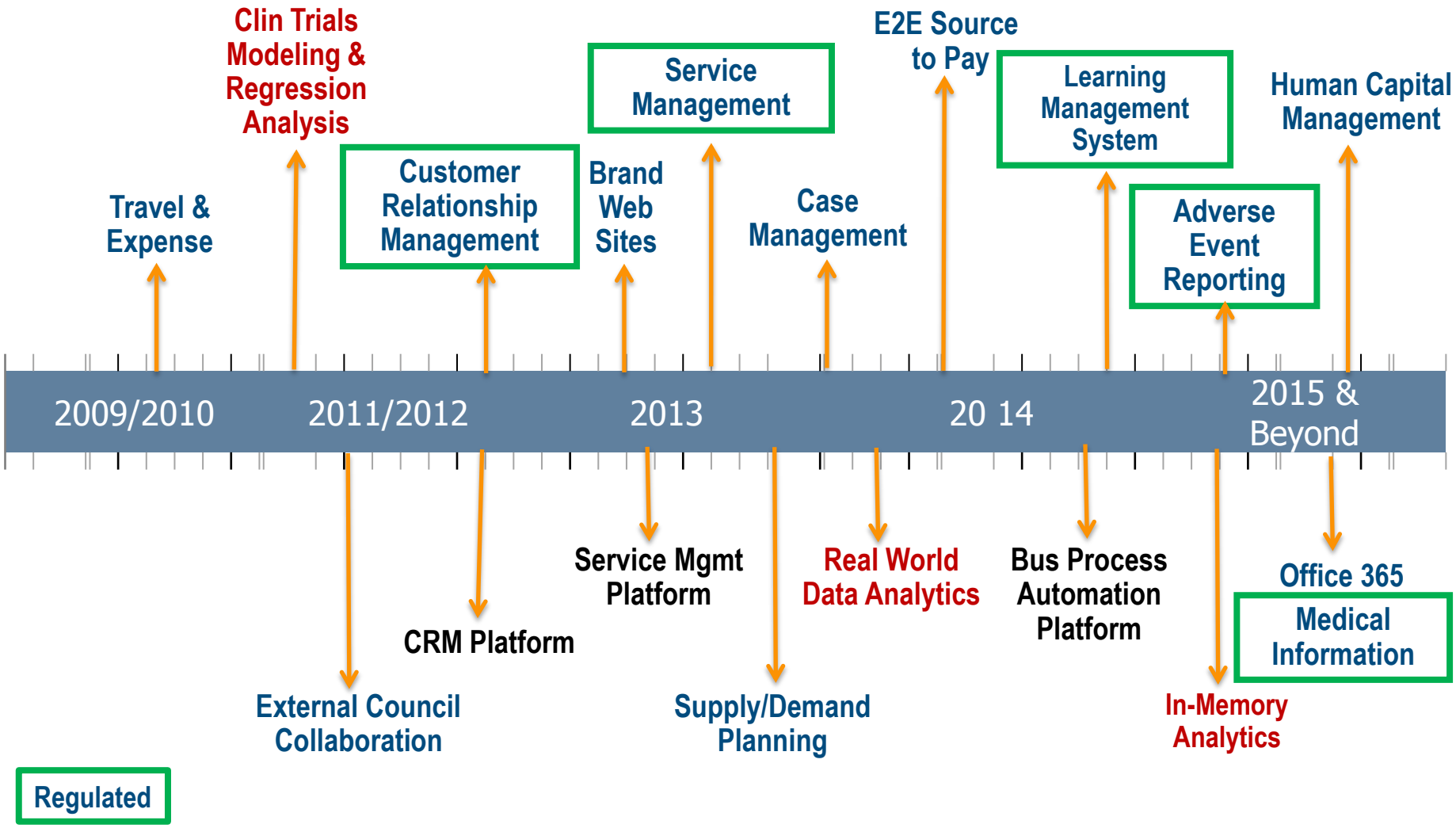
CLOUD COMPUTING IN A REGULATED ENVIRONMENT AT BMS

Topics

- BMS Cloud Computing Journey
- Cloud Opportunity and Challenges in a Regulated Environment
- Global Perspective of Cloud Compliance & Validation
- Elements of a Cloud Compliance Framework

