IBM Security

The Security Implications of Moving to the Cloud

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

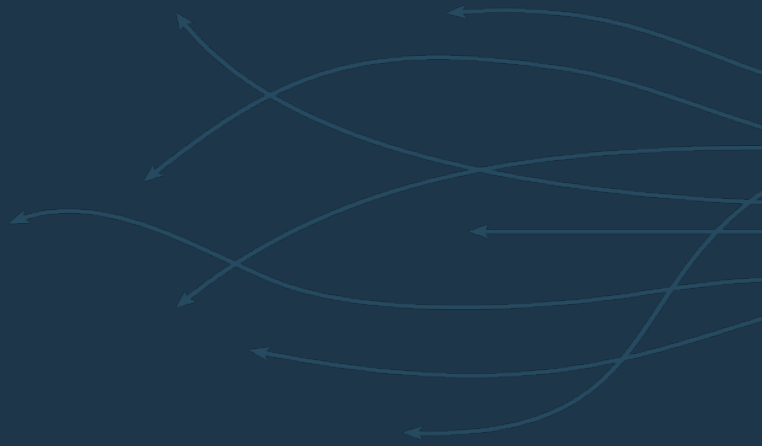
July 16, 2019 Meeting

Ready to Win!

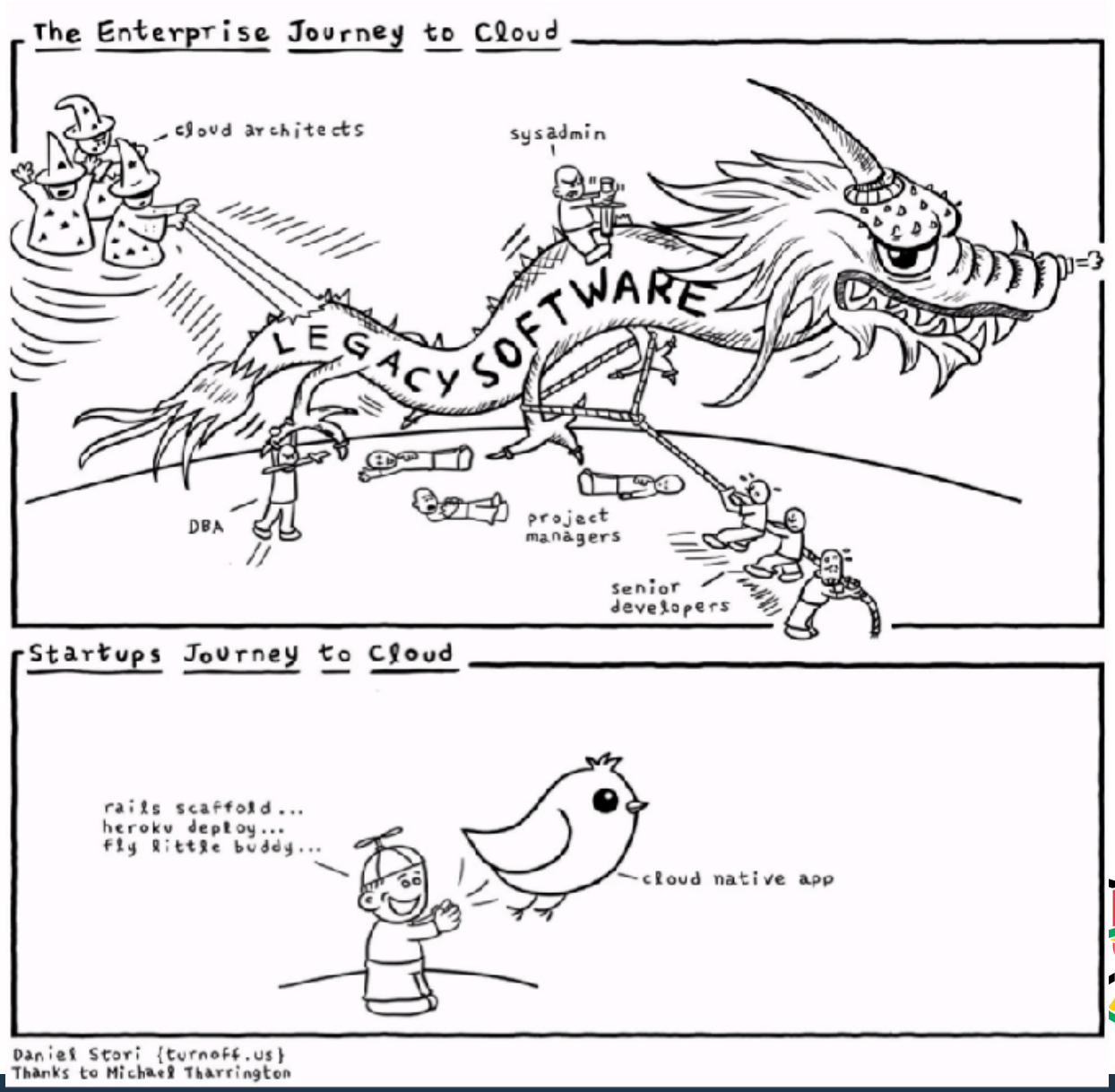
Agenda

