IBM Security

The Security Implications of Moving to the Cloud

CYBERSECURITY SUMMIT DC METRO

David A. Cass
VP/CISO & Cloud Security Services Global Partner

June 28, 2018 Meeting

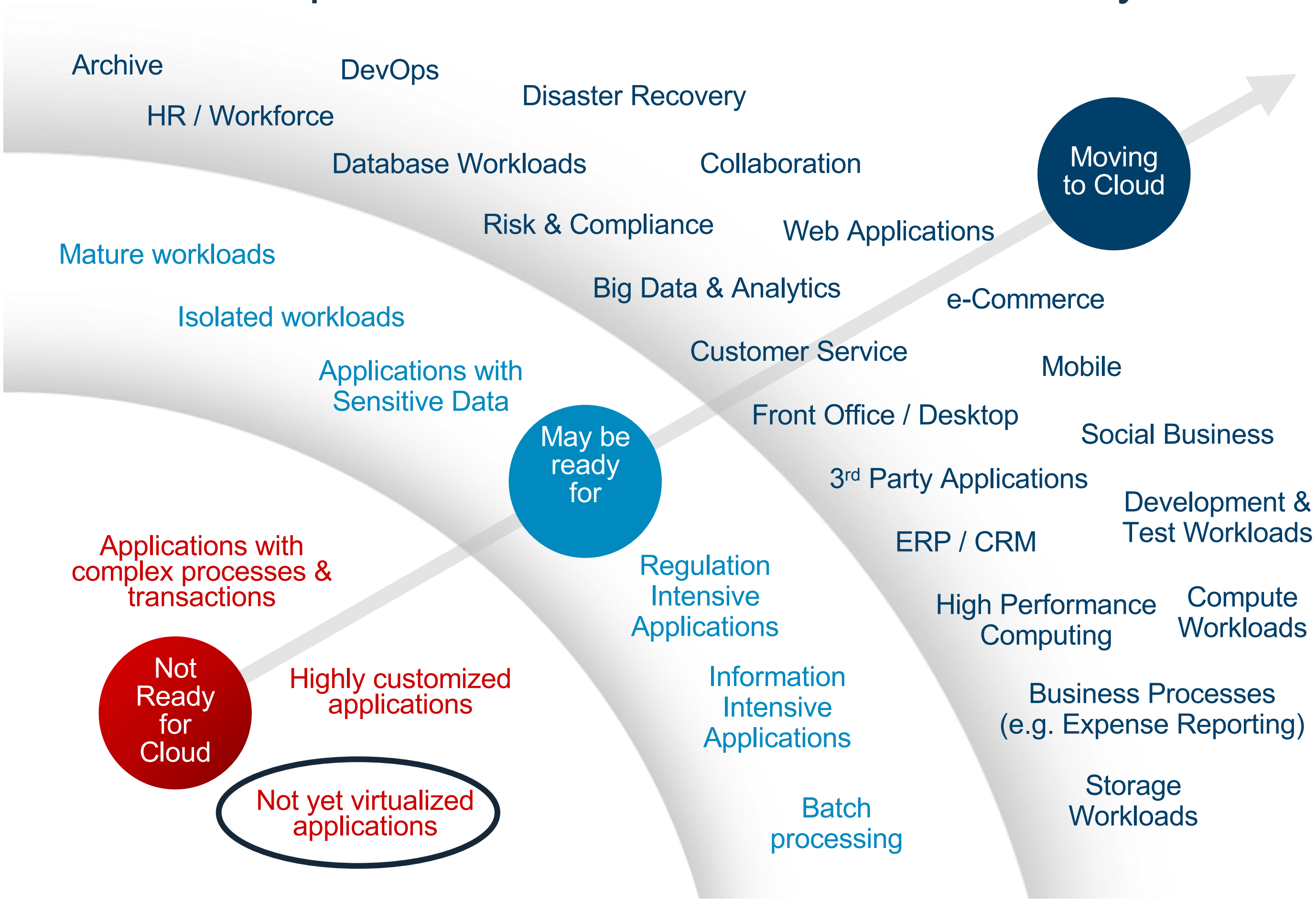
Ready to Win!

Agenda

- Cloud Myths
- Cloud Security Concerns
- The Cloud Journey
- Steps to develop a cloud security strategy

Cloud Myths

What’s Really Going On:
Cloud adoption and business value is driven by workloads



Archive

DevOps

HR / Workforce

Disaster Recovery

Database Workloads

Collaboration

Moving to Cloud

Risk & Compliance

Web Applications

Big Data & Analytics

e-Commerce

Customer Service

Mobile

Front Office / Desktop

Social Business

3rd Party Applications

Development & Test Workloads

ERP / CRM

High Performance Computing

Compute Workloads

Business Processes (e.g. Expense Reporting)

Storage Workloads

Mature workloads

Isolated workloads

Applications with Sensitive Data

May be ready for

Regulation Intensive Applications

Information Intensive Applications

Batch processing

Applications with complex processes & transactions

Not Ready for Cloud

Highly customized applications

Not yet virtualized applications

Cloud Concerns

Cloud security programs face harsh realities every day

Top Cloud Questions from Leadership

Are we protected from the latest threats?

Have we protected our most critical data?

Do we have access to the right skill sets?

Are we adapting to changing platforms?

Are we operating at an appropriate maturity level for our industry?

Are we communicating our risks clearly to our leaders and our board?

Are we maximizing the value of our security investments?

