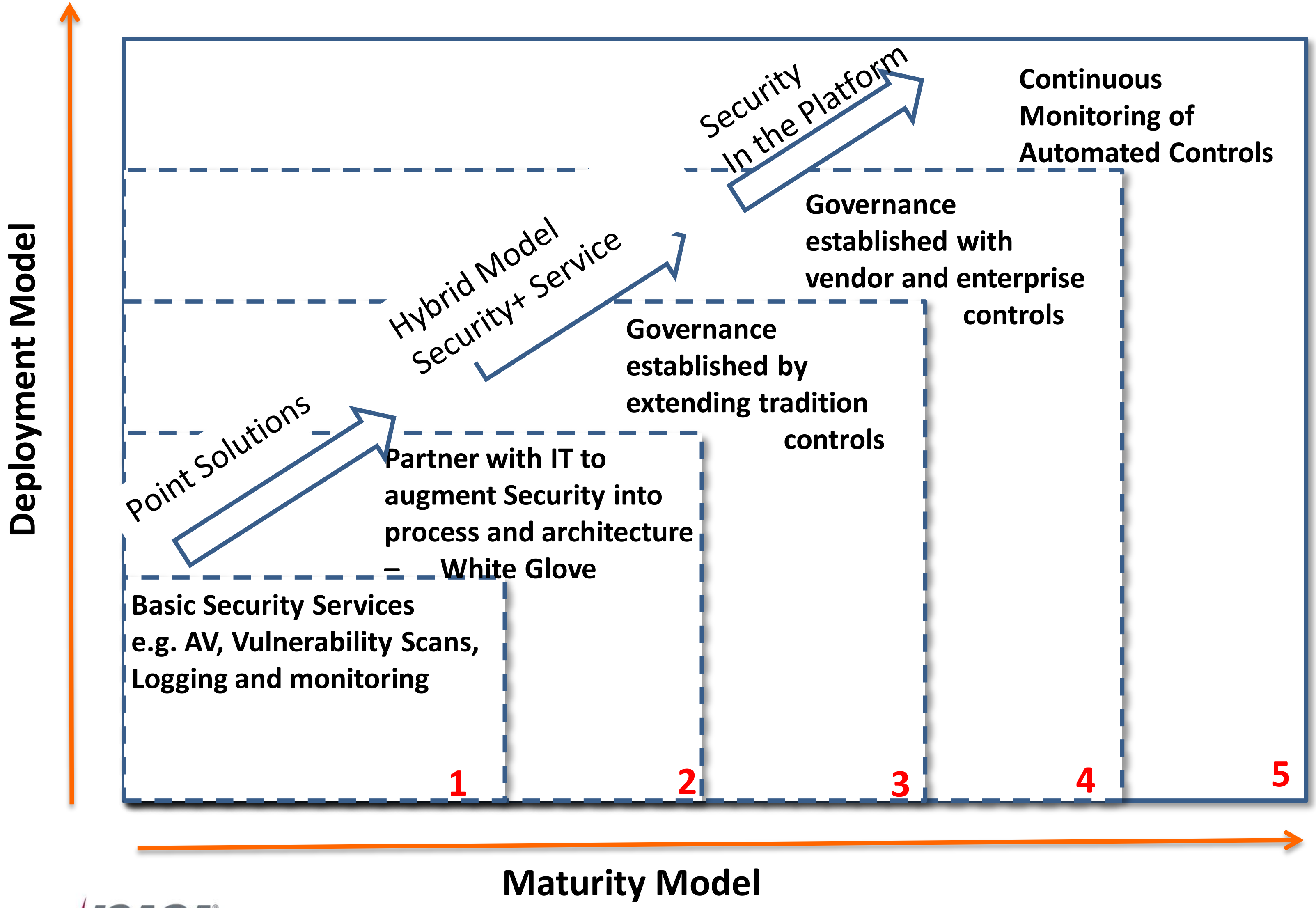
Automation

- Security Automation
- Self-service security
- Security architecture
- Vulnerability Monitoring & response

Enablement

- Guard Rails
- Security Principles
- Risk based deployment
- White Glove Services
- Approved Patterns

Governance Maturity Model



Deployment Model

Basic Security Services e.g. AV, Vulnerability Scans, Logging and monitoring

1

Point Solutions

Partner with IT to augment Security into process and architecture – White Glove

2

Hybrid Model Security+ Service

Governance established by extending tradition controls

3

Governance established with vendor and enterprise controls

4

Security In the Platform

Continuous Monitoring of Automated Controls

5

Maturity Model

Key Takeaways

- Cloud risk management strategy is essential to enable Cloud adoption while managing Security, Privacy and Compliance Risks
- Successful Cloud transformation requires investment in people, process and technology with long term horizon
- Build Security controls into Cloud Deployment and Operating Models
- Manage Risk, Not Zero Risk

Q&A