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

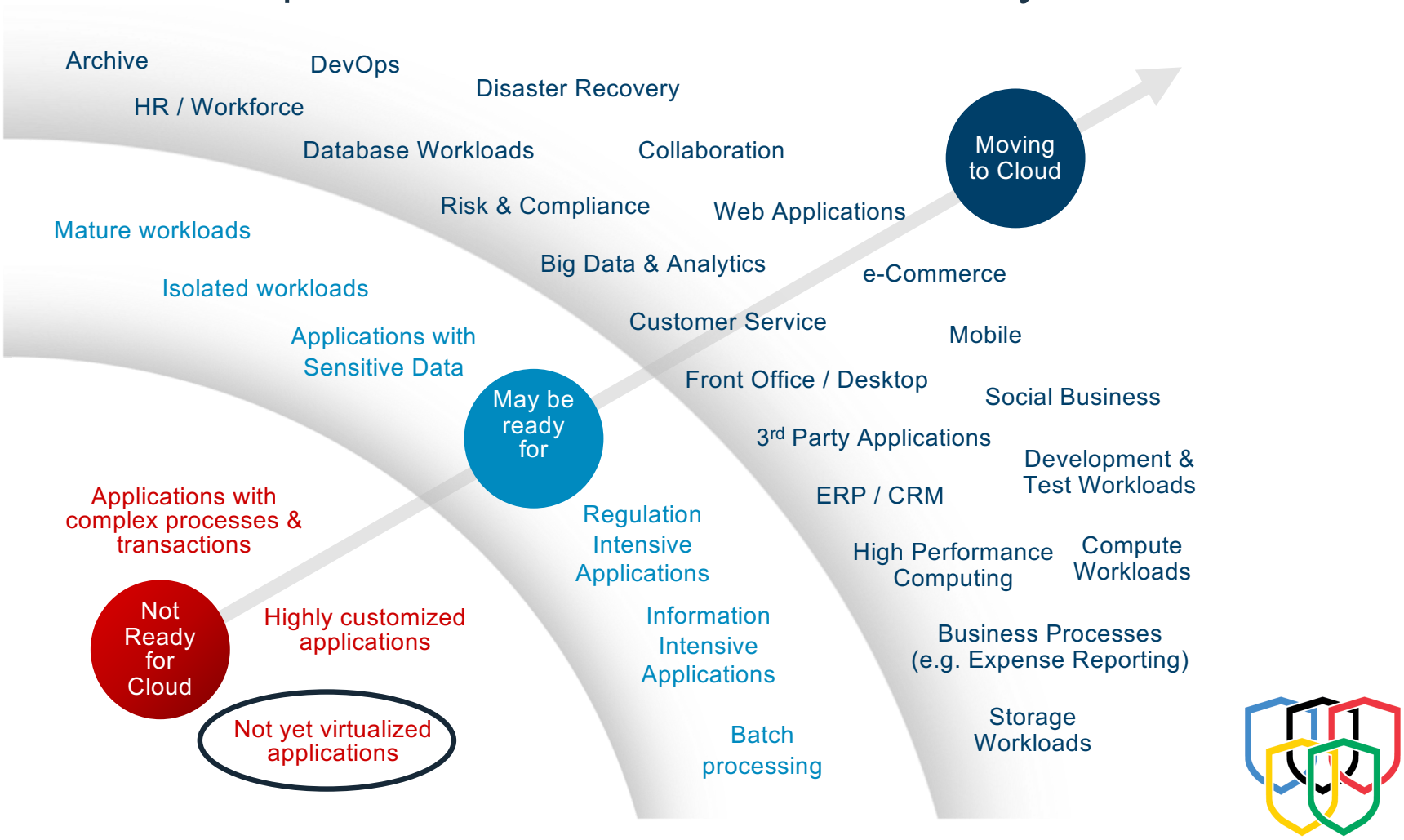
Cloud Myths



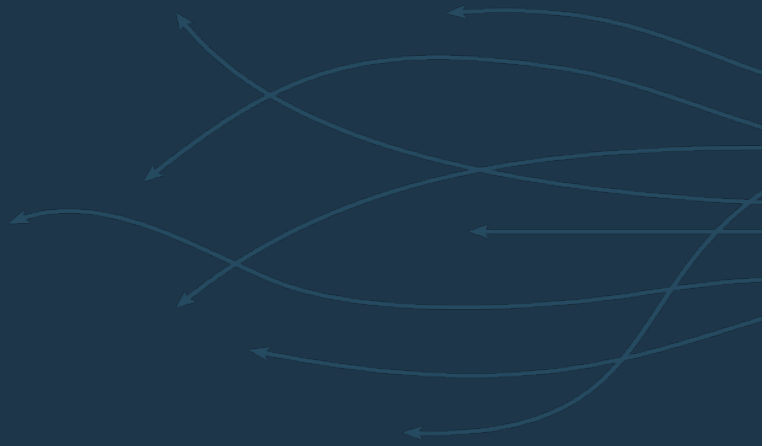
Cloud requires cultural change!



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



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?

