DATA GOVERNANCE

The ask

Example Corp now has a number of development and test workloads in AWS. Many of these workloads make use of data storage services such as Amazon RDS and Amazon S3. The customer has recently established a dedicated data governance team, who have been tasked with identifying controls for workloads that process data classified as confidential or internal-use only.

The data governance team has recently issued guidelines around the use of encryption for data at rest and in transit in the cloud. We have below an excerpt from the data governance standard:

> 3.1.1 All cloud data storage systems must be configured to support encryption at rest and in transit using industry supported encryption algorithms for data classified as Confidential, or Internal-Use only. For a list of approved encryption algorithms and key-lengths please see Appendix A.

From these guidelines there are two new requirements:

- The data governance team at Example Corp wants to get visibility into resources where encryption at rest is not being used
- The team wants to use AWS Service Catalog to make it easy for development teams to comply with the encryption-at-rest requirement, without having to set it up themselves.

These requirements will shape the work that goes into building additional data governance controls as development teams look to use additional AWS services to store production or material data.

The plan

We are going to create and deploy a data governance control using an AWS Config managed rule to ensure the teams are using encryption when creating an RDS instance. We will then create a self service Service Catalog product so the teams can create compliant resources.

- Create the control
- Provision the control
- Create the product

Note

If you need help at any time please raise your hand.