GovRAMP Box portal evidence submission.

* Include **date/time stamp** on all documents and screenshots where applicable.
* Description – Include a narrative on how the artifact supports the control requirement(s).
  + For example, AC-2(j)- description and evidence/screenshot supporting a quarterly review for privileged accounts access and an example of an annual review for all other users (non-privileged).
  + Attach as many screenshots needed to support how the control is being met.
  + The same evidence can be uploaded for multiple controls where applicable.

Other forms of documents can be uploaded to the folder as in policies, procedures, scans, etc.

|  |  |
| --- | --- |
| Control ID: RA-05 |  |
| Description:  a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; | *Control Implementation Statement; evidence references* |
| b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:  1. Enumerating platforms, software flaws, and improper configurations;  2. Formatting checklists and test procedures; and  3. Measuring vulnerability impact; |  |
| c. Analyze vulnerability scan reports and results from vulnerability monitoring; |  |
| d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; |  |
| e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and |  |
| f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned. |  |