Ever-changing threat landscape
Skills shortage
Adapting Platforms
Innovation to lead
Connected systems
Evolving techniques and technology

Compliance and data protection are the main inhibitors to cloud adoption

PRIVACY & COMPLIANCE

INSIDER THREATS

SECURITY SKILLS GAP

DATA PROTECTION

MONITORING

password
123456
Data Breach
yber Attack

Cloud security programs face harsh realities every day

Recent concerns from Leadership & Regulators

Data Residency may not be the same as Data Sovereignty

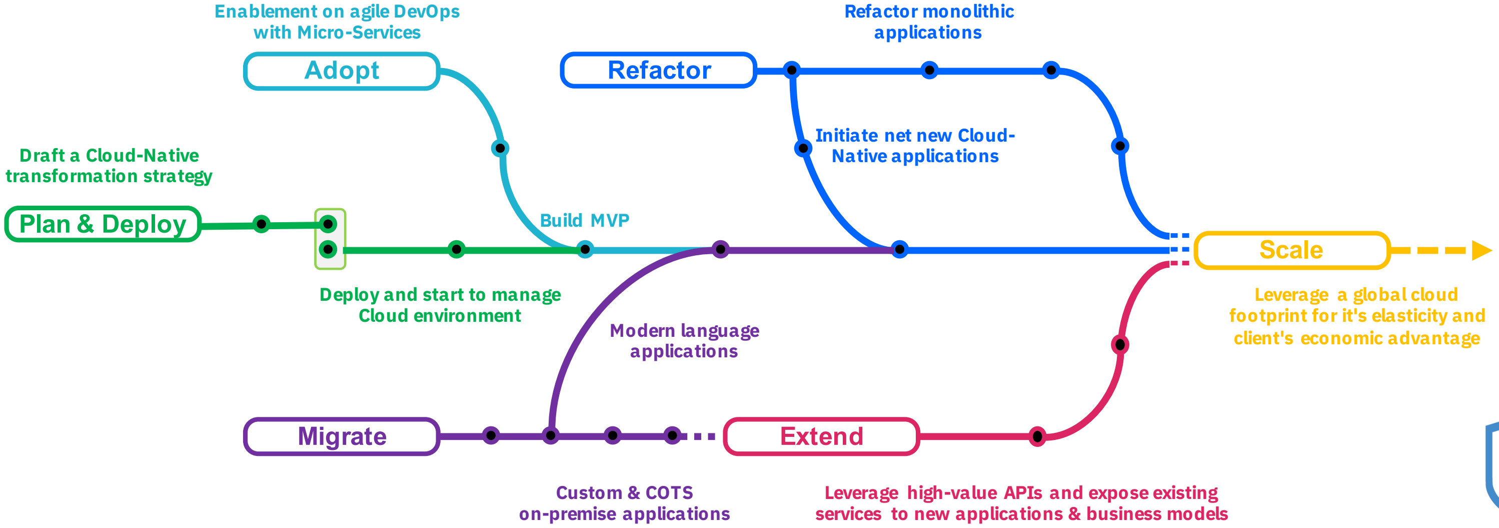
Concentration Risk

Business Continuity / Disaster Recovery

Cloud Journey

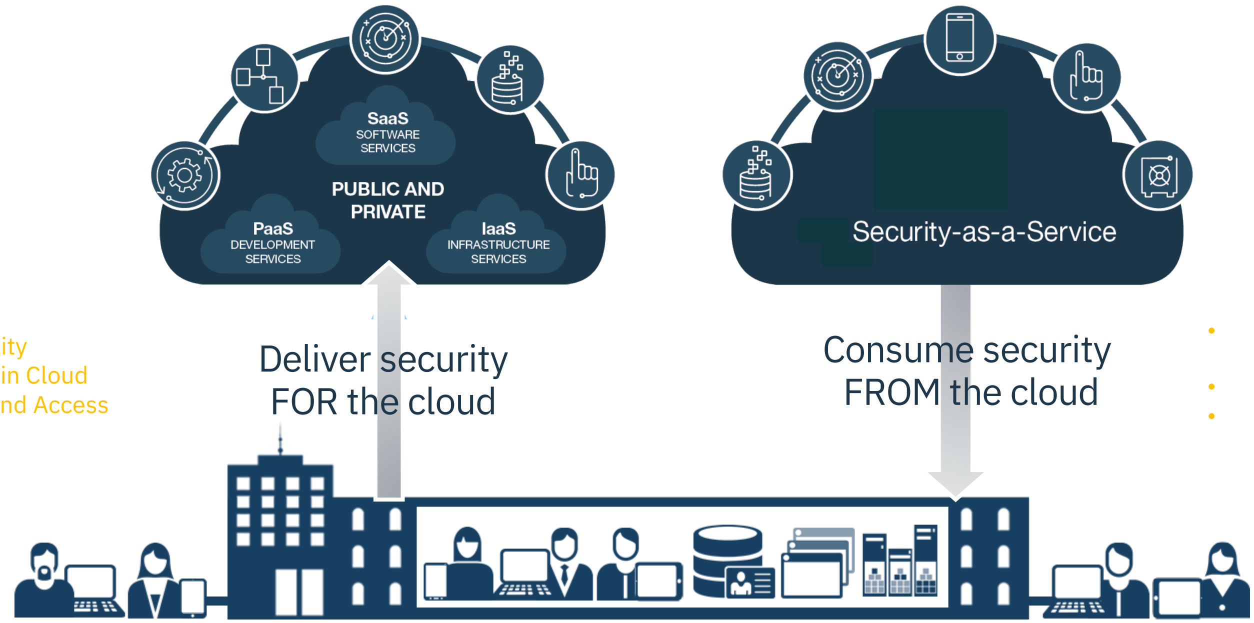
Cloud Journey

- Understand that cloud is a journey – it is not just a change in technology
- Industry understanding is important
- Cloud maturity & capabilities are important