Compliance and data protection are the main inhibitors to cloud adoption

Cloud security programs face harsh realities every day

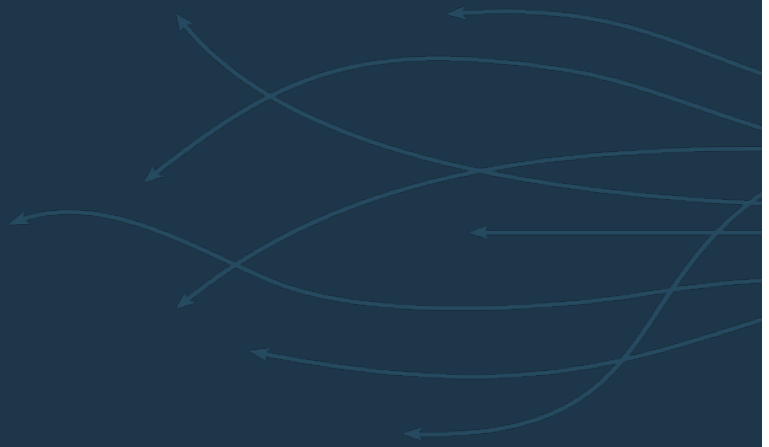
Recent concerns from Leadership & Regulators

Data Residency may not be the same as Data Sovereignty

Concentration Risk

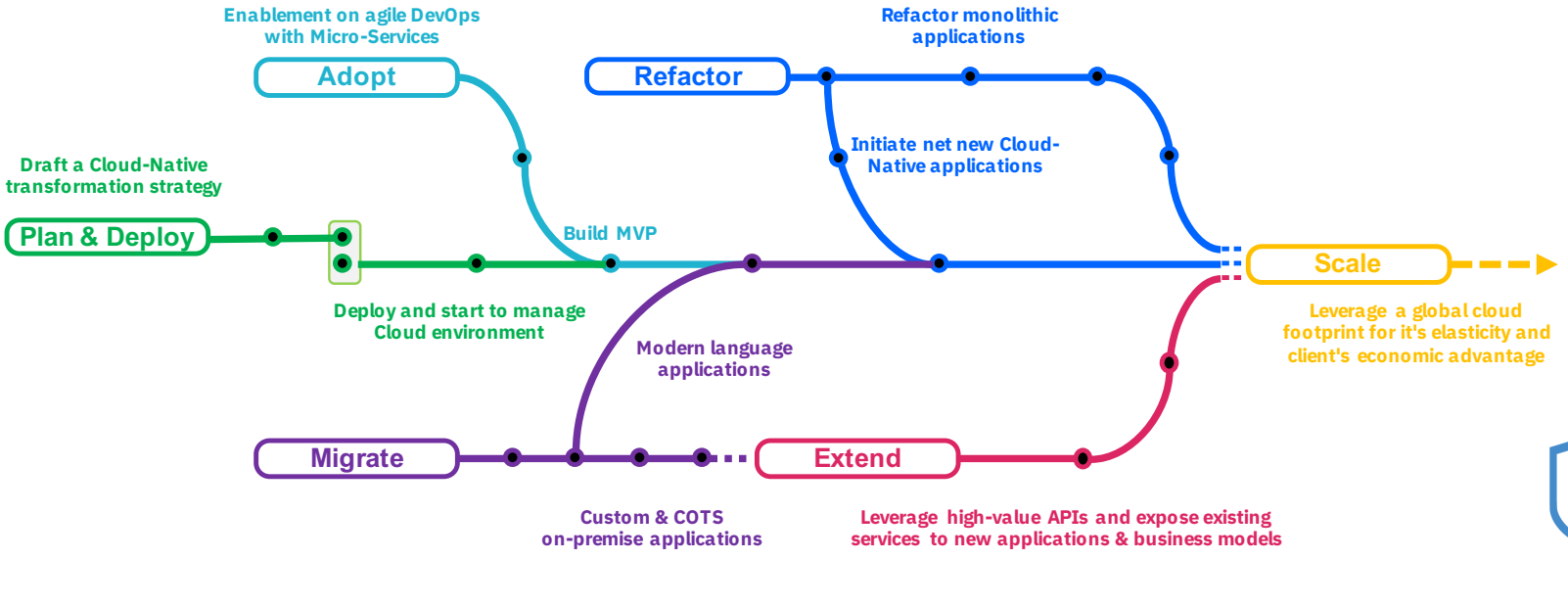
Business Continuity / Disaster Recovery

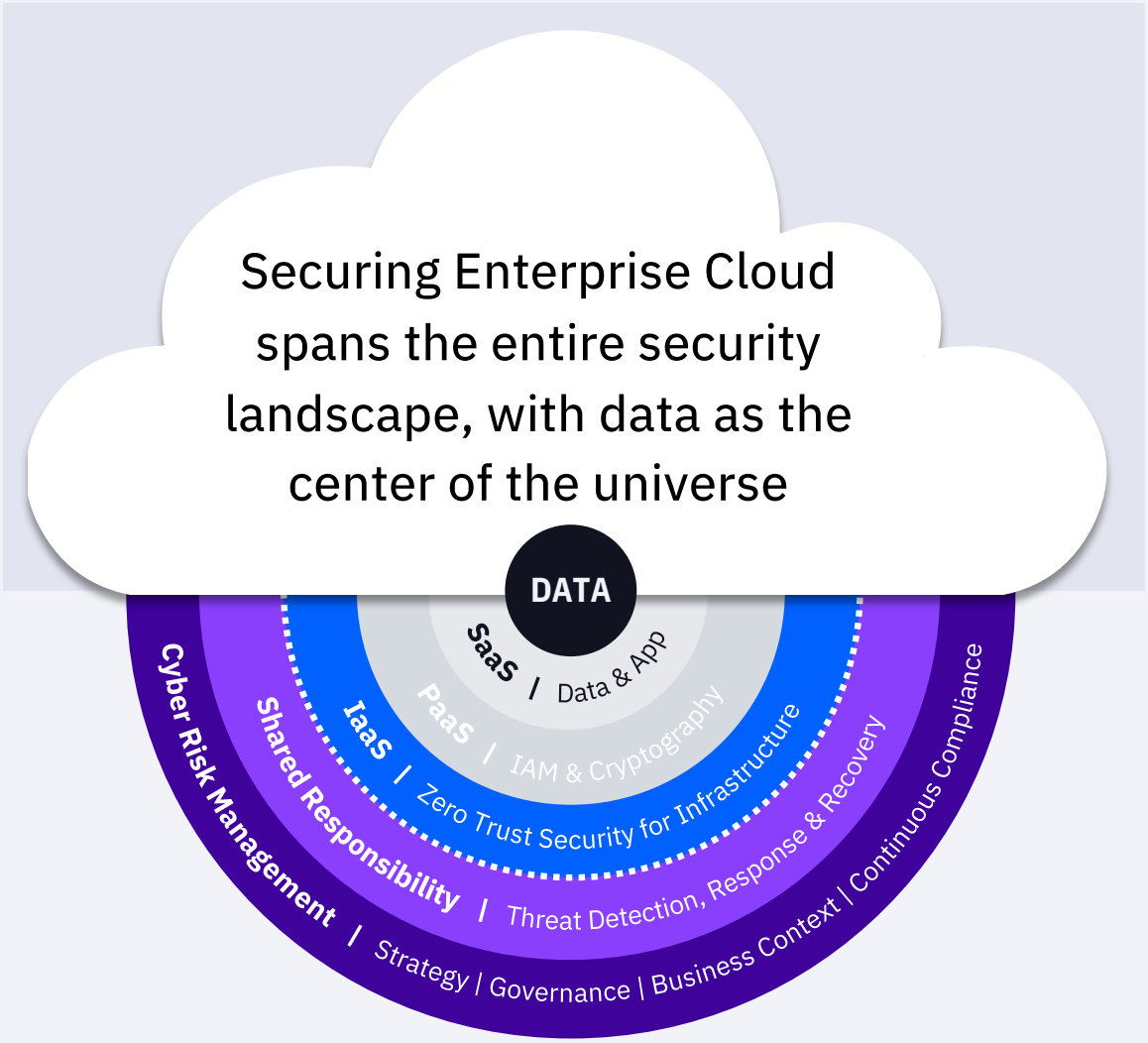
Cloud Journey



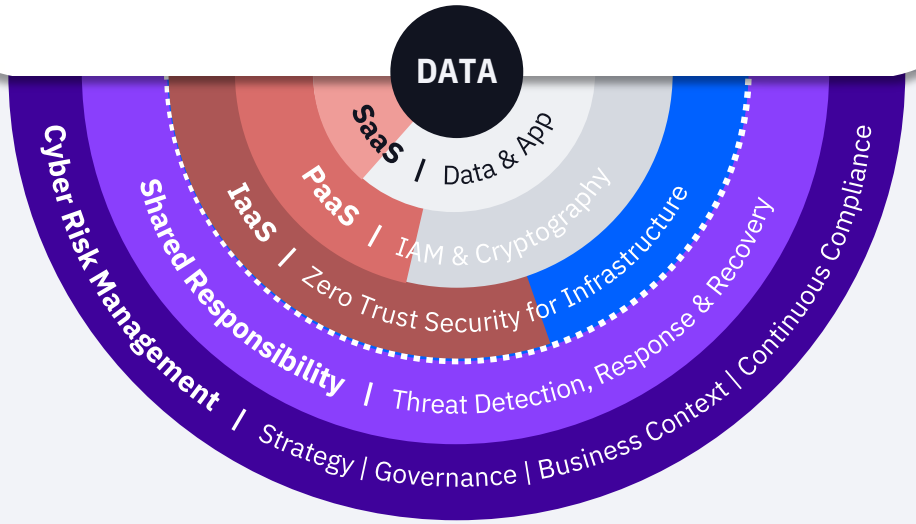
Cloud Journey

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




Securing Enterprise Cloud spans the entire security landscape, with data as the center of the universe
DATA
SaaS / Data & App
PaaS / IAM & Cryptography
IaaS / Zero Trust Security for Infrastructure
Shared Responsibility / Threat Detection, Response & Recovery
Cyber Risk Management / Strategy | Governance | Business Context | Continuous Compliance

Native security controls are helpful but not sufficient, especially across multiple clouds or hybrid environments



Cloud Native Capabilities

How can I integrate my native security tools into my overall security operations?

How do I centrally manage policy across my on-premise and cloud environments?

What are my security responsibilities vs. my Cloud Service Provider's?

How do I develop cloud applications that are secure by design?

How do I secure my critical data on cloud?

How do I secure access to my cloud workloads?

