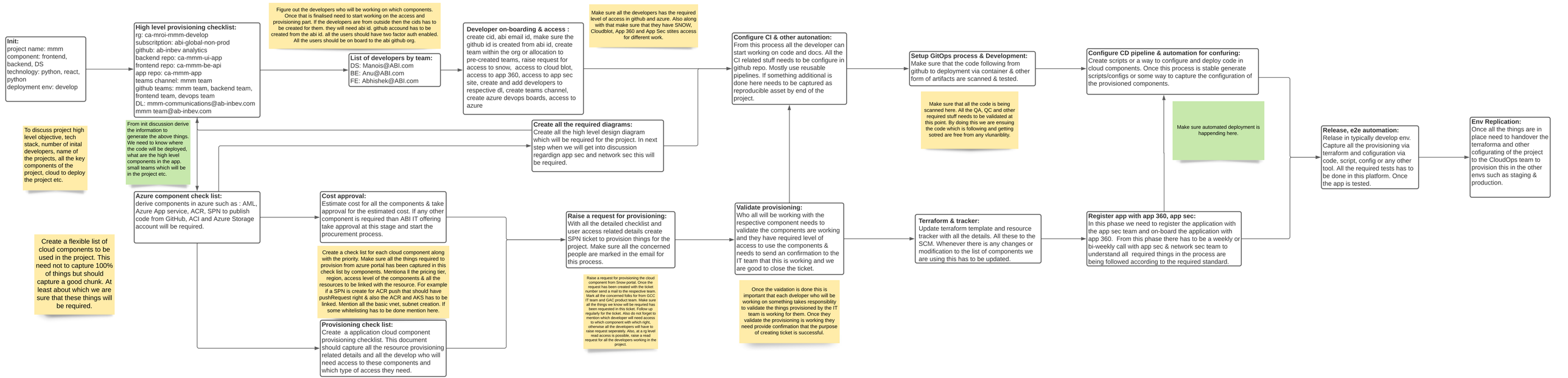
Init:
project name: mmm
component: frontend, backend, DS
technology: python, react, python
deployment env: develop
High level provisioning checklist:
rg: ca-mroi-mmm-develop
subscritption: abi-global-non-prod
github: ab-inbev analytics
backend repo: ca-mmm-ui-app
frontend repo: ca-mmm-be-api
app repo: ca-mmm-app
teams channel: mmm team
github teams: mmm team, backend team, frontend team, devops team
DL: mmm-communications@ab-inbev.com
mmm team@ab-inbev.com
Figure out the developers who will be working on which components. Once that is finalised need to start working on the access and provisioning part. If the developers are from outside then the cids has to be created for them. they will need abi id. github accound has to be created from the abi id. all the users should have two factor auth enabled. All the users should be on board to the abi github org.
List of developers by team:
DS: Manois@ABI.com
BE: Anu@ABI.com
FE: Abhishek@ABI.com
Developer on-boarding & access :
create cid, abi email id, make sure the github id is created from abi id, create team within the org or allocation to pre-created teams, raise request for access to snow, access to cloud blot, access to app 360, access to app sec site, create and add developers to respective dl, create teams channel, create azure devops boards, access to azure
Make sure all the developers has the required level of access in github and azure. Also along with that make sure that they have SNOW, Cloudblot, App 360 and App Sec stites access for different work.
Configure CI & other autonation:
From this process all the developer can start working on code and docs. All the CI related stuff needs to be configure in github repo. Mostly use reusable pipelines. If something additional is done here needs to be captured as reproducible asset by end of the project.
Setup GitOps process & Development:
Make sure that the code following from github to deployment via container & other form of artifacts are scanned & tested.
Make sure that all the code is being scanned here. All the QA, QC and other required stuff needs to be validated at this point. By doing this we are ensuing the code which is following and getting sotred are free from any vlunaribility.
Configure CD pipeline & automation for confuring:
Create scripts or a way to configure and deploy code in cloud components. Once this process is stable generate scripts/configs or some way to capture the configuration of the provisioned components.
Make sure automated deployment is happending here.
Release, e2e automation:
Relase in typically develop env. Capture all the provisioning via terraform and cofiguration via code, script, config or any other tool. All the required tests has to be done in this platform. Once the app is tested.
Env Replication:
Once all the things are in place need to handover the terraforma and other cofigurating of the project to the CloudOps team to provision this in the other envs such as staging & production.
To discuss project high level objective, tech stack, number of inital developers, name of the projects, all the key components of the project, cloud to deploy the project etc.
From init discussion derive the information to generate the above things. We need to know where the code will be deployed, what are the high level components in the app. small teams which will be in the project etc.
Create all the required diagrams:
Create all the high level design diagram which will be required for the project. In next step when we will get into discussion regardign app sec and network sec this will be required.
Azure component check list:
derive components in azure such as : AML, Azure App service, ACR, SPN to publish code from GitHub, ACI and Azure Storage account will be required.
Create a flexible list of cloud components to be used in the project. This need not to capture 100% of things but should capture a good chunk. At least about which we are sure that these things will be required.
Cost approval:
Estimate cost for all the components & take approval for the estimated cost. If any other component is required than ABI IT offering take approval at this stage and start the procurement process.
Create a check list for each cloud component along with the priority. Make sure all the things required to provision from azure portal has been captured in this check list by components. Mentiona ll the pricing tier, region, access level of the components & all the resources to be linked with the resource. For example if a SPN is create for ACR push that should have pushRequest right & also the ACR and AKS has to be linked. Mention all the basic vnet, subnet creation. If some whitelisting has to be done mention here.
Provisioning check list:
Create a application cloud component provisioning checklist. This document should capture all the resource provisioning related details and all the develop who will need access to these components and which type of access they need.
Raise a request for provisioning:
With all the detailed checklist and user access related details create SPN ticket to provision things for the project. Make sure all the concerned people are marked in the email for this process.
Raise a request for provisioning the cloud component from Snow portal. Once the request has been created with the ticket number send a mail to the respective team. Mark all the concerned folks for from GCC IT team and GAC product team. Make sure all the things we know will be requried has been requested in this ticket. Follow up regularly for the ticket. Also do not forget to mention which developer will need access to which component with which right, otherwise all the developers will have to raise request seperately. Also, at a rg level read access is possible, raise a read request for all the developers working in the project.
Validate provisioning:
Who all will be working with the respective component needs to validate the components are working and they have required level of access to use the components & needs to send an confirmation to the IT team that this is working and we are good to close the ticket.
Once the vaidation is done this is important that each dveloper who will be working on something takes responsiblity to validate the things provisioned by the IT team is working for them. Once they validate the provisioning is working they need provide confimation that the purpose of creating ticket is successful.
Terraform & tracker:
Update terraform template and resource tracker with all the details. All these to the SCM. Whenever there is any changes or modification to the list of components we are using this has to be updated.
Register app with app 360, app sec:
In this phase we need to register the application with the app sec team and on-board the application with app 360. From this phase there has to be a weekly or bi-weekly call with app sec & network sec team to understand all requried things in the process are being followed according to the required standard.