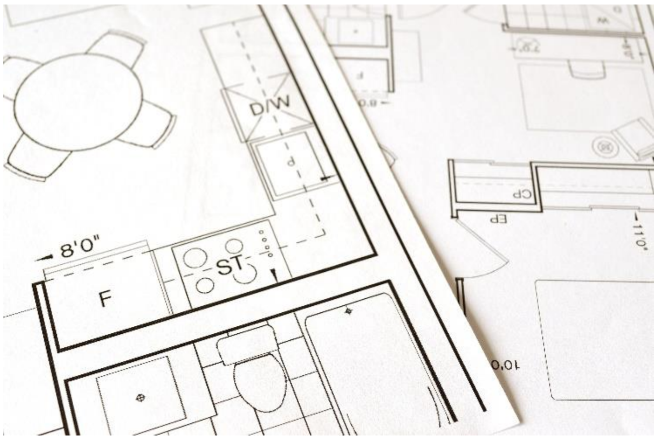
Transforming Governments with IBM and AWS

Governments are on their digital transformation journey nowadays, understanding the value of technology making it an indispensable consideration in their vision and strategy. Cloud plays an imperative role in their IT strategy which could make them competitive to others already enjoying its blessings. It is not a straightforward path for any government institute as they plan for their cloud strategy. There are several pillars they must ponder deep before their decision-making compares to other sectors. This assessment is certainly of an extremely high standard as the workloads can carry the entire country's or sector's data. Cloud providers supporting these workloads must have passed all the required compliance and standards.

AWS offers a set of services that can support highly sensitive and regulated government workloads. Government workloads explicitly demand comprehensive security, isolation of the workloads, compliance with the regulated standards and frameworks, and Hybrid Cloud architecture. AWS services have achieved the Global, Regional, and even country-level compliance certification to make it a government ready cloud platform. Taking further steps towards more agile Governments requires legacy workloads modernization to cloud-native distributed microservices architecture. This blog will provide a brief understanding of how AWS capabilities can support specifically the government workloads demands.

AWS GovCloud (US) regions allow the government customers and their partners to build secure cloud solutions that comply with FedRAMP's high baseline, CJIS, ITAR, EAR, DOD-SRG, FIPS 140-2, IRS-1075. These regions are operated by the employees who are U.S. citizens on U.S. soil. These regions meet all the compliance mandates, safeguard sensitive data, strengthen the Identity management, improve cloud visibility, and provides enhanced protection to accounts and workloads.

Cloud Native Architecture



Governments cannot get the entire benefits of the cloud without using serverless technology, containers, and microservices. These are fast-emerging industry standards allowing to move, build, and manage the distributed microservices architecture.

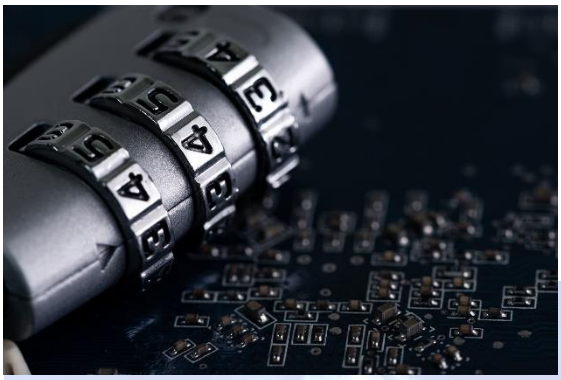
Microservices belong to a type of architecture in which applications are split into component pieces, each of which performs a specific fine-grained function. Microservices run inside containers, which include everything a microservice needs to run, such as code, dependencies, and libraries. Containers provide optimal portability across cloud and on-premises environments. Serverless services help to focus on application development than underlying infrastructure management. Container platforms provide a system for automating deployment, scaling, and management of containerized applications.

Many Government applications are still essentially monoliths. Agencies should try to identify applications where microservices could be used to improve performance. In these cases, the application should be incrementally broken down into smaller deployable components. The target runtime for these components could be a vendor-proprietary container platform or Managed Kubernetes or a Serverless Functions or Serverless platform built for running containers. These platforms should have smooth integration with all the native cloud services.

