Poster Board No. 0063

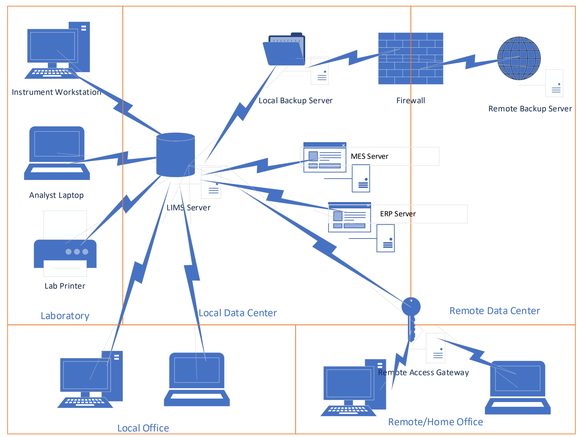
Cloud Based and Hosted Laboratory Information Systems: Balancing their Advantages and Disadvantages

Jim Elliott
Trinity Consultants Life Sciences – ADVENT Engineering

Abstract

Cloud-based and hosted Laboratory Information Systems (LIMS) offer a range of benefits including scalability, ease of implementation, improved collaboration, and real-time data access among geographically dispersed operations; however, security, infrastructure outages, and system and data stewardship issues pose challenges. This poster explores the benefits of a Cloud-based or Hosted LIMS as well as options for ensuring system and data security, approaches to mitigate the impact of infrastructure disruptions, and balancing responsibilities between the LIMS Vendor and the End User Company. By carefully considering and implementing the appropriate options, companies can leverage the benefits of cloud-based and hosted LIMS solutions while minimizing associated risks.

Figure 1. Typical On Premises LIMS Installation



Benefits of On Premises LIMS

- Customer has full control of the application, infrastructure, and their configuration
- Customer has full control over the security of the system and who has access
- Customer has full custody of the data stored in the system
- Customer has the ability to make customizations to the application and interfaces and keep those customizations secret to give them a competitive advantage
- Customer can interface to any other system they own, regardless of vendor support
- Customer has full control and accountability for the validation status
- Customer can upgrade on their own schedule
- Customer can build system using infrastructure that they are familiar with
- Relationship to the Vendor is transactional
- Vendor is not needed to support regulatory audits
- Can easily archive older data no longer required
- Can easily migrate to another vendor and/or platform

Disadvantages of On Premises LIMS

- Requires a qualified data center
- Requires IT staff to support the data center, infrastructure, platform, and application
- Expensive up front costs for servers and their software licenses
- Support from vendor more expensive on a per call basis
- New features not available when released
- Requires deep familiarity with system to configure and maintain
- Upgrades when skipping version is more complicated

Risks to be Assessed and Communicated

- 100% Reliant on infrastructure outside of your control
  - Impact of downtime on site's operation
  - What is the redundancy provided (ISP and Vendor)
  - Robustness of vendor's security
- Upgrade Cadence
  - What is the vendor's upgrade cadence and does the company have resources to support that cadence
- System Configuration Lockdown
  - Clear boundaries as to what configuration is managed by customer and vendor
  - Ability to review/audit system configuration managed by vendor
- Data Flow Mapping
  - Where does data leave the company's custody and becomes custody of vendor
  - What is the encryption at each stage and who holds the keys
  - Ability to review audit trails for components in vendor's control
  - Upgrades may impact data flows and data repositories
- Vendor Validation is a key component of the validation strategy
  - Do they have a robust System Life Cyle (SLC) Process
  - Are they following their procedures and SLC process
  - Does that SLC align with the company's SLC for a seamless validation package
  - What is vendor's availability and priority of supporting regulatory audits
  - What do upgrade validation packages entail
  - How much validation is required after vendor is complete
- Vendor Lock-In
  - Is there a process to export customer data to a neutral format for archiving
  - Is there a process to export/migrate customer data to another vendor
  - How to access customer data in the event the vendor goes out of business
- Upper Management and End User Buy-In
  - Critical that Upper Management understands risk assessments
  - End Users need to know how to support operations when there are issues with remote resources

Steps to Mitigate Risk

- Ironclad Service Level Agreement
- Robust and Clear Shared Responsibility Agreement
- Audit the vendor to ensure they have a robust System Lifecycle Process
- Review the validation and lifecycle documents with a critical eye
- On site validation still needs to be done to address site activities and procedures after vendor package is accepted
- Ensure all data is mapped and encrypted in both transit and at rest
- Confirm that upgrades do not impact agreements or assumptions that agreements are based on
- Re-audit them to ensure they are staying in compliance
- Require Upper Management and End Users to review and approve vendor agreements and risk assessments
- Ensure resources are hosted in compliant locations

Shared Responsibility Matrix Comparison

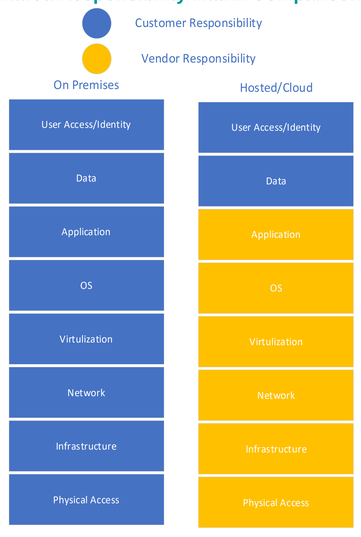
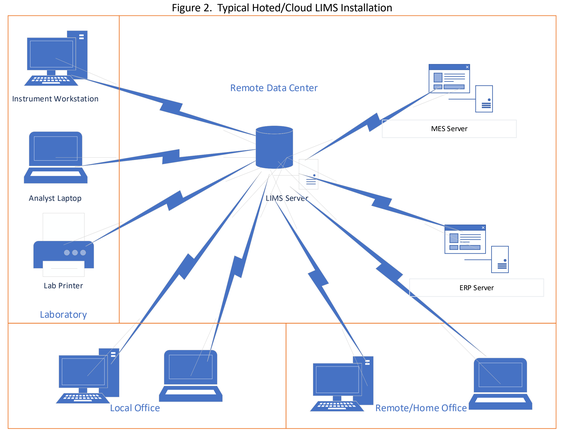


Figure 2. Typical Hoted/Cloud LIMS Installation



Benefits of Hosted/Cloud LIMS

- Lower up front cost
- Faster implementation
- Less validation on site
- Always on current version
- Access to new features sooner
- Interfaces managed by host
- No cost for upgrades
- No hardware refresh costs/effort
- Minimal infrastructure requirements
- Minimal IT staffing
- Easily scalable

Disadvantages of Hosted/Cloud LIMS

- Must upgrade on vendor's schedule
- More complicated risk structure
  - Reliant on outside infrastructure
  - Reliant on outside support
  - Reliant on outside validation
  - Reliant on vendor for Data Integrity
  - Reliant on vendor for regulatory audits
- Potential to have needed features deprecated
- Potential to have new features added that are not wanted
- Data might be difficult to migrate to another system/vendor/platform
- Potential for data to be hosted in another country with different data governance laws
- Vendor might use 3rd party components with a different release cadence

Conclusion

Cloud Based and Hosted LIMS solutions can be a great option for a small or startup company that does not have an internal IT staff or data center; however, due diligence needs to be performed to ensure that the LIMS provider is the right company to partner with. Furthermore, a robust Shared Responsibility Matrix agreement needs to be in place and enforced to ensure that the system is supported in a compliant manner. Lastly, end users and upper management need to be informed and agree to the risks associated with relying on another company that is the custodians of mission critical data.