BMS Journey of Cloud Computing

SaaS, IaaS, PaaS



Trends Emerging from the Five Year Journey

- SaaS has been the predominant cloud model deployed
  - Approximately 90 SaaS solutions in Production
  - Supported in a multi-tenet environment with single and multiple instances
  - SaaS often selected by business partners for simplicity, lower cost, speed of deployment and continuous delivery of new features and functions

- Increased leveraging of PaaS
  - CRM, Business Process Automation, and Service Management PaaS models are supporting the delivery of numerous SaaS solutions
  - SaaS solutions are a combination of commercially available offerings and in-house developed verticals

Trends Emerging from the Five Year Journey

- Expanded use of IaaS
  - IaaS initially leveraged for its compute power
    - Security addressed with Virtual Private Cloud (VPC), custom developed portal for access and data encryption
  - IT controls are now being developed to manage data storage as well as compute power
  - Data integration challenges emerging
    - Cloud to Cloud
    - Cloud to On-Premise
    - Planning adequate network capacity for Big Data analytics
  - Using IaaS for Dev & Test environments while developing Production support model
  - Using IaaS to advance DevOps as an agile application development practice

Cloud Opportunity and Challenges in a Regulated Environment

Opportunities and Challenges Expanded

Opportunities	Challenges
Hosting solutions with best in class systems Masks complexity from end-users	Pharma companies reluctant to store data on the cloud due to data security concerns, compliance requirements and loss of control
Reduction in capital costs for hardware/software –Lowers "cost of ownership"	Corporate governance of cloud usage is not mature
Location and device independence	May not know where (physically) data is located
Eliminate need to maintain separate DR environment/DR testing	Vendor disaster recovery specifics, are they adequate and tested?
On demand computing and storage resources (pay for resources utilized)	Tracking costs and storage resources will require strict monitoring
Reduction in maintenance for hardware/software	Loss of in-house technical expertise
Decreased "customization"	Change in user mind-set
More frequent delivery of new features and functions	IT required to support continuous upgrades and new releases
Environmentally friendly	Can't "touch" your servers

Global Perspective of Cloud Compliance & Validation

Global Cloud Compliance & Validation

- Global Regulators Expect:
  - Applications should be validated
  - IT infrastructure should be qualified
  - Data integrity and security must be maintained
- Status of Regulatory Guidance
  - Neither FDA nor EMA have issued any formal guidance around cloud.
  - FDA has a cloud working group in ‘learning’ mode and cloud-related guidance not on list of planned guidance for 2015
  - GAMP® and cross industry guides such as ITIL, ISO 27001, IEEE, ASTM, TickIT, CMMi provide guidance on Application and Infrastructure Development, Validation / Qualification, Operation, Support and Retirement

Global Cloud Compliance & Validation

- Current Environment
  - Accountability for compliance remains with the regulated company, but compliance controls may be delegated to others with appropriate management control
  - Basic premises do not change in an outsourced environment, including cloud, what changes is the chain of command and trust
  - Apply basic validation and Electronic Records and Signatures (ERES) concepts as best we can to our cloud/SaaS providers and the unique risks that they present.
- Future Trends
  - Sophistication of cloud services evolving and is focusing more on compliance and access to information
  - Like E-signature controls, does the industry need to get together with regulators to drive clear guidance on cloud?

Elements of a Cloud Compliance Framework

Key Elements

- Vendor Selection
  Pick the right partner
- Security and Data Integrity
  Protect your assets
- Qualification and Validation
  Make sure it works for you
- Ongoing Monitoring and Change Management
  Make sure it keeps working




Vendor Selection

- ✓ **<u>Ensure RFI/RFP questions account for cloud concerns</u>**
- ✓ Check experience and references
- ✓ Try before you buy
- ✓ Be clear on your expectations
- ✓ Audit (if you can)