AWS has a rich set of services that can help government application workloads to move, build, manage smoothly in a cloud environment. AWS ECS is a proprietary AWS Container Platform that can be used for building cloud Native Microservices Architecture. AWS also supports the highly appreciated Kubernetes platform in developer's community as a managed offering called as 'Elastic Kubernetes Service (EKS)'. If the Government agencies find the serverless as one of the productive platforms, the choices are AWS Lambda and AWS

Fargate. With AWS Lambda, the required application code can be natively run in AWS and it supports most of the modern programming languages. AWS Fargate supports running containers natively without bothering about the underlying containers platform.

Security and Compliance



Security and Compliance are the first-class citizens for the Government workloads. While migrating or building new government workloads, the security and compliance to government norms are of the highest priority. AWS Provides a rich set of tooling, meeting the workloads security and compliance requirements such as AWS KMS for Data encryption key management service, AWS KMS also allows the customer-managed key or customer-supplied key for higher control on the key management to strengthen the encryption in the cloud. The data in AWS is always encrypted when it is at rest adhering to the best configuration practices provided by AWS. Data in transit can also be encrypted using the TLS encryption where AWS Certificate Manager can help to do that. Network security for the government workloads can be achieved with a set of AWS services such as AWS Virtual Private Cloud (VPC), Security Groups (SGs) and Network Access Control Lists (NACLs), Web Application Firewall (WAF), AWS Shield.

Government workloads are highly compliant workloads. The AWS Compliance Program helps customers to understand the robust controls in place at AWS to maintain security and compliance in the cloud. AWS's achieved Global, Regional, and country-specific compliance certifications in security, Data Protection, Payments Card Industry, Government Data Standards, Protected Health information-HIPPA, GDPR, etc provides confidence for migrating or building Governments workloads in the cloud.

Isolation of the Government workloads can be achieved with the AWS VPCs private subnets and public subnets configuration. With demilitarized zones implementation on AWS, the Government's workloads can be separated from the external world. The external facing services for internet access can be hosted in public subnets. Backend services, databases can be hosted in private subnet with no internet access. Further, multiple layers of security, including security groups and network access control lists can help control access to Amazon EC2 instances in each subnet.

Hybrid Cloud

Hybrid architecture is a reality for Government workloads where public cloud is integrated with on premises with a single control plane. There are plenty of factors why Government workloads are more likely to fall under this architecture. Few of them are Government regulatory requirements for data residency, highly latency sensitive workloads which cannot be moved to the cloud, Local data processing, modernization of highly integrated enterprise workloads.

AWS Outposts can help to realise Hybrid Cloud architecture to integrate on-premises and cloud operations. It supports a broad spectrum of use cases using a common set of cloud services, tools, and APIs across on-premises and cloud environments. There are plenty of services currently AWS outposts are providing including AWS ECS and EKS for Government's Modernized container workloads, Amazon EMR for data processing and analytics, Amazon RDS for database workloads, Amazon S3 for storage needs. The operational needs can also be served by AWS CloudFormation, Amazon CloudWatch, AWS CloudTrail, Cloud 9.

As there are many more AWS services likely to be released on Outposts, it becomes a choice of Hybrid platform where Governments can initiate their modernization efforts. It provides the seamless experience across the cloud workloads whether those are running in AWS public cloud or on Outposts in Government datacentres adhering to the imperative security and compliance regulations and frameworks.

