Update Azure Guardrails Policy

Tester	Reviewer

Overview

- The Guardrails are broken down into three initiatives (aka policy sets). *Full Guardrails* is applied to Prod and non-prod and is the most restrictive. *Reduced Guardrails* enforces a subset of these to be used in POV and Sandbox. *Shared Guardrails* is for shared services where some restrictions are required but others (such as Public IPs and non-BHP VM images) are permitted.
- Custom policies are defined in custom.tf and references to built in policies are found in data.tf.
- The policies are gathered together as initiatives in guardrails.tf, they are then assigned to management groups in assignments.tf.
- The dev branch is long-lived and triggers the Terraform Cloud workspace **azure-guardrails-dev**. This applies to the management group structure under **root-mg-dev**.
- The master branch triggers the Terraform Cloud workspace **azure-guardrails**. This applies to the management group structure under **root-mg**

Platform:	**Azure**
Owner of this SOP:	@ Rob Excell
Cloud Operations Representative:	@ Derek Sherin

Problem

- When requesters are updating Azure policies for specific resources. After provisioning the infrastructure, we can use the Guardrails' pipeline we used to provision the resources to update the policies. It will not destroy the existing configuration, rather update the *tags*.

Solution

1. Find the provider name as per Guardrails policy request.
2. Validate the existing policy code (policy.yaml · dev · bhp-cloudfactory / azure-foundations / azure-guardrails · GitLab)
3. Create a new branch based on master branch and add the changes as mentioned above.
4. Merge code from your branch to dev branch. Delete source branch.
5. It will trigger the dev pipeline, which will apply the policies to the management group structure under **root-mg-dev**.
6. Refer the logs in Terraform Cloud workspace **azure-guardrails-dev**.
7. Once validated, for NON-EXEMPTION alterations (Exemptions can be done under a service request alone), create a ServiceNow change based on CHG0146432. Merge request to master branch. (Do not delete dev branch as it is long-lived)
8. Merging the code in master will trigger master pipeline, which will deploy the policies to the management group structure under **root-mg**.
9. Refer to the logs in Terraform Cloud workspace **azure-guardrails**.
10. Ensure the services endorsed in Gitlab Guardrails repo https://gitlab.com/bhp-cloudfactory/azure-foundations/azure-guardrails/-/blob/master/policy.yaml#L26 are mentioned in the Guardrails documentation on SharePoint