Cloud models and compliance requirements… which is right for you?

Bill Franklin, Director, Coalfire
Stephanie Tayengco, VP of Technical Operations, Logicworks

March 17, 2015

Speaker Introduction

Bill Franklin, Director, TAAS, East Region
(Technology, Advisory and Assessment Services)
Coalfire Systems, Inc.

Stephanie Tayengco, VP of Technical Operations
Logicworks

- Cloud / Service / Deployment Models
- Cloud Considerations
- Cloud Trends in Healthcare
- Cloud Adoption
- Security Responsibility
- Understanding your cloud provider
- Q&A

About Coalfire

We help our clients recognize and control IT-related risk, and maintain compliance with all major industry and government standards.

- Our approach and methods validated by more than 5,000 projects
- Accurate and ***independent*** audit and assessments.
- Consolidated Audit Program across PCI/HIPAA/FISMA/SOC/ISO and more

Coalfire logicworks

ZOLL

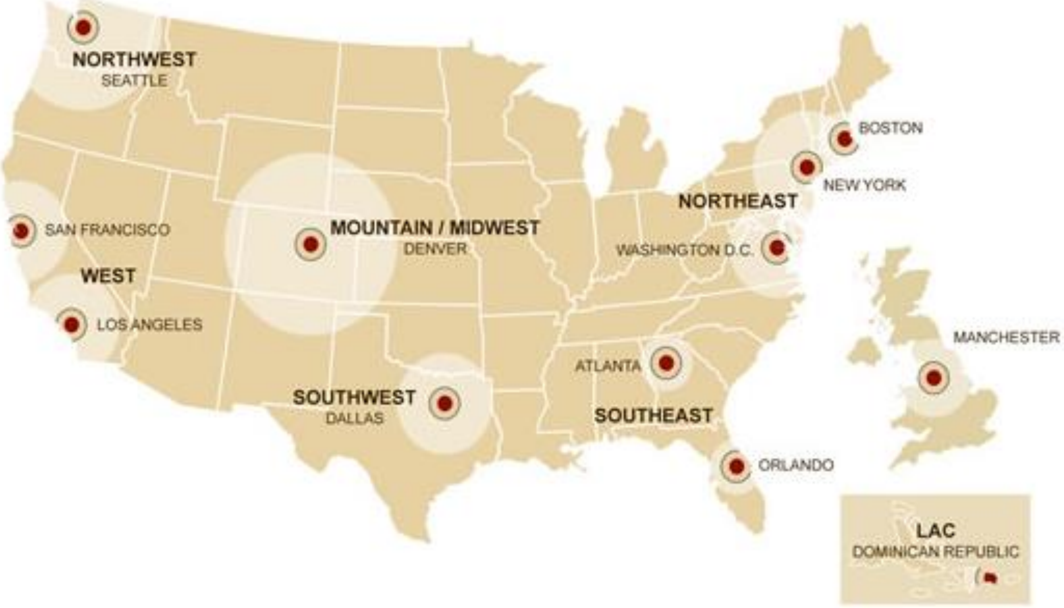
DENVER HEALTH
Level One Care for ALL

PHYTEL

SEATTLE CANCER CARE ALLIANCE

ORACLE

GHX
Global Healthcare Exchange



