POLICIES AND REGULATIONS FOR THE DIGITAL DISCOM

Narayana Birakayala

Capture Business Development Lead - India

Worldwide Public Sector

A new era and a new model for Power & Utilities

ACHIEVE
operational efficiency and excellence.

IMPROVE
your security and compliance posture.

REDUCE
time to business insights.

BUILD
innovative applications fast.

aws

Disruption is Much Easier Today

ENGIE	enel	centrica	TALEN ENERGY
Digital transformation to IoT	Datacenter migration for savings, agility and speed	On-premise datacenter to cloud to IoT for connected home & DER	Cloud transformation with NERC and FERC compliance

This is something "born in the cloud" companies have already discovered

aws

Cloud paves the way for **disruptive innovation.**

Evolution Of Cloud Adoption
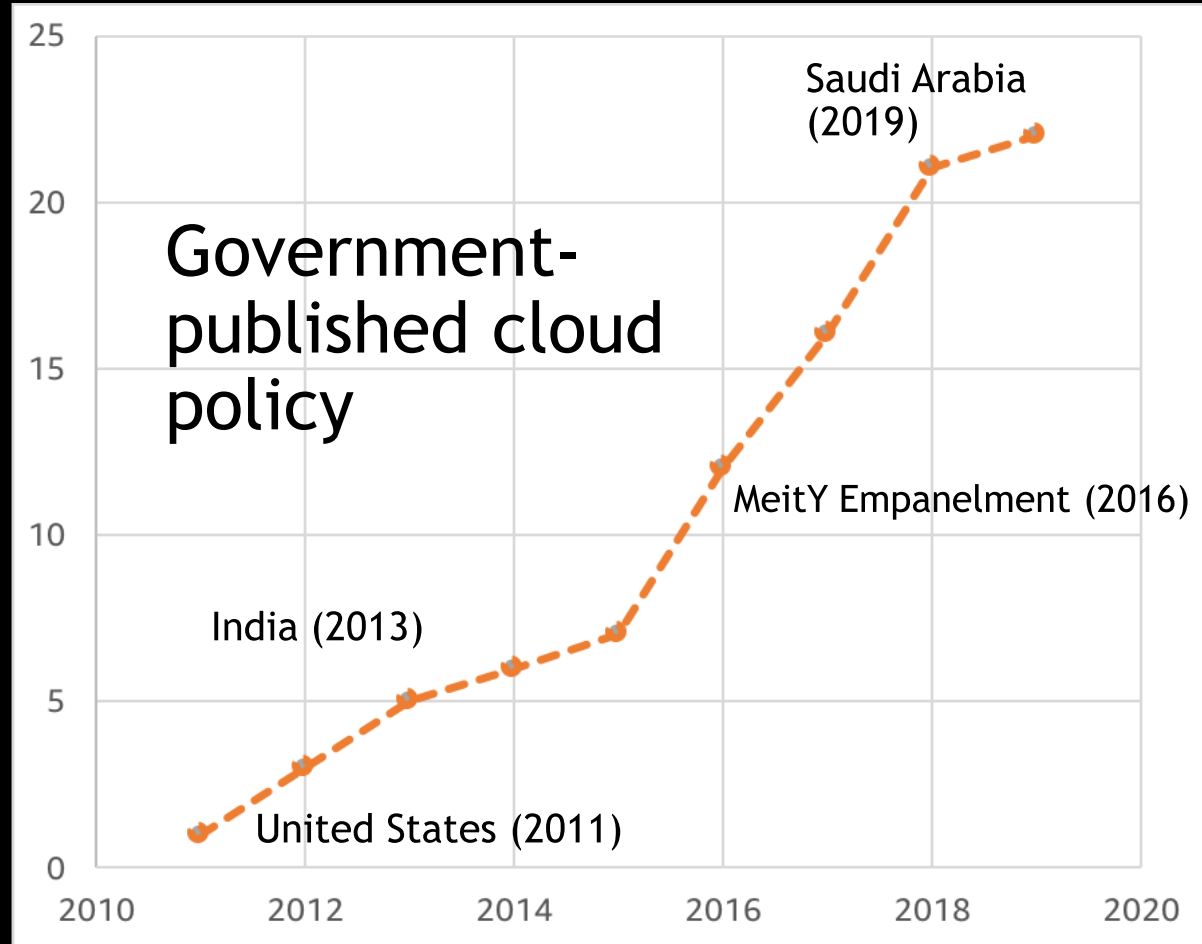
Broad Adoption

