FedRAMP 20x Pilot Assessment Methodology.

Scoping:

1. Identify the KSIs that are truly reflective of the Vaultes (CSP) unique offering (CSO), which is “GRC tool to manage CSP’s KSI”.
2. Understand the **evolutionary nature of the CSO, this tool will go through multiple iterations (MVP’s)**
3. Understand the high-level authorized boundary elements and security tooling built-in to the ABD.
4. Determine evidence sources (logs, IaC repos, pipeline configs, dashboards, manual, ad hoc screenshots, CSP corporate specific etc.).

Evidence Collection:

1. Evidence should be automated where possible (pipeline outputs, webhooks, protected API endpoints, scripts, machine-readable reports).
2. Reviewed the logic embedded within Azure PowerShell cmdlets (command-lets).
3. Ensure that the cmdlets variables are binding to the appropriate Azure Service and/or assets to meet the core requirements of each KSI’s.

Validation:

1. Run the JSON output from the PowerShell, analyze the JSON response (key value pair) to ensure that the output meets the intent (scope, rigor and requirements) of the associated KSI’s.
2. Ideally in the future assessment, we will run this against actual Azure Inventory (more specifically SBOM to account for the entire tech stack (infrastructure plus the application codebase).