North Shore LIJ
North Shore-Long Island Jewish Health System

McKESSON
Empowering Healthcare

Epic

Cerner

GENTIVA

dexcom

The Children's Hospital

ClearDATA
HEALTHCARE · COMPLIANT · CLOUD

ADVISORY SERVICES

AUDIT & ASSESSMENTS

COALFIRE LABS
DIGITAL FORENSICS

PENETRATION TESTING

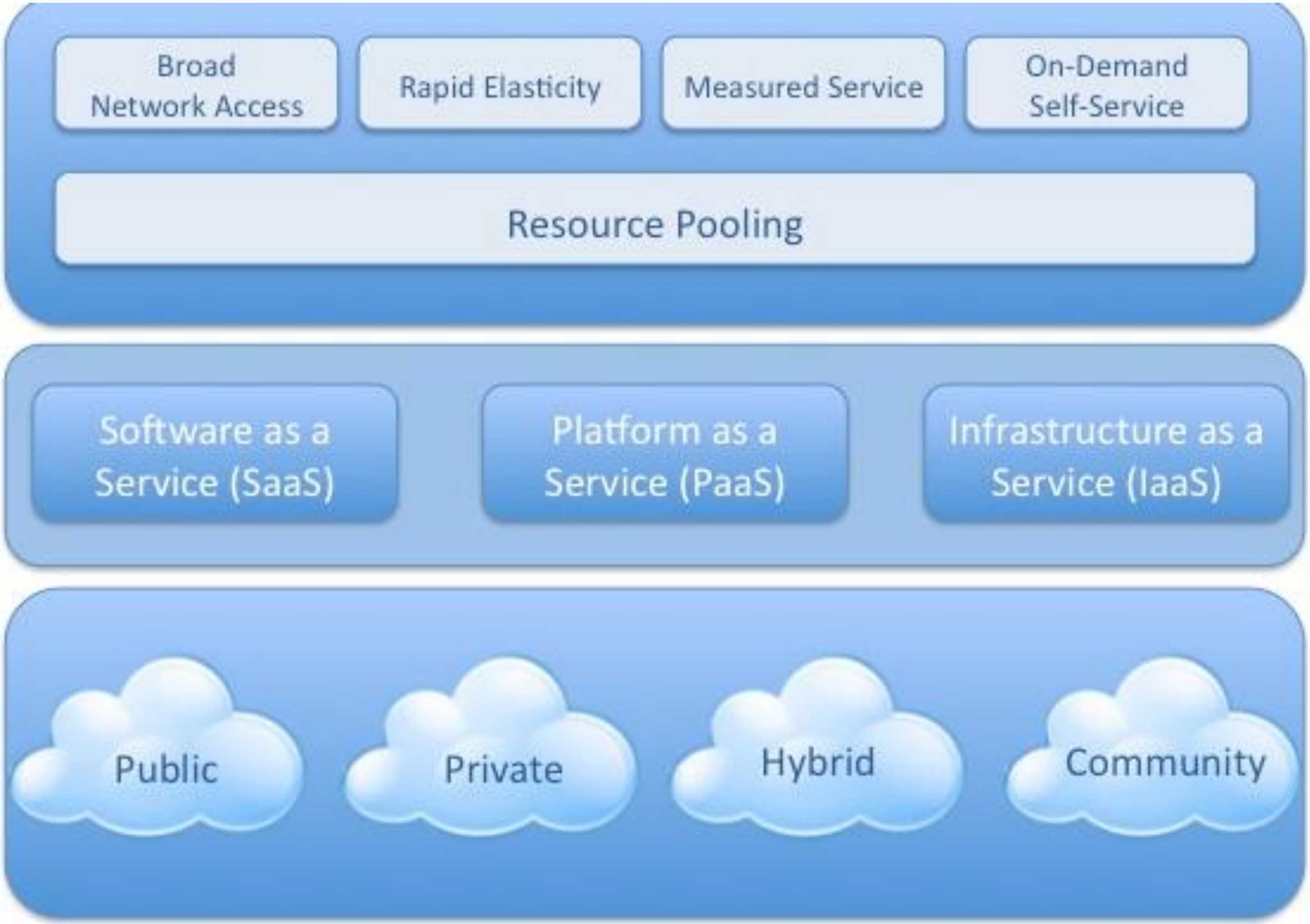
CLOUD & VIRTUALIZATION

APPLICATION SECURITY

NAVIS SERVICES

Coalfire

Cloud models



Broad Network Access

Rapid Elasticity

Measured Service

On-Demand Self-Service

Resource Pooling

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Public

Private

Hybrid

Community

Essential Characteristics

Service Models

Deployment Models

Service Models Defined

NIST Defined

- **SaaS**: Software as a Service – Software provided as a service running in the cloud providers environment
- **PaaS**: Platform as a Service – Application development platform runs on cloud providers hardware and development software
- **IaaS**: Infrastructure as a Service – Hardware – Servers, storage solution, network components, and underlying operating systems

