Cloud Readiness Assessment

Converged Orchestration.
Organizations who have regulatory concerns, the move to the cloud is not without risk. Enterprises have significant concerns about storing business data outside the walls of their enterprises, due to contract IT staff possessing a high level of access and control over information; available technology options to secure and manage user access and authentication; or even intentional or accidental actions of employees or contractors.

To allow organizations to gain value from cloud computing initiatives while addressing compliance concerns, Locuz offers Cloud Readiness Assessment. Through this assessment, organizations are able to identify sensitive or regulated content and notify key stakeholders including compliance officers, company executives, and administrators of any at-risk content. Once the initial assessment is complete, a best practices approach is outlined to separate regulated and non-regulated content or workloads, and subsequently migrate appropriate content to the cloud.

Cloud adoption is gaining speed as organizations worldwide believe this will put them ahead of their competition. The immediate pull to cloud computing is reduced total cost of ownership and less hardware for IT administrators to maintain.
Cloud Readiness Assessment includes interactive consultations with stakeholders to determine business practices, goals and opportunities. A thorough analysis of existing IT assets is completed using right assessment tools covering IT Infrastructure, Security posture, DC environment, Cost & Benefit Analysis, etc.
Locuz Cloud
Readiness Approach

Phase 1:
ASSESSMENT

This phase comprises of assessment of current Infrastructure, Tools being used, Cost & Benefit Analysis, and Security & Risk Assessment.
Assessment Activities and Outcome

**Activities**
- Onsite project kick-off
- Data center architecture and operations review
- Operational analysis including consideration of business objectives
- Identify and interview stakeholders
- Identify systems and review of the infrastructure and management tools deployed

**Outcomes**
- Scope and objectives

---

**Data Collection**

**Activities**
- Technical audit and analysis
- Installation of data collection tool(s)

**Outcomes**
- Raw information is gathered and packaged for analysis

---

**Analysis**

**Activities**
- Analysis of all collected data by Locuz Cloud Consultants
- Findings documented

**Outcomes**
- Comprehensive report on cloud opportunities and readiness
- Determine recommended solutions and strategy based on findings

---

**Report**

**Activities**
- Onsite presentation of assessment findings by Locuz Cloud Consultants
- Delivery of concrete, actionable recommendations

**Outcomes**
- Executive summary of findings
- Full documentation of analysis and recommendations in Cloud Readiness report
- Identification of impacts on current services
- Recommended adoption strategies for adoption of private, hybrid or public cloud
- Next-steps

---

**Assessment Summary**

- A thorough review of IT services, common infrastructure, organizational and Service Management process components
- An IT strategy that provides a clear strategic path towards Business Service Management, including Cloud capability
- A roadmap providing a defined set of activities needed for Cloud readiness
- A security and compliance analysis of risks to your organization

---

**Assessment Advantages**

- Evaluation by our experienced Cloud Consultants generates current information about your organization’s IT as a solid foundation for successful planning
- The assessment right-sizes your budget and capability estimate, to help avoid overspending and optimize user experience
- An interactive interview with stakeholders facilitates “buy-in” and aligns solutions with the needs unique to your organization
- A written report by our experts provides the blueprint for a business case justification as well as performance, reliability, environmental, management and security designs
Phase 2: CLASSIFY

All the IT workloads of an organization may not be suitable and compliant for cloud migration. Based on the assessment report it is important to classify the workloads as Cloud compatible or non-compatible. Locuz consultants will prepare the classification report based on the analysis of various Cloud readiness parameters of workload, security, compliance etc.

Phase 3: RESTRUCTURE

There may be a need to restructure the cloud compatible workloads to make it Cloud ready before any planning of migration to Private / Public cloud. Locuz will recommend a best practice approach for the workload restructure. The following are the sample list of activities for restructure.

- Consolidation & Aggregation
- Resource Pooling & Sharing
- Plan for Workload Migration
- P2V & V2V
- Define Workflow
- Development
- Application Readiness

Phase 4: MIGRATE

Based on the Assessment Report, the recommended workloads will be planned to migrate to Cloud (Private / Public). Initially low priority workload will be migrated and after the confirmation of stability and availability tests, the necessary workloads will be migrated to cloud environment. Determine migration schedules and project milestones to ensure content is migrated to the cloud according to business need, allowing for roll-out to end users as business needs dictate. Propose a schedule for ongoing risk / trend analysis reports to monitor and understand exposure levels and whether the existing controls are working appropriately. All contingency steps will be planned to roll back in case of any situational need.

- Virtual to Cloud (V2C)
- Self-Provisioning & Automation
- Workload Balance
- Service Orchestration
- Workflow deployment
- Imply Security
- Monitoring & Reporting
Sample
Cloud Readiness Assessment Report

❖ An executive summary
❖ Overview of the assessment scope and objectives
❖ Assumptions and limitations of the assessment
❖ Methods and tools used
❖ Design of the current environment or systems with applicable diagrams
❖ Security requirements
❖ Summary of findings and recommendations
❖ Assessment results:
   ❖ General control review
   ❖ Risk assessment, including identified assets, threats, impact and the risk results analysis
❖ Recommended actions
❖ Cloud Readiness Status Level