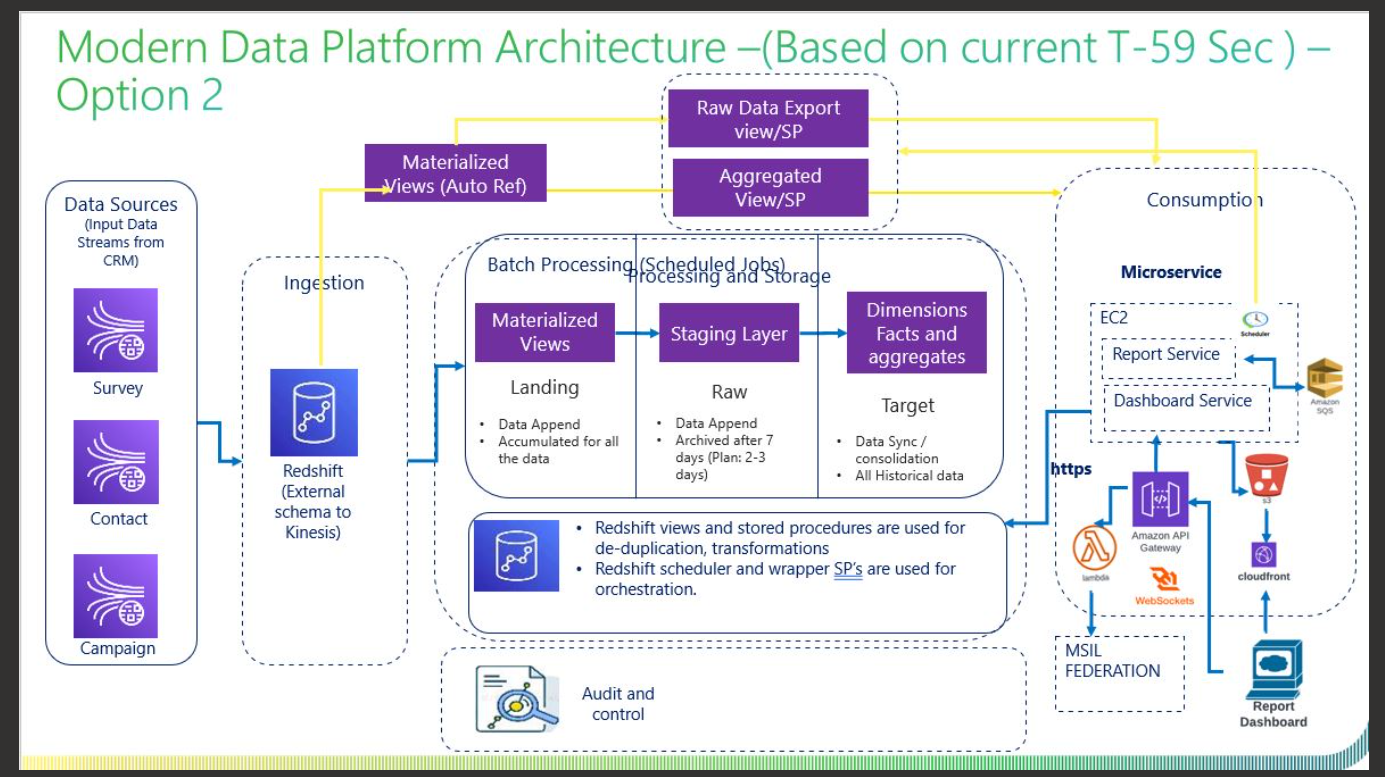
**DEVOPS PROPOSAL FOR MSIL-MDPA**

## Deployment Architecture



## AWS Infrastructure

**Terraform**

Terraform is being proposed for the IaaS.

Or

**AWS Services**

AWS Cloud Formation template will also be used for configuring and provisioning the required infrastructure.

**Infrastructure and Application Monitoring**

The application and infrastructure monitoring are being monitored using the CloudWatch

## AWS Governance

**Authentication & Authorization**:

Authentication mechanism will be enabled for the validation of the user identity validation across with the domain users configured. IAM primary focus is with the access & the permission.

**Authorization**

Access rights for the individuals are configured for the controlling of the access across the resources /services in the AWS cloud. Not every user will have access to every application. The isolation of the access will be done through the Identity & Access management.

AWS Standard practices will be performed so that the project and the BU across the region are handled only by the respective projects.

**IAM:**

We can centrally manage users, security credentials such as access keys, and permissions that control which resources users can access. Using IAM

**Users** can access the assigned resources through the permission configured through the policies.

**Groups**: A group is being configured with the common group policies so that any policy applied are immediately traversed across all users in the group. The groups are customized for each project specific. This is customized based on the need of the requirement given.

Roles are configured for the complete isolation of the independent projects. Roles are not configured with any users however they can be intake or consumed by the authorized users. Different roles will be configured for the project specific execution.

**Policies:**

Policies are the one of the important key factors to maintain the roles and the permission across the cloud.

Policies are AWS objects attached to the users, groups, resources to define the permission that needs to be granted for accessing across the cloud.   
AWS policies in specific the following will be configured for the platform:

* Access Control
* Identity
* Resource level permission
* Service control policies
* Access control List
* Session Policies

Privilege Admin access will be configured so that the template layout, formation of the Cloud Formation Template of the services across the platform, validation of the users account and unique Id creation for the project, settings up the policies applied across the board.

## DevOps CI/CD Pipeline

Different pipelines are going to be configured with all the requirement stages for WebApp, Platform API and DB deployment.

The following are the steps execution as part of the Jenkins pipelines:

Checkout: This stage checks out the code from the specified Git repository and branch.  
Build: This stage installs the required packages and builds the application.  
Deploy: This stage deploys the built app to the specified AWS resourses.

The AWS block is used in the pipelines to configure the AWS credentials and region which will allow the Jenkins to deploy the required parameters.