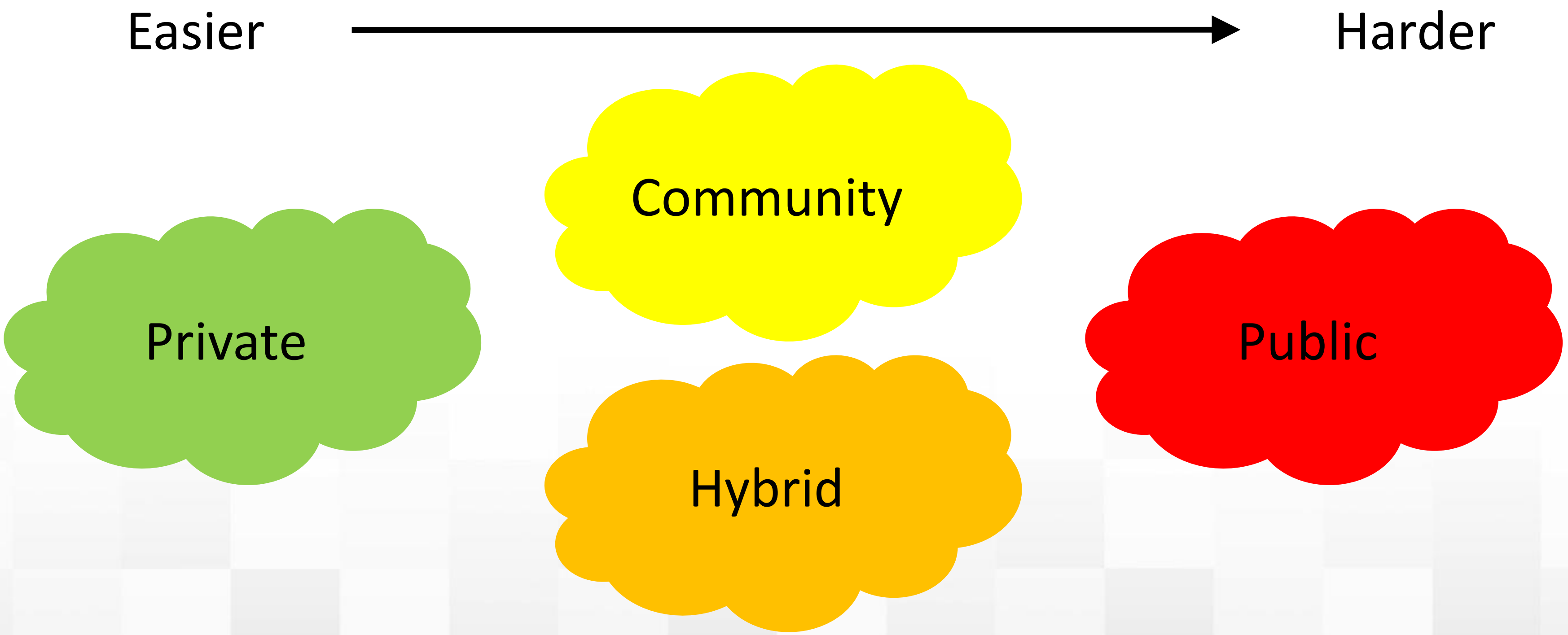
Others

- **DaaS**: Data as a Service – One central location for all data of an organization
- **CaaS**: Communication as a Service – VOIP, Internet Telephony, IM, etc…
- **MaaS**: Monitoring as a Service – Provides monitoring functionality for other services such as applications, servers, or any other IT system or component
- **XaaS**: Anything as a Service

Deployment Models Raise Challenges

Security and Compliance

Accountability and Due Diligence



Easier

Harder

Private

Community

Hybrid

Public

All clouds are not created equal

Dedicated Environment

- ➢ Devices and systems dedicated to your business
  - Reduce Risk
  - Increase Cost

Multi-Tenant Environment – Leverages large servers with multiple clients

- ➢ Devices and systems shared among users
  - Reduce Cost
  - Increase Risk

Multi-Tenant Risk Example

Shared Database with multiple clients' data

- Application Error
- Database Corruption

Are Controls in place such as:

- SDLC (System Development Life Cycle)
- Authentication
- Access Rights
- Data Verification

If the controls aren't in place:

- Your data is exposed to other cloud vendor clients
- Other cloud vendor clients' data appears in your environment