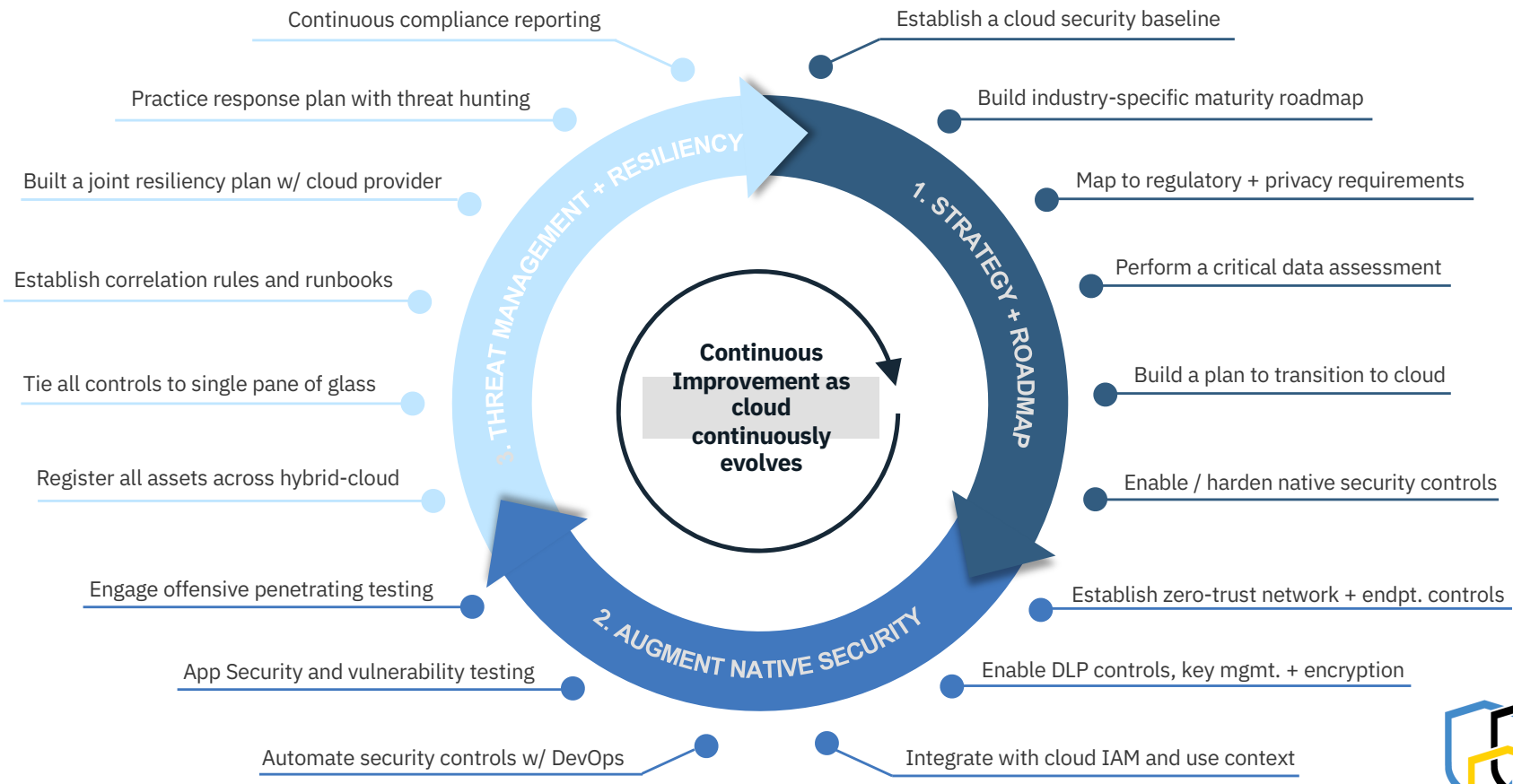
How can I get visibility into and manage Shadow IT usage?

How do I keep up with changing compliance regulations?

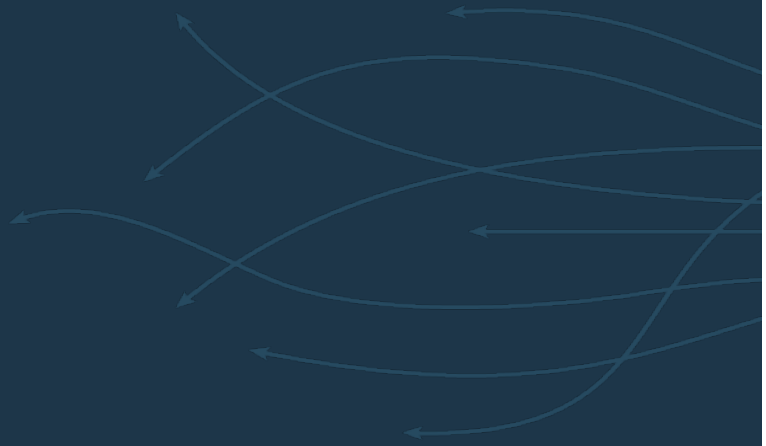
How can I ensure my native security tools are properly configured?

How can I apply security without impacting the speed of business innovation?