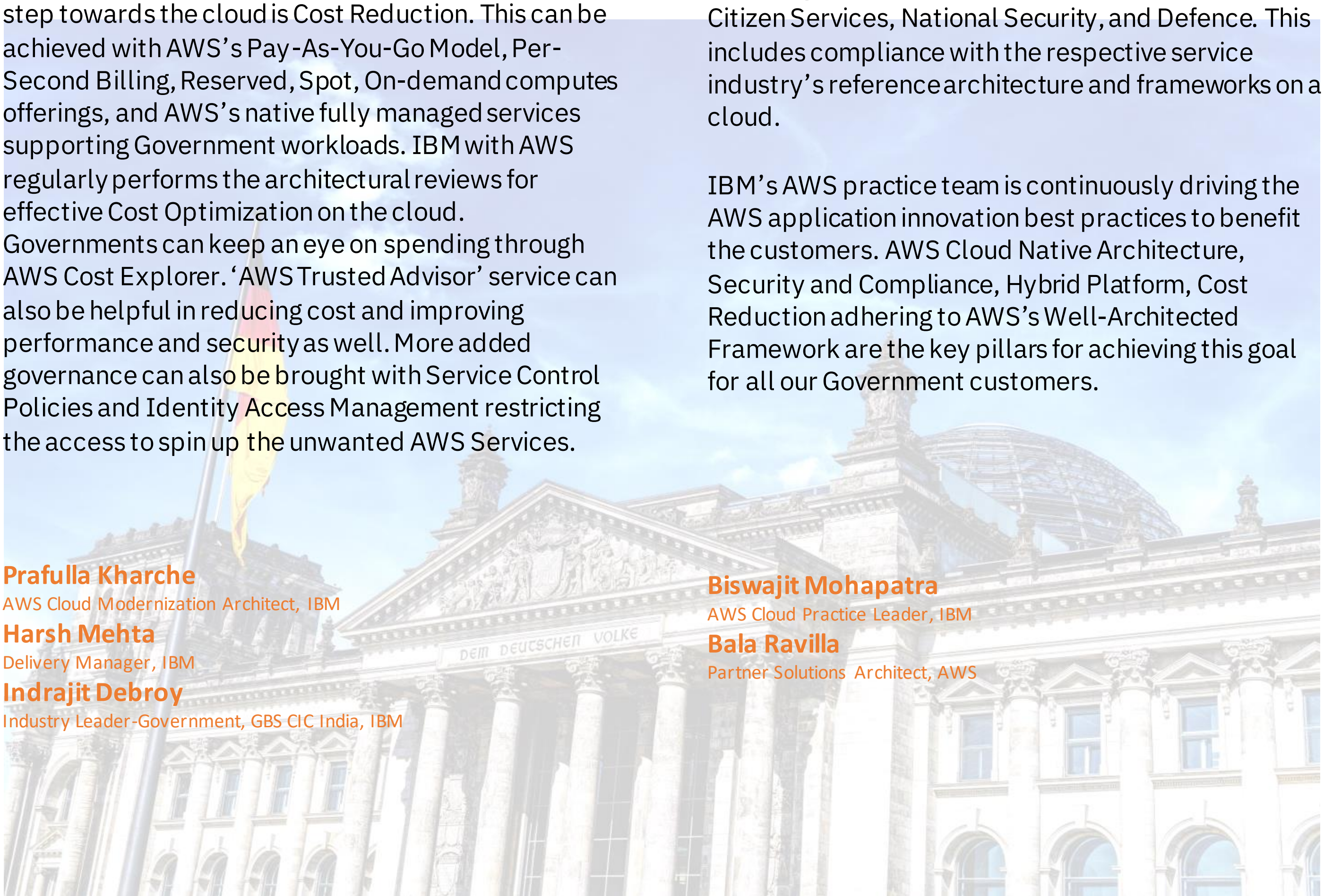
Cost Reduction

One of the business drivers for Governments to take a step towards the cloud is Cost Reduction. This can be achieved with AWS's Pay-As-You-Go Model, Per-Second Billing, Reserved, Spot, On-demand computes offerings, and AWS's native fully managed services supporting Government workloads. IBM with AWS regularly performs the architectural reviews for effective Cost Optimization on the cloud. Governments can keep an eye on spending through AWS Cost Explorer. 'AWS Trusted Advisor' service can also be helpful in reducing cost and improving performance and security as well. More added governance can also be brought with Service Control Policies and Identity Access Management restricting the access to spin up the unwanted AWS Services.

IBM Global Services and AWS are committed to migrate, modernize, build, and manage the Government workloads. IBM services with the AWS experts and Thought Leaders drive the Government digital journey from strategy to implementation and operations. IBM GBS's Government Leaders with more than decades of domain expertise are committed to make Government's AWS cloud journey as smooth as possible.

There are several Government service industries where IBM is driving the AWS modernization efforts including Healthcare, Financial and Fiscal Affairs, Citizen Services, National Security, and Defence. This includes compliance with the respective service industry's reference architecture and frameworks on a cloud.

IBM's AWS practice team is continuously driving the AWS application innovation best practices to benefit the customers. AWS Cloud Native Architecture, Security and Compliance, Hybrid Platform, Cost Reduction adhering to AWS's Well-Architected Framework are the key pillars for achieving this goal for all our Government customers.



Prafulla Kharche
AWS Cloud Modernization Architect, IBM

Harsh Mehta
Delivery Manager, IBM

Indrajit Debroy
Industry Leader-Government, GBS CIC India, IBM

Biswajit Mohapatra
AWS Cloud Practice Leader, IBM

Bala Ravilla
Partner Solutions Architect, AWS