Security and Data Integrity Controls

- Enlist your security experts and ask key questions.
  - What type of data are we planning to put in the cloud and how critical is it to our business?
  - Does the company have guidelines per what's permitted in the cloud?
  - Determine how much of the 'stack' you need to worry about…where's the risk?
  - What type of controls do we need to protect our assets?
- Keep in mind, 21 CFR Part 11 'Open System' controls.
- Get a thorough understanding of the controls offered by the vendor.
  - Look for certifications, i.e. SAS 70/SSAE 16
  - Include security experts when you assess/audit
  - Search helpful Web resources
    - https://cloudsecurityalliance.org

cloud CSA security alliance℠

Qualification and Validation

Q. How do we qualify or validate a system that we don't control?

Q. How do we qualify infrastructure that we can't see or touch or even physically locate?

Think about the objective of the activity and then determine how a cloud solution can achieve that objective:

- Determine how much of the 'stack' you need to consider…where's the risk?
- Update your procedures to allow the vendor to do some of the work for you.
- Audit, review and formally accept vendor's process.
- Get agreement on documentation custody.
- Clearly document the rationale for your approach.
- Don't give away too much…you still have to defend it.

Ongoing Monitoring and Change Management

- Does your provider have documented processes for incident, change and problem management?
- When problems occur in the environment, do you expect to be notified?
- How will you react when the provider makes changes? Will you even know?
- Can you get upgrades/patches on your schedule or do you have to adhere to the vendor's?
- How much time do you get to assess and test changes before they are rolled into your production environment?
- Will the vendor allow you to audit periodically once the service is up and running?

Q. Where can you rely on vendor process and control and where do you need to insert your own?

APPENDIX

Appendix
Cloud Computing Paradigms

Cloud Introduction

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of essential characteristics, service models, and deployment models.

Cloud Service Models – Three Layers

Software as a Service (SaaS): The service provider hosts the software. Removes the requirement for the customer to install it, manage it, or buy hardware to support it...a simple connection to use the software.

Platform as a Service (PaaS): Black-box services with which developers can build applications on top of the compute infrastructure. Can include developer tools offered as a service to build services, or data access and database services, or billing services.

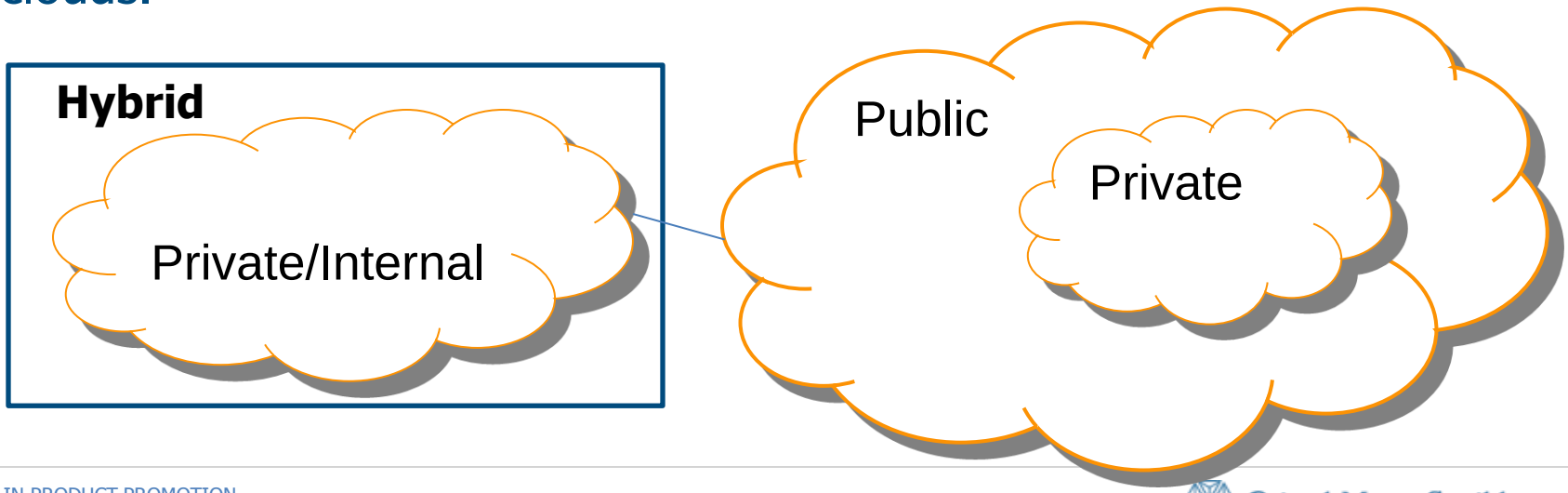
Infrastructure as a Service (IaaS): Offers storage and compute resources that developers and IT organizations can use to deliver business solutions.