Enablement on agile DevOps with Micro-Services
Adopt
Refactor monolithic applications
Refactor
Initiate net new Cloud-Native applications
Draft a Cloud-Native transformation strategy
Plan & Deploy
Build MVP
Scale
Deploy and start to manage Cloud environment
Modern language applications
Leverage a global cloud footprint for it's elasticity and client's economic advantage
Migrate
Extend
Custom & COTS on-premise applications
Leverage high-value APIs and expose existing services to new applications & business models

Security is **FOR** the cloud and FROM the cloud

- DevSecOps
- Workload Visibility
- Data Protection in Cloud
- Cloud Identity and Access

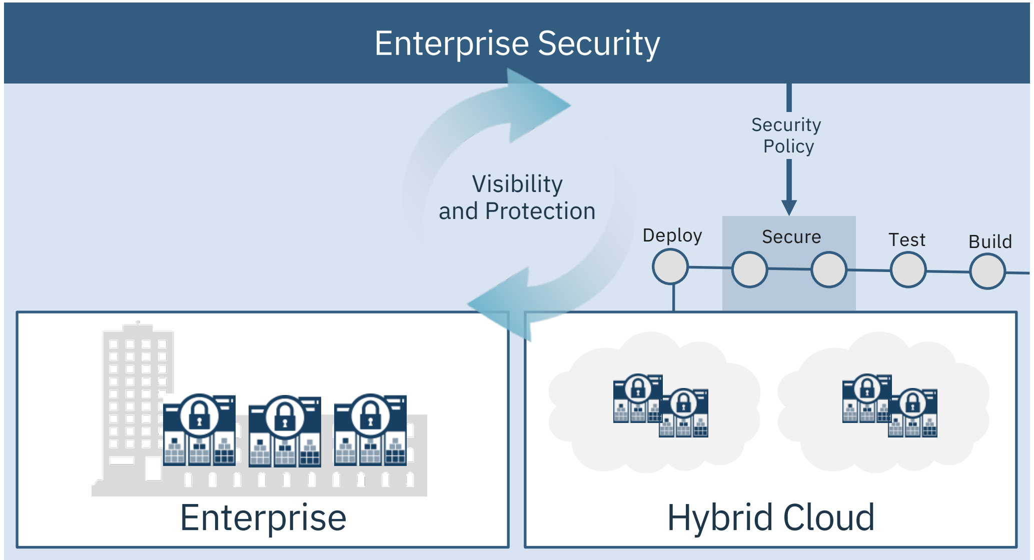


Deliver security FOR the cloud

Consume security FROM the cloud

- Eliminates software management
- Ease of purchase
- Ease of deployment

Cloud is disrupting enterprise security with shared responsibility



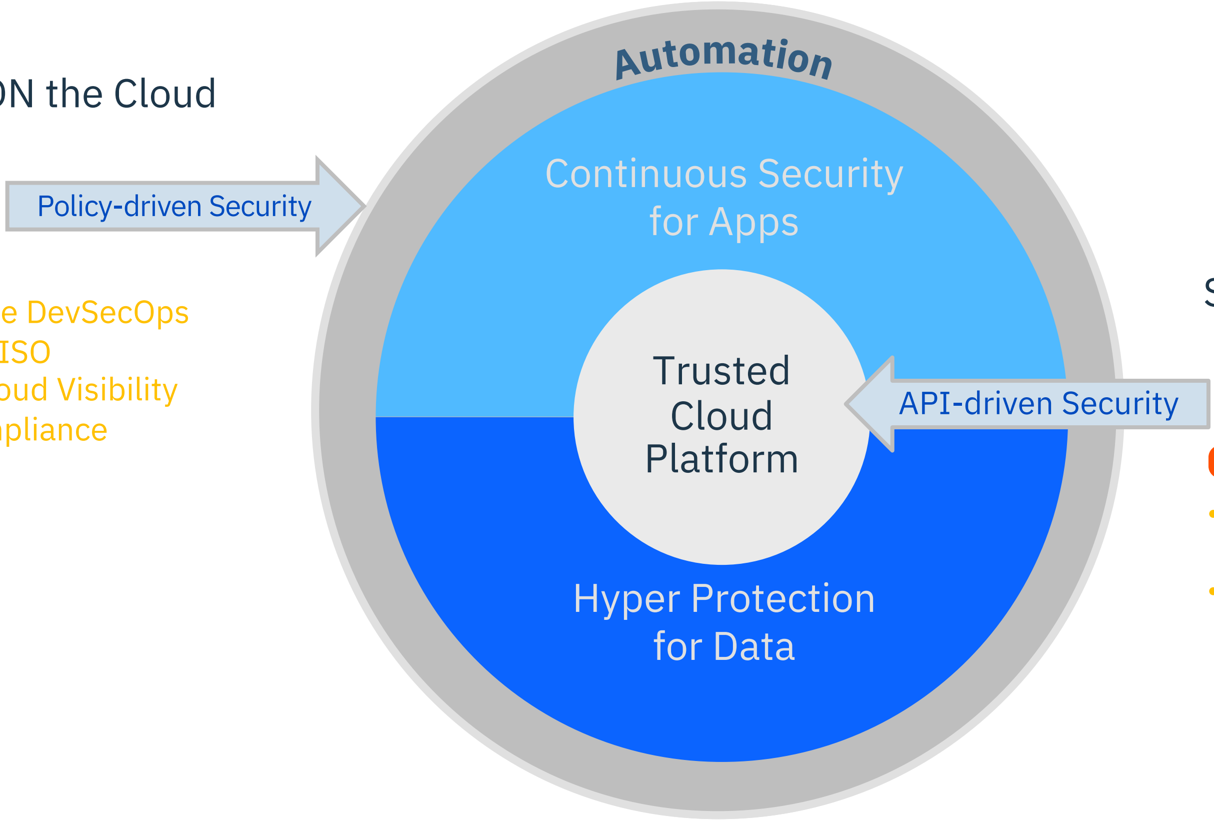
Traditional security controls and infrastructure operational practices are changing to **data and workload centric** cloud security policies, technologies and practices

