| **#** | **WP Ref** | **Observation** | **Implication / Business Risk** | **Recommendation** | **Management’s Response** |
| --- | --- | --- | --- | --- | --- |
|  | IT260 | **Missing Access Request Documentation**  1 of 15 users selected did not have an access request form with signed approval. | Consistent use of documentation is important in enabling management to monitor the operational effectiveness of controls, especially in the event of attrition or turnover at the administrator position.  If the provisioning administrator were to leave the organization, the request and approval documentation would no longer be available, preventing management from being able to monitor the appropriateness of user access. | Ensure access request forms are used for all access requests. | We will have updated our user access provisioning policy and reviewed it with the APS Administrators, ensuring they are aware that all access requests must be submitted and approved in writing before provisioning new accounts going forward, regardless of the access being requested. |
|  | ITxxx | **Informal Policies & Procedures**  Policies and procedures for user administration and program change management on the Oracle Financials application are not formally documented. | Formal policy and procedure documentation is necessary to capture institutional knowledge, to help ensure that all critical functions of the IT operations are completed, and to help ensure that the Company’s networks and systems are used appropriately by their employees. A lack of documented security standards can lead to inconsistent administration, unclear lines of authority and responsibility for security, and the lack of continuity in the event of staff turnover.  An informal program change management process increases the risk of unauthorized and/or untested changes being migrated to the production environment, which may alter the effectiveness of programmed accounting controls, cause data corruption, or result in systems failure. Additionally, an informal user administration process increases the risk that unauthorized users may access the Oracle application, enter inaccurate financial data, or remove existing data. Any of these effects could cause material errors in the financial statements. | Formally document user administration and program change policies and procedures for Oracle Financials. The documented policies should be distributed to employees responsible for performing the processes.  Also ensure that the policies and procedures provide for the creation and retention of documentation supporting the application of user access and change management controls to aid management in monitoring the effectiveness of their internal control environment on a regular basis. |  |
|  | ITxxx | IT Segregation of Duties Developers and analysts have write-access to the production environment.  There is no formal documentation of change requests, user acceptance, or test results. | A strong System Development Life-Cycle (SDLC) includes steps to ensure that each change is evaluated, authorized by appropriate levels of management, prioritized, and re-prioritized on a regular basis, ensuring IT resources are appropriately allocated.  A strong SDLC also includes steps for adequate levels of testing of program changes in a separate environment before moving them into the production environment, ensuring changes do not have adverse effects to the application and the overall IT environment.  Most importantly, access to the production environment should be restricted to as few, trusted individuals as possible. There should also be a separation of duties between staff that develop changes, and staff with write-access to the production environment.  Each of these steps should be documented to ensure the process is consistently followed and to maintain accountability for those important actions. | Access to production should be limited to ensure that duties are appropriately segregated between development and deployment.  Require formal documentation for all steps of the SDLC.  The production environment should be monitored to help ensure that unauthorized changes are not performed. |  |