**Simple Dose Audit #21170**

**SVP’s: Raymond Auger**

**SME’s: Bill Mullins, Gaurav Sachdeva, Padma Ajit**

**POC: Jeanne Willis**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Project Name** | **Project Type** | **Oversight** | **Lead** | **Sub-Lead** | **Staff** |
| 21170 - SimpleDose | Audit | Sarah Kubiak | Michael Bavasso | Seun Mafi | Dan Benner, Daniel Rodrigues, Ashish Joshi |

**Brainstorming**

* Security Administration/User Access = Michael, Dan, Daniel
  + Critical File Access / Privileged Access / User Recertification
    - Not looking at Frontend (or endpoint)
    - Sarah will provide examples from a prior audit \*\*
* Where are these data points or storage located and who has access?
* Where are the key execution files? Libraries, directories…
  + User Provisioning Method (focus on back end process)
  + Is this Oracle with UNIX servers… Who has Root access? (Phil Albert?)
  + Not testing the provision process, only who is making the reviews.
  + How is Periodic Access Review (PAR) performed and who reviews the access for the critical program data files specific to SimpleDose? Critical files and directories
  + What is the Deprovisioning process for critical files, libraries, and directories?
    - What tool is being used for access requests?
  + What are the critical systems files for SimpleDose?• Which users and groups have access to these critical system files?o Program files that allow SimpleDose to functiono Full directory names and fileo List of users and groupso Associated permissionso If there are any new directories being pushed into production in the future, is there a validation process that permissions are accurate from pre-production into production.• What is the user provisioning process for these critical system files?• Is there a revalidation process?• How are these critical system files restricted? What is the security over these CLDs?
* Change Management = Michael, Ashish
  + System Changes (Modifications to SimpleDose critical system files)
  + Are APIs being used?
  + UAT
  + Change Migration (Code Deployment - who can do this) – release mgmt.
  + Defect Mgmt process – managing them/prioritizing them/SLAs/ involving appropriate parties
    - Jenkins tool, Pilot at this point.
    - What timing and types of Emergency changes, frequency of changes
  + Secure Code Review
  + Vulnerability Management
  + ITNow / ServiceNow?
  + Phase I is in scope only!!
    - What types of releases took place?
      * Change tickets, program implementation schedules… Code based on the release
* Application Processing = Michael, Seun
  + Job Scheduling – exceptions/failures.
    - Who controls the job scheduler?
      * Add, Modifies, deletes
    - How is it being monitored?
    - Is there a backout process?
  + What are the automated/key jobs are being used?
  + Is there a UI?
    - Are there any manual components?
* Resiliency = Michael, Ashish
  + Disaster Recovery/Data Backup - surface touch
  + Is there a plan?
  + What is the testing schedule?
    - Risk level of system and data? UCMDB??
    - Tier 2a? What are the RTO/RPO?
      * Check policy
  + Are local backups being scheduled?
  + Who is monitoring the backups?
    - Are there alerts in place for backup failures?
    - Who is notified and what media is being used?
* Where are the backups being restored to?
  + Offsite, local backup…
  + Verify that the same encryption is being used for Prod version.
  + Is there a Hot Site?
* Data Integrity/Validity = Michael, Dan, Daniel
  + Data Accuracy and Completeness
  + Reporting- We might want to look at some of their key reports and check for data accuracy
    - What types of reports are there within SDA?
    - Are there reports which other systems are relied upon?
    - Are the reports monitored?
  + Data Retention Policy – is it being adhered to?
  + What type of data does this system have?
    - What the movement of the data is? What type of data comes into SDA, and what goes downstream?
    - End to end, of the process where the data begins in SDA and what is modified.
  + Understanding what processes are in place to address potential loss of data.
    - Balancing Controls
    - Validation of data - Input editing
* Capacity / Scalability = Michael, Ashish, Seun
  + ~~Migrating data from old to new application during Q1 2021.~~
  + What are the tools being used, load balancing tools?
  + app size for growth (capacity limits) size/space/volume
  + How is the future grown being monitored?
  + Data sync? Is it required?
    - Cardinality??
  + \*\*\*\* Is this system on prem or in the cloud?
  + How many users currently on system?
    - Is CPU being measured?
      * Performance testing. Is P testing done routinely?
      * Who is reviewing the results, KPI reports?
        + Alerts in place?
        + SLA for responding to a potential max??
        + What are the report metrics? Memory, storage, usage…
    - How many are expected?
    - Are there peak processing times?
    - Is there a login estimation of those processing times?