A programmatic approach to securing the hybrid enterprise



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

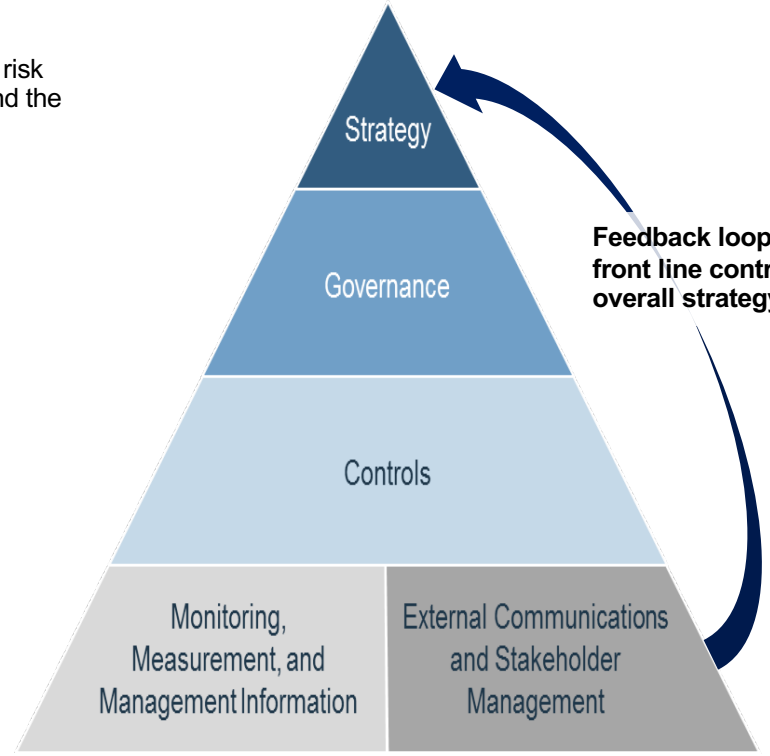
CONTROLS

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



GOVERNANCE

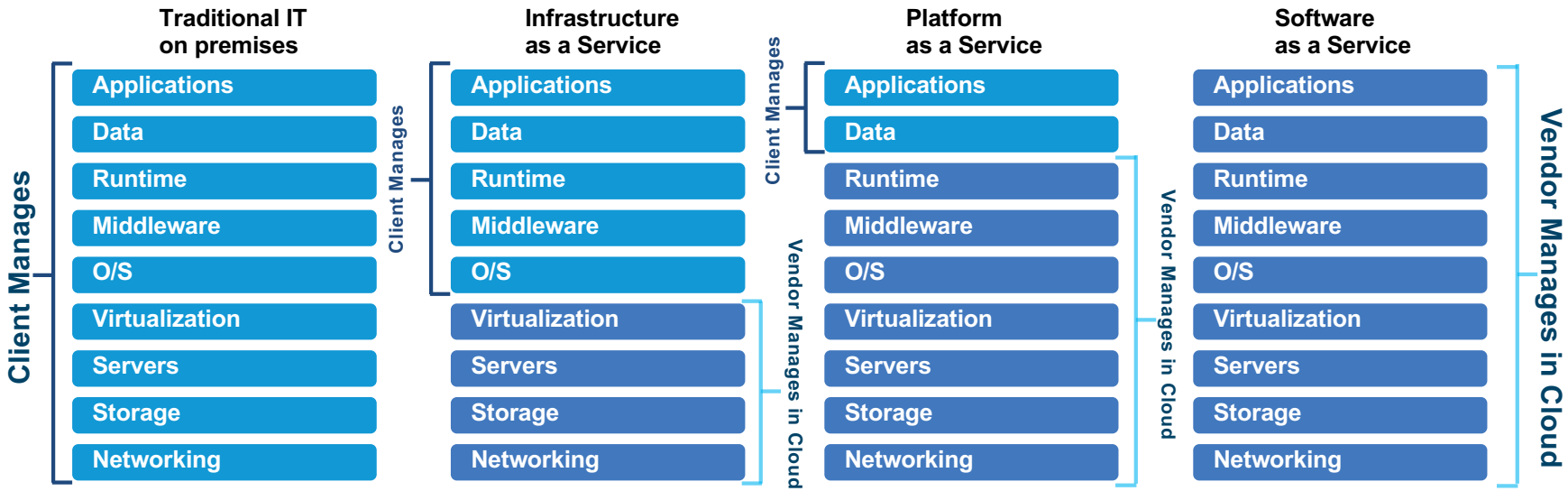
Define organizational roles and responsibilities, policy framework and arrangements for oversight of the risk profile and risk management framework

Feedback loop – from front line controls to overall strategy

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



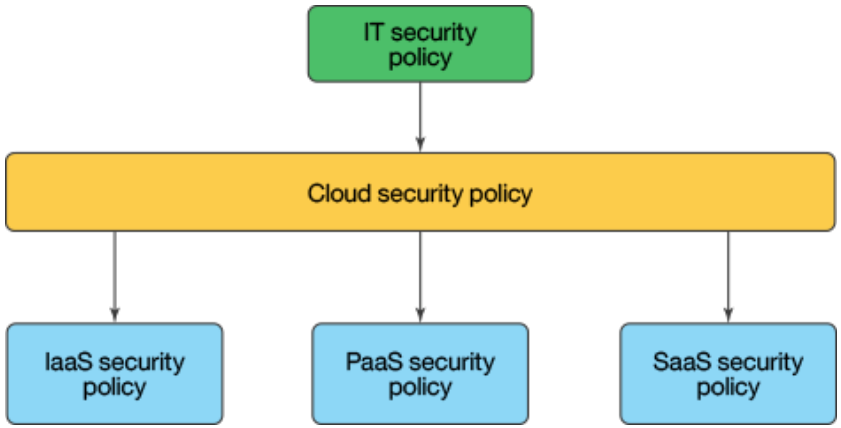
Integration of Roles, Processes, Information, and Technology covers the new cloud models needing additional service management