A holistic view of Security IN the Cloud and ON the Cloud

Security ON the Cloud

CISO Office

- Influence DevSecOps by the CISO
- Multi-Cloud Visibility and compliance


Automation

Continuous Security for Apps

Trusted Cloud Platform

Hyper Protection for Data

Policy-driven Security

API-driven Security

Security IN the Cloud

LoB / Developer

- Native Platform Security Services
- Automated and Continuous DevSecOps for the LOB

Steps to Develop a Cloud Security Strategy

A note on Strategy

“Strategy without tactics is the slowest route to victory.

Tactics without Strategy is the noise before defeat.”

- Sun Tzu

Any move to cloud requires a holistic approach

STRATEGY

Set the overall strategic approach to assessing and managing risk, and the risk appetite that fits with business goals and the firm's environment

Outline the budget, roadmap and implementation approach

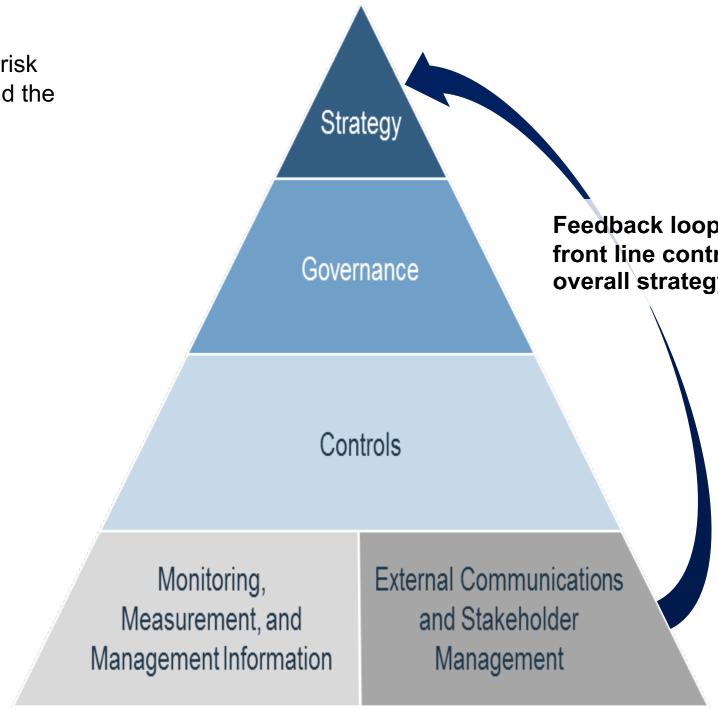
CONTROLS

Define the control environment that delivers the chosen risk appetite and enforces the policy framework

MONITORING, MEASURING AND MANAGEMENT INFORMATION

Monitor threats, incidents and the performance of controls

Track the performance of risk management against risk appetite, using quantitative metrics where possible



Strategy
Governance
Controls
Monitoring, Measurement, and Management Information
External Communications and Stakeholder Management