➢ **What is the impact?**

➢ **Is it significant?**

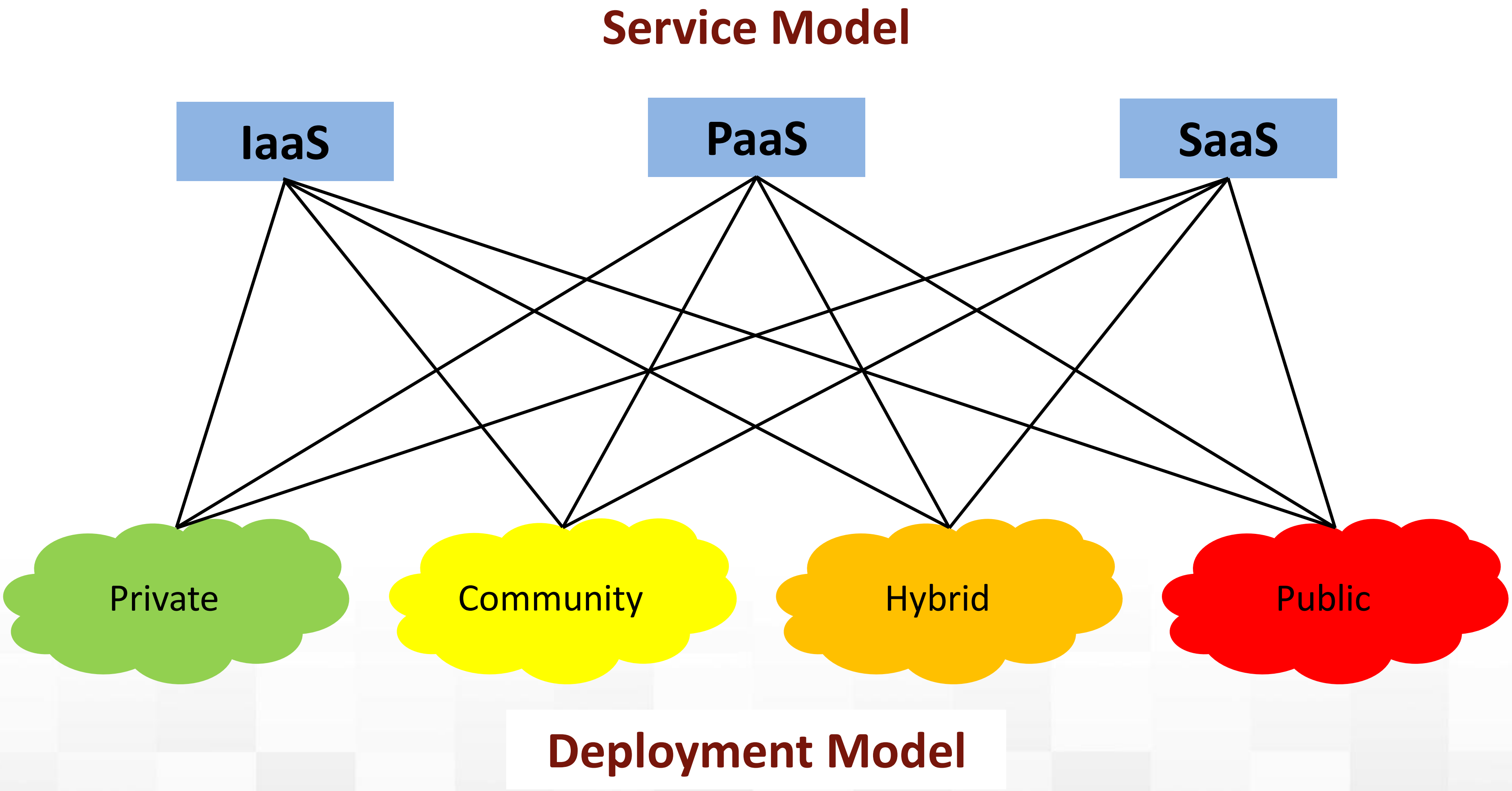
Which cloud is right for you?

Weighing Cloud Service and Deployment Model and Your Environment

YOU MUST CONSIDER:

1. **How critical the data and applications are to your business**
2. Regulatory and/or Data Protection Requirements
3. How integrated cloud services need to be with enterprise functions both:
   - In-house
   - Outsourced
4. Other factors important to your business

Combinations



Service Model

IaaS

PaaS

SaaS

Private

Community

Hybrid

Public

Deployment Model

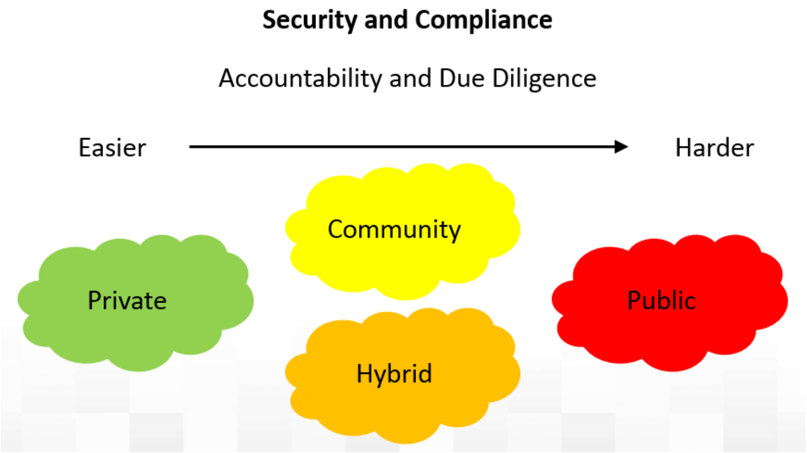
Benefits…

- **Reliability -** The inherent resiliency of the cloud provides a higher degree of redundancy and continuity support than is typical
- **Cost Effective -** Resource pooling for ‘Utility’ (eMail, Collaboration, etc.) functions allows lower cost when provided on a large scale basis
- **Scalable -** The ability to meet increased infrastructure needs faster
- **Physical Security -** Large scale cloud hosting takes place in facilities that provide a better physical environment and security than most SMB data centers
- **Compliance* -** Controls aligned to regulatory requirements (HIPAA, GLBA, PCI