FUTURE OF

Oracle Lifecycle Management

Cloud

It's estimated 50% of companies will move some assets to the Cloud over the next 5 years. This consolidation will mean even more emphasis on security. It also means traditional service providers being displaced and replaced with Cloud providers who will use state-of-the-art automation tools to automate Database Administration

By 2025 ....

80% of development apps will move to the Cloud

300Bn USD will be spent on Cloud Development & Test

80% of maintenance budget will be spent on the Cloud

Customizations

Heavy ERP customizations have always been the norm in the past but that may be changing. This can significantly increase the cost and unpredictability of upgrades. However automation software will introduce some predictive capabilities to minimize functional impact and performance.

On only average **9%** of the actual files get deployed

Organizations vastly over-test with some **36%** of scenarios being unnecessary

Organizations with customizations have an average of **6 releases/year**

47% of patches affect 4 E-Business Modules(AP,INV,PO and AR)

Data Growth

Big data keeps getting bigger both in the sheer numbers of distinct databases capacity. As the footprints expand the need for specialized tools and automation will become a critical part of proactive management.

38% of users run 100 or more distinct databases

10% run more than 1000 distinct databases

30% of users have data growth of 20%

42% of Oracle customers take more than 24hours to create a development database

Automated Testing

The Cloud will introduce more standardization and along with a concentrated pool of Databases and Application it will become more economical and practical to always execute regression tests. This will also make upgrades much faster and feasible

66% of companies automate half of their testing

83% of companies report constant or exponential growth in testing

64% of companies use open source testing tools

Cybersecurity

New laws carrying severe penalties like the 2018 EU GDPR will mean greater attention to applying security patches. In fact this will become a mandatory by the auditors. Data Masking will also become critical as new legislation is now preventing data from going offshore without it.

51% of users fail to keep systems at current patch levels

74% of customers cite Security and Governance as significant impact on administration

Only **49%** of users apply patches quarterly

Customer are on average **13months** behind on patch levels

Only **50%** of customers encrypt data

76% of customers perform security assessments