Feedback loop – from front line controls to overall strategy

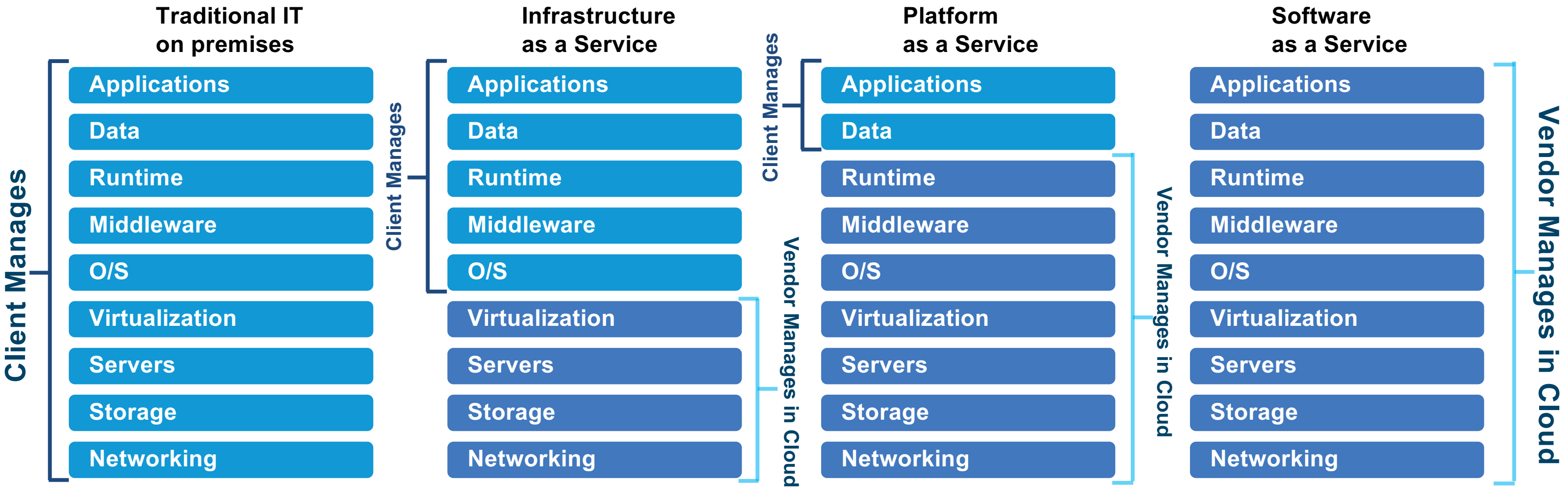
GOVERNANCE

Define organizational roles and responsibilities, policy framework and arrangements for oversight of the risk profile and risk management framework

EXTERNAL COMMUNICATION AND STAKEHOLDER MANAGEMENT

Manage external reporting requirements and requests, and engagement with external stakeholders such as regulators

Steps to Develop a Cloud Security Strategy



Traditional IT on premises	Infrastructure as a Service	Platform as a Service	Software as a Service
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Client Manages

Client Manages

Vendor Manages in Cloud

Client Manages

Vendor Manages in Cloud

Vendor Manages in Cloud

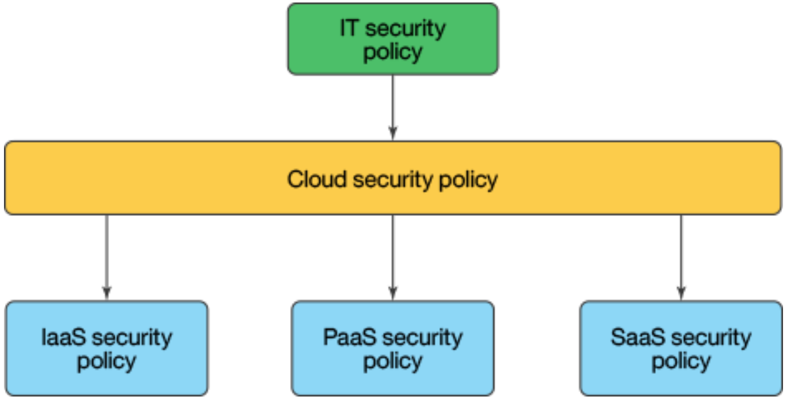
Integration of Roles, Processes, Information, and Technology covers the new cloud models needing additional service management

Additional Service Management Needed

Provided by Cloud Provider

Steps to Develop a Cloud Security Strategy

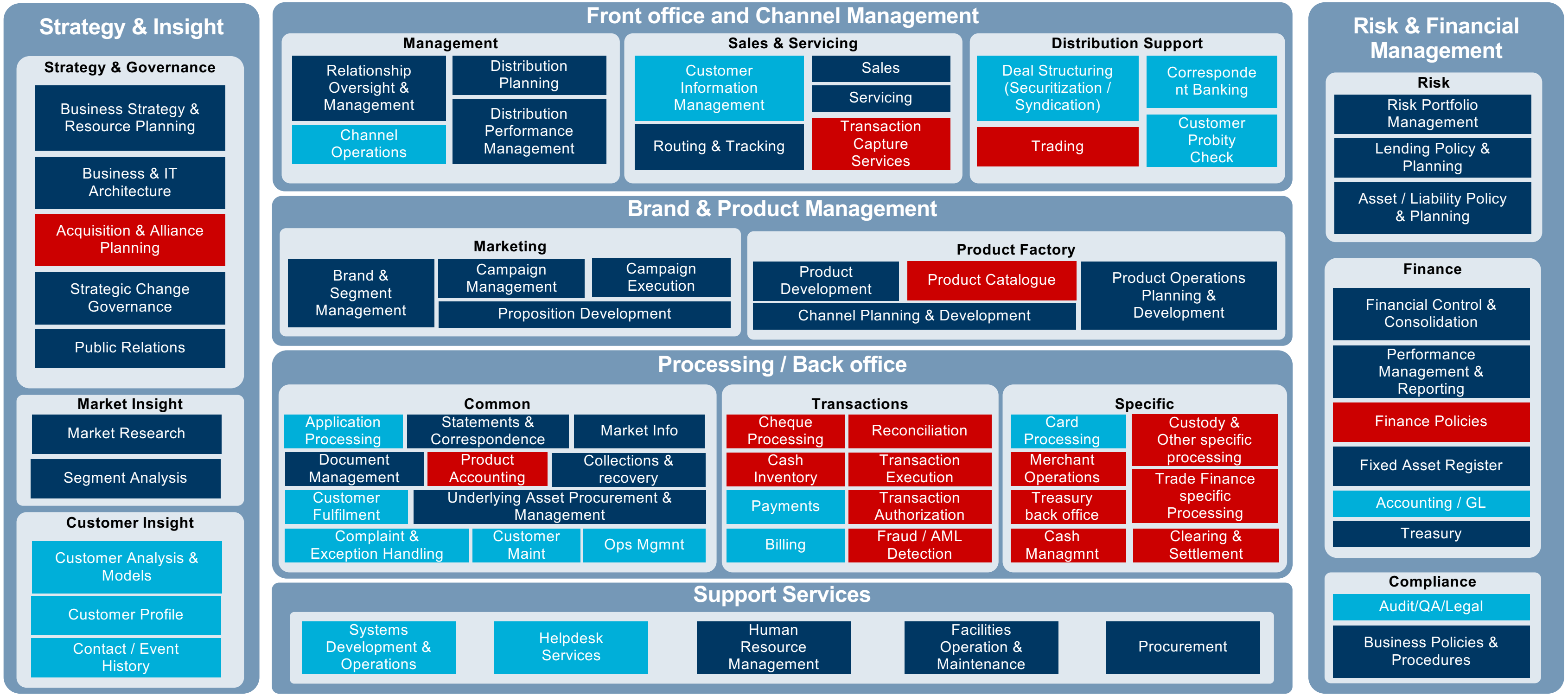
- Evaluate Security Governance / Organization
  - Cloud Security Governance Models
  - Organization design
  - DevOps



