*This document will attempt to outline a high level overview of what an end-to-end automation flow might look like. In this example, we'll be assuming that the automation workflow is triggered by an end user submitting a request through some form of ticketing system like ServiceNow. An intake form is completed by the end user with required and optional fields available.*

1. *User fills out intake form. Required details:* 
   * *Details necessary to build safe name (appid, region, environment, etc.)*
   * *Groups/users to grant access to the safe*
   * *If safe will be used in automatic secret retrieval with DAP (to select LOBUser to add to safe owners)*
   * *Dual account requirements (for password grouping and platform selection)*
   * *Password rotation interval (for platform selection)*
   * *Details about the account(s) being stored in the safe (for platform selection)*
2. *Automation starts by consuming the intake form*
3. *PVWA REST API call is performed to create the safe (safe name derived from details provided in intake form)*
4. *PVWA REST API call is performed to define safe owners (safe owner groups/users and required ACLs provided in intake form)*
5. *PVWA REST API call is performed to create password objects in safe (details, including platform derived from intake form)*
6. *Automation builds DAP policy for application policy namespace from template and pushes to SCM repo where the root policy is stored (policy template values derived from intake form details)*
7. *CI/CD pipeline for loading the root policy is triggered by webhook in SCM repo*
8. *PVWA REST API call is performed to store service account for management of the application namespace policy are added to the Safe*
9. *Requestor is emailed pertinent details regarding next steps and request is closed in ticketing system*