**Assumptions for Eaton LDAP Upgrade Project – ODSEE to OUD**

* No change to the LDAP schema is required for the move to OUD
* No change to the LDAP Namespace is required for the move to OUD
* New servers will be provisioned by Eaton (cloud VM, On premise VM, or physical hardware)
* The server OS will be compatible with the latest version of Oracle Unified Directory (OUD) 12c found [here](https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/sysrs/system-requirements-and-specifications.html#GUID-880D655D-F9FB-439B-8001-10AA78D0FC57).
* OUD deployment architecture will mirror the existing ODSEE architecture.
* KPMG will employ offshore resources to execute the installation and migration of directory services configuration and data.
* KPMG will have a dedicated US based resource to manage the upgrade project.
* KPMG will perform system integration testing.
* KPMG will perform the upgrade/migration in 3 Eaton environments (Dev, Test, Production)
* The deployment for each environment will include two data centers with two to three servers in each data center.
* User acceptance testing (UAT) will require Eaton applications to validate the OUD directory functionality is operating as expected after migration.
* UAT will occur in a pre-production environment.
* KPMG expects Eaton application teams to supply there own test scripts that exercise functions served by the LDAP directory service. This includes but is not limited to
* User authentication
* User search
* Role / Group membership queries
* New user registration
* User provisioning
* User profile updates
* User password updates
* User disabled status.
* Deployment of the new servers in production will be dependent on Eaton stakeholder approval of UAT test results.
* The Eaton directory services architecture includes a global / local load balancer which manages traffic to the current ODSEE servers, and the cutover to the new OUD servers will be facilitated by an update to the load balancer LDAP server IP address configuration.
* The project will adhere to relevant compliance and regulatory requirements related to data storage, security, and privacy.
* The project plan will include a communication and engagement strategy for end-users to ensure that they are aware of the changes and understand the benefits of the upgrade.
* The project will include a rollback plan in case of unexpected issues during deployment or UAT testing.
* The project will include an ongoing maintenance plan for the upgraded directory to ensure continued functionality and security.
* The project will set up appropriate monitoring and alerting mechanisms to ensure timely identification of any issues post deployment.
* KPMG will manage project risks with regular updates via project status of project Risks, Action Items, Issues, and Decisions

**Questions from Managed Services – OUD Support**

* Volume of users / groups / roles that will be migrated from ODSEE to OUD?
* Are service accounts / admin accounts / functional accounts to be managed in OUD?
* Provide information on the high level proposed OUD architecture (e.g. No. of OUD servers, proxy setup, replication model, HA setup)
* Provide the expected volumes for the following –
* a) Incident tickets per month
* b) Service Requests per month
* c) No. of Patching per quarter
* Is OUD server upgrade part of scope?
* Are there plans to use Oracle Unified Directory Services Manager (OUDSM) for managing OUD instances? Or are we expected to use command-line interface for daily OUD related operations ?
* Is managing Access Control Instruction (ACIs) part of the scope?
* Are there any upstream / downstream applications consuming OUD data? If yes, are we expected to support any of the related operations?
* Expectations pertaining to OUD stack monitoring (e.g., How frequently are the servers to be monitored? Etc.)
* Are there any expectations on shell script creations for OUD stack management?
* Does the BAU operations involve performing any specific tasks?
* Expected Support Coverage model? E.g. 8x5, 24x7, Offshore/Onshore
* Are adequate SOPs available to support the OUD setup?
* Are there any OUD specific reporting and documentation requirements?
* Are SSL certificate renewals for OUD part of the scope?
* Are there any additional systems other than OUD that need to be supported?