Steps to Develop a Cloud Security Strategy

- Determine Cloud Security Assessment Approach
  - Business process focused
  - Application Tiering Model
  - Builds in Security Requirements / Risk Tolerance

Banking & Insurance – Use Cases and Cloud Readiness as of March 2017



Strategy & Insight

Strategy & Governance
- ■ Business Strategy & Resource Planning
- ■ Business & IT Architecture
- 🟥 Acquisition & Alliance Planning
- ■ Strategic Change Governance
- ■ Public Relations

Market Insight
- ■ Market Research
- ■ Segment Analysis

Customer Insight
- 🟦 Customer Analysis & Models
- 🟦 Customer Profile
- 🟦 Contact / Event History

Front office and Channel Management

Management
- ■ Relationship Oversight & Management
- ■ Distribution Planning
- 🟦 Channel Operations
- ■ Distribution Performance Management

Sales & Servicing
- 🟦 Customer Information Management
- ■ Sales
- ■ Servicing
- ■ Routing & Tracking
- 🟥 Transaction Capture Services

Distribution Support
- 🟦 Deal Structuring (Securitization / Syndication)
- 🟦 Corresponde nt Banking
- 🟥 Trading
- 🟦 Customer Probity Check

Brand & Product Management

Marketing
- ■ Brand & Segment Management
- ■ Campaign Management
- ■ Campaign Execution
- ■ Proposition Development

Product Factory
- ■ Product Development
- 🟥 Product Catalogue
- ■ Product Operations Planning & Development
- ■ Channel Planning & Development

Processing / Back office

Common
- 🟦 Application Processing
- ■ Statements & Correspondence
- ■ Market Info
- ■ Document Management
- 🟥 Product Accounting
- ■ Collections & recovery
- 🟦 Customer Fulfilment
- ■ Underlying Asset Procurement & Management
- 🟦 Complaint & Exception Handling
- 🟦 Customer Maint
- 🟦 Ops Mgmnt

Transactions
- 🟥 Cheque Processing
- 🟥 Reconciliation
- 🟥 Cash Inventory
- 🟥 Transaction Execution
- 🟦 Payments
- 🟥 Transaction Authorization
- 🟦 Billing
- 🟥 Fraud / AML Detection

Specific
- 🟦 Card Processing
- 🟥 Custody & Other specific processing
- 🟥 Merchant Operations
- 🟥 Trade Finance specific Processing
- 🟥 Treasury back office
- 🟥 Cash Managmnt
- 🟥 Clearing & Settlement

Support Services

- 🟦 Systems Development & Operations
- 🟦 Helpdesk Services
- ■ Human Resource Management
- ■ Facilities Operation & Maintenance
- ■ Procurement

Risk & Financial Management

Risk
- ■ Risk Portfolio Management
- ■ Lending Policy & Planning
- ■ Asset / Liability Policy & Planning

Finance
- ■ Financial Control & Consolidation
- ■ Performance Management & Reporting
- 🟥 Finance Policies
- ■ Fixed Asset Register
- 🟦 Accounting / GL
- ■ Treasury

Compliance
- 🟦 Audit/QA/Legal
- ■ Business Policies & Procedures

NOTE: The above is a representative example only

■ More ready for cloud
🟦 May be ready for cloud
🟥 Currently being evaluated for cloud

Data Security

Examples for discussion purposes – this information needs to be defined to for your specific organization's requirements.