Additional Service Management Needed

Provided by Cloud Provider

Steps to Develop a Cloud Security Strategy

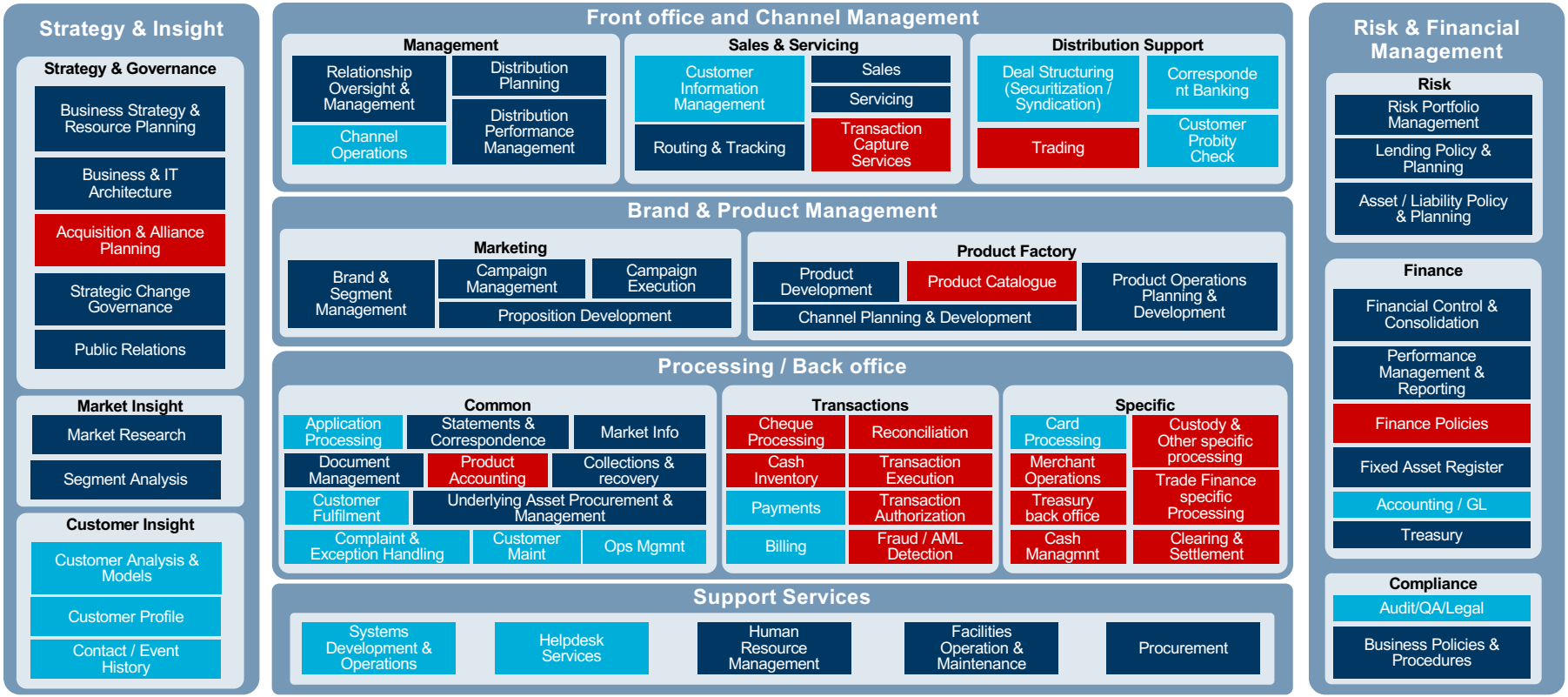
- Evaluate Security Governance / Organization
  - Cloud Security Governance Models
  - Organization design
  - DevOps