Cloud Deployment Models

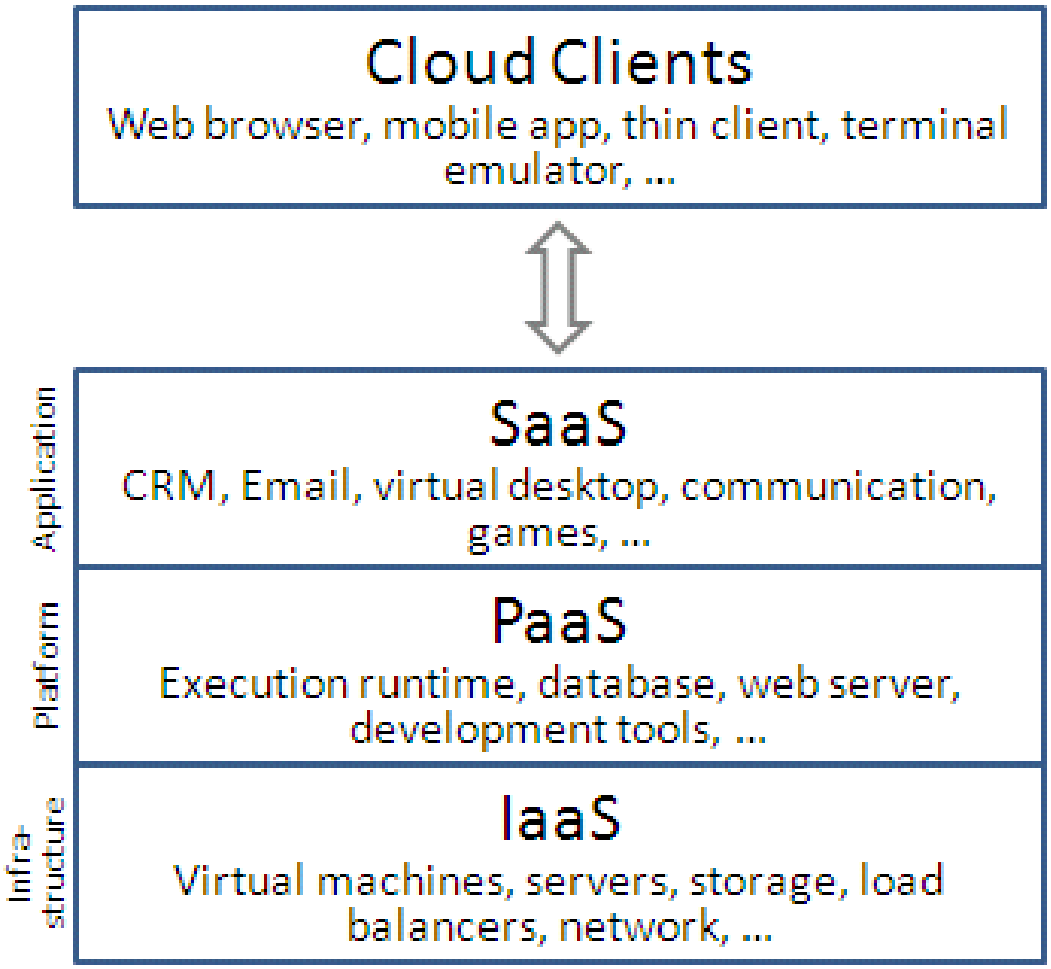
Public clouds: Virtualized data centers outside a company's firewall. Generally, a service provider makes resources available to companies, on demand, over the public Internet.

Private clouds: Virtualized cloud data centers inside a company's firewall. Can also be a private space dedicated to a company within a cloud provider's data center.

Hybrid clouds: Combines aspects of both public and private clouds.



Cloud Service Model examples



Security Relative to Service Models