Requirement	Level 1	Level 2	Level 3	Level 4	Level 5
Security Focus	Not in place	Focus on specific areas that impact team directly.	Data strategy with security Tiers	Full compliance with security Tier requirements	Fully compliant with periodic compliance reviews
Data Classification	Not in place	Data Classification (IVC) Policy awareness but not consistently followed	Data Classification (IVC) Policy understood, data is appropriately classified, but policy requirements not consistently followed	Data Classification (IVC) Policy understood, data is appropriately classified, and policy requirements consistently followed	Regular self audits, testing, and assessment/validation of Data Classification compliance
Data models / flows	Not in place	Know who to go to for data models and data flows	Data models and data flows kept locally	Data models and data flows stored centrally	Data Transfer agreements in place to match all data flows; Data loss prevention in place for in scope systems
Data Ownership	Not in place	Data owners understood but not documented	Data owners defined and documented. Some understanding of data location.	Data owners defined and registered. Data locations defined and registered.	Enterprise registry of data owners with full registry of data location by type. Periodic revalidation of data ownership and location.
Data Access	Not in place	Data access not well defined; AdHoc data access procedures	Data access granted by individual based on individual request; Manual request and provisioing system	Data access granted mostly by need to know, automated request and provisioning system	Access granted proactively restricted to minimum needs; Periodic data access reviews

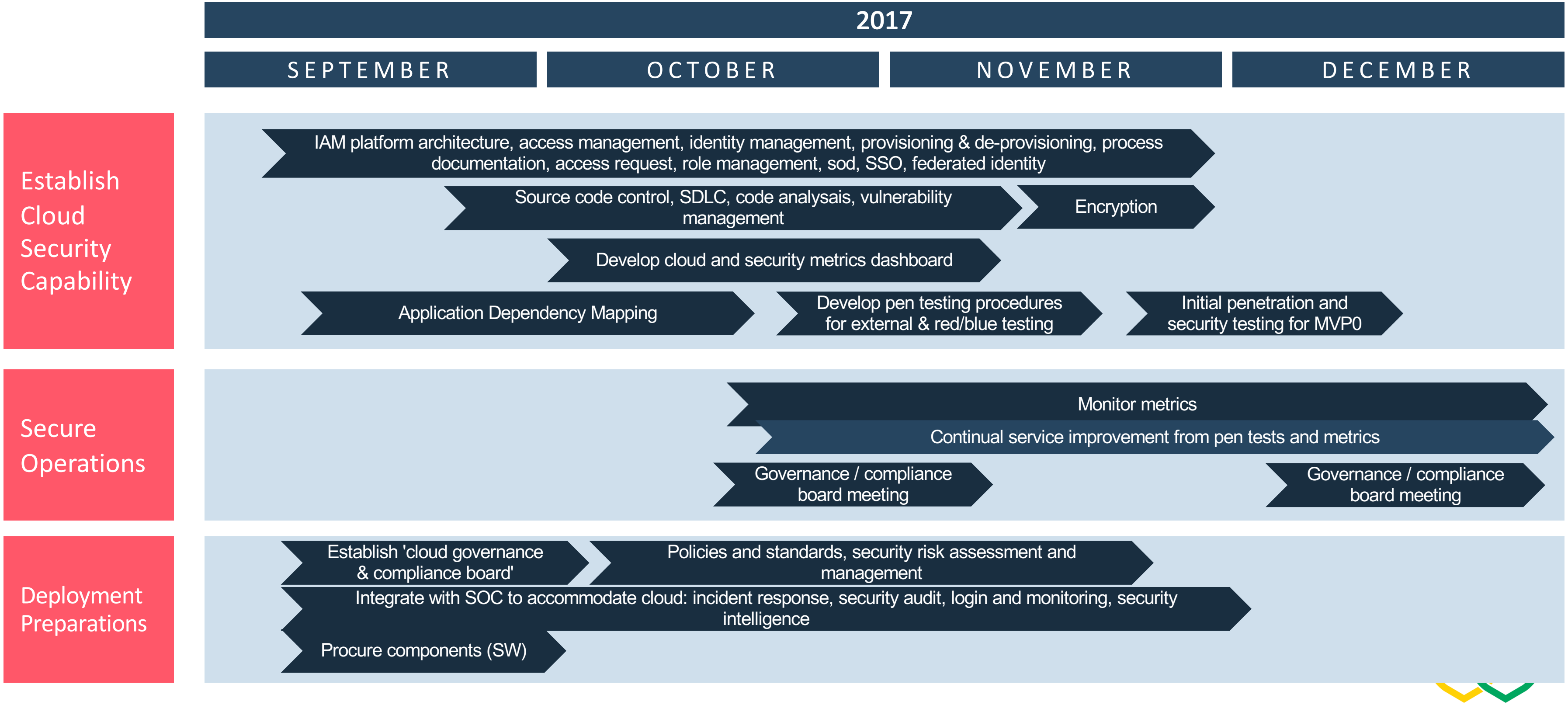
Maturity Level Expectations By Tier

		Maturity Level Expectation				
Tiering	Tier#	Application Security	Network & Systems	Data Security	Secure OPS	Security Strat & Org
Tier 1: Regulated Data (PHI, SOX, SPII, PCI, etc.)	1	4	4	5	4	4
Tier 2: Confidential, Attorney Client Privileged Data, Intellectual Property and Personally Identifiable (External)	2	3	4	4	4	4
Tier 3: Confidential, Attorney Client Privileged Data, Intellectual Property and Personally Identifiable (Internal)	3	3	3	4	4	3
Tier 4: Public Data (No Distinction between external & Internal)	4	3	4	3	3	3
Tier 5: Temporary Environment for POC, Lab work or Testing (No Prod or "Real" Data)	5	2	2	2	2	2

Example for discussion purposes – this information needs to be defined for your specific organization's requirements.