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 2019



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

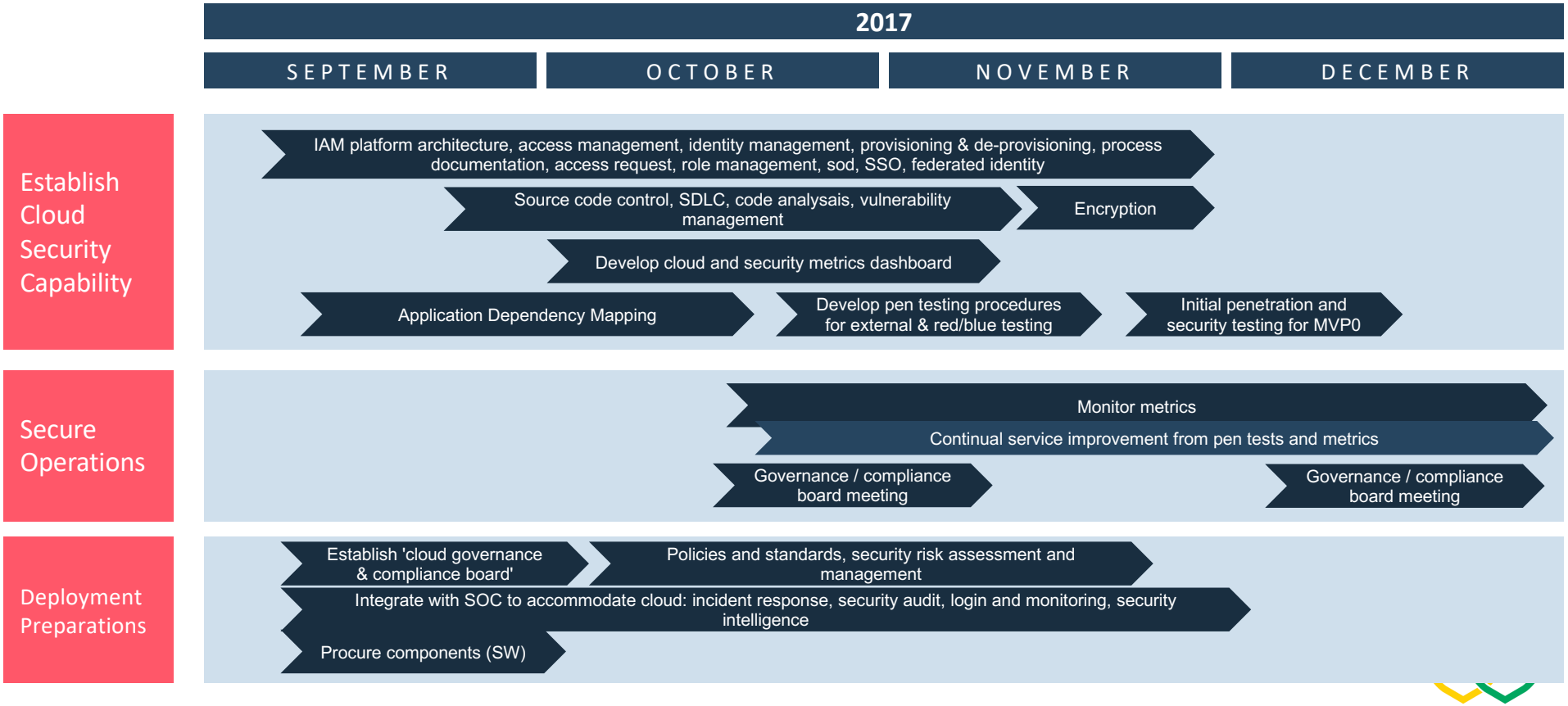
Maturity Level Expectations By Tier

		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

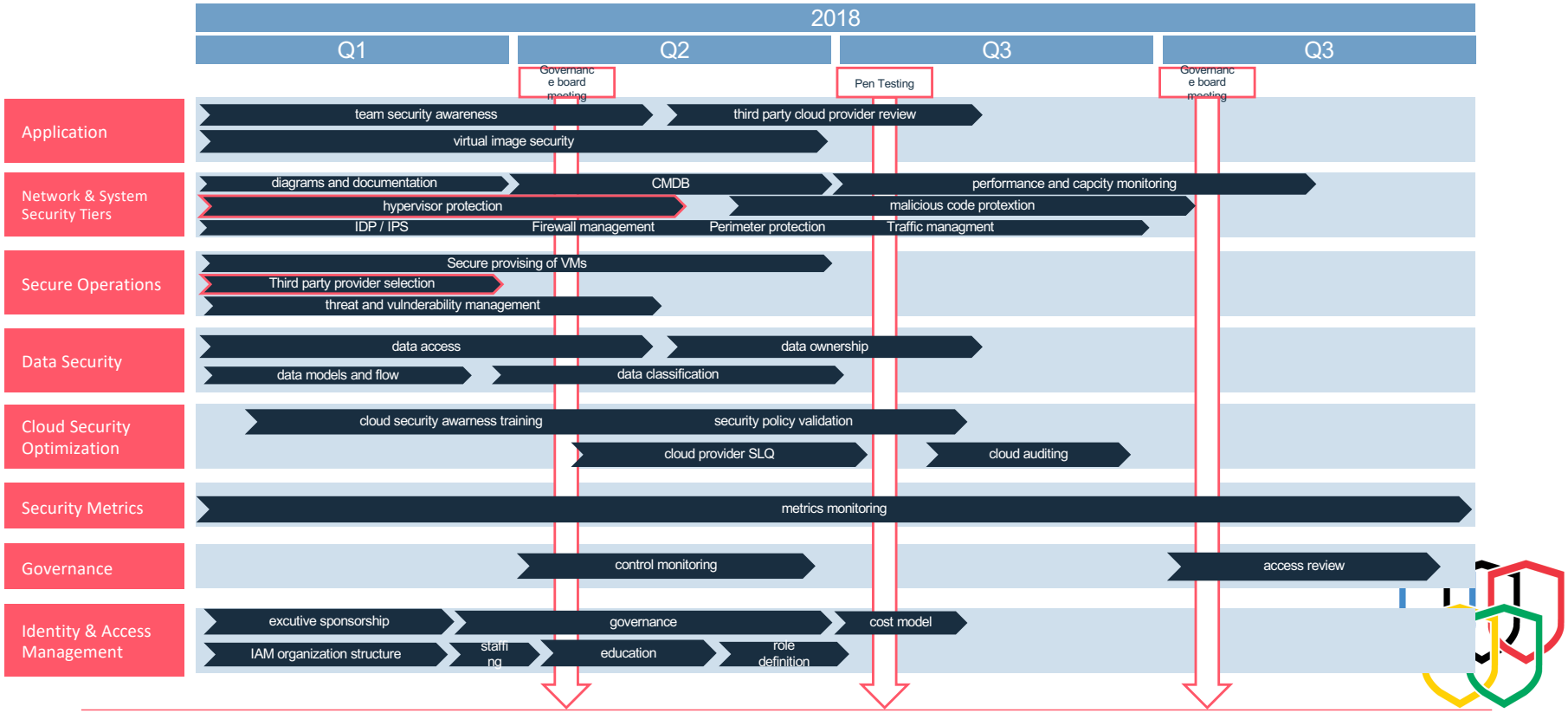
Setting up a hybrid cloud from zero to MVP



ROADMAP EXAMPLE

Year 1 after cloud establishment.

SECURITY & COMPLIANCE ROADMAP FOR T1



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.