Skills and Culture

Acquisition/Procurement

Security & Compliance

Policy

Definition

aws

Cloud first, cloud by default, and cloud native

Government-published cloud policy

Saudi Arabia (2019)

MeitY Empanelment (2016)

India (2013)

United States (2011)

UK's Cloud First Policy

"When procuring new or existing services, public sector organisations should consider and fully evaluate potential cloud solutions first before considering any other option."

aws

Cloud Policies in India

"The Government is mandating all departments to deploy their existing or new applications on Cloud except Top Secret and Secret."

Government of Telangana (2020)

"All Government organizations must use cloud infrastructure services instead of using Government owned datacentres or data centres owned by the organization or co-locating their infrastructure in any Government owned/ privately owned data centre. Procurement of new hardware in existing data centres should be strictly avoided.."
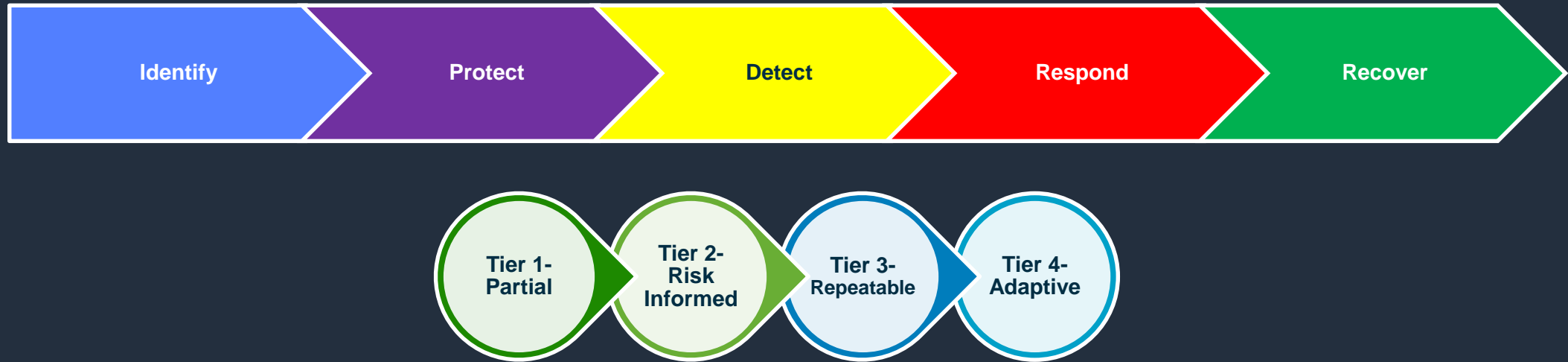
Government of Maharashtra (2018)

"Government departments at the Centre and States to first evaluate the option of using the GI Cloud for implementation of all new projects funded by the government. Existing applications, services and projects may be evaluated to assess whether they should migrate to the GI Cloud.""

MeghRaj Cloud Policy,
Ministry of Electronics and Information Technology (2013)

aws

NIST Cybersecurity Framework

CSF offers a simple-yet-effective risk-based, outcome-focused framework to enable organizations to address cybersecurity risks consistent with their business and mission needs

| Identify | Protect | Detect | Respond | Recover |

Tier 1- Partial → Tier 2- Risk Informed → Tier 3- Repeatable → Tier 4- Adaptive

A voluntary framework, originally intended for critical infrastructure, comprised of best practices to help organizations of any size and in any sector improve the cybersecurity, risk management, and resilience of their systems

aws

From Statements of Intent to Meaningful Action...

✓ Cloud First Policy for Utilities
✓ Data Classification & Security Standards
✓ Procurement Policies – Cloud Aligned
✓ CSP Empanelment – Ease of Procurement

Thank You

AWS
Cloud
Services