ROADMAP EXAMPLE

Setting up a hybrid cloud from zero to MVP



2017

SEPTEMBER | OCTOBER | NOVEMBER | DECEMBER

Establish Cloud Security Capability

- IAM platform architecture, access management, identity management, provisioning & de-provisioning, process documentation, access request, role management, sod, SSO, federated identity
- Source code control, SDLC, code analysais, vulnerability management
- Encryption
- Develop cloud and security metrics dashboard
- Application Dependency Mapping
- Develop pen testing procedures for external & red/blue testing
- Initial penetration and security testing for MVP0

Secure Operations

- Monitor metrics
- Continual service improvement from pen tests and metrics
- Governance / compliance board meeting
- Governance / compliance board meeting

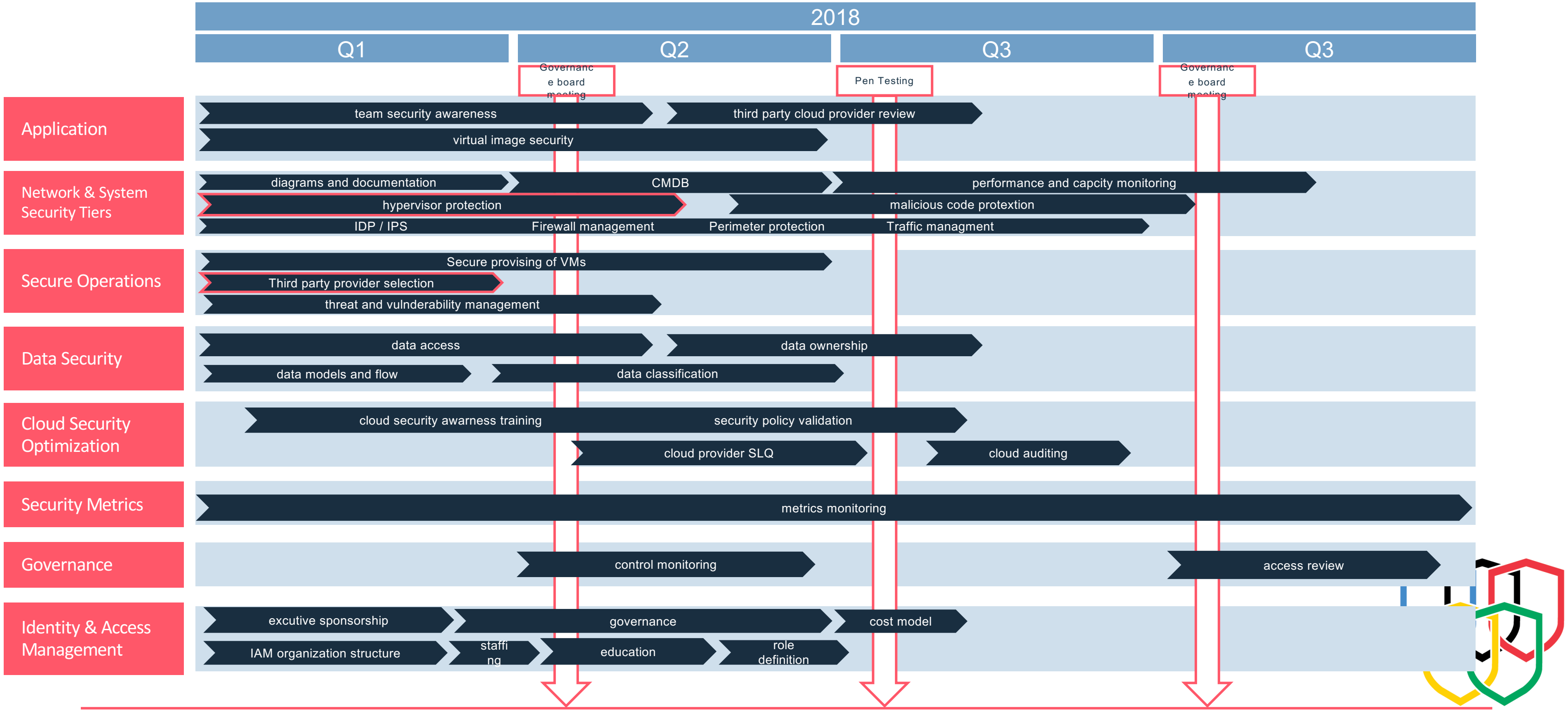
Deployment Preparations

- Establish 'cloud governance & compliance board'
- Policies and standards, security risk assessment and management
- Integrate with SOC to accommodate cloud: incident response, security audit, login and monitoring, security intelligence
- Procure components (SW)

ROADMAP EXAMPLE

Year 1 after cloud establishment.

SECURITY & COMPLIANCE ROADMAP FOR T1



2018

Q1

Q2

Q3

Q3

Governance board meeting

Pen Testing

Governance board meeting

Application

team security awareness

third party cloud provider review

virtual image security

Network & System Security Tiers

diagrams and documentation

CMDB

performance and capcity monitoring

hypervisor protection

malicious code protextion

IDP / IPS

Firewall management

Perimeter protection

Traffic managment

Secure Operations

Secure provising of VMs

Third party provider selection

threat and vulnderability management

Data Security

data access

data ownership

data models and flow

data classification

Cloud Security Optimization

cloud security awarness training

security policy validation

cloud provider SLQ

cloud auditing

Security Metrics

metrics monitoring

Governance

control monitoring

access review

Identity & Access Management

excutive sponsorship

governance

cost model

IAM organization structure

staffing

education

role definition

IBM Security

THANK YOU

FOLLOW US ON:

ibm.com/security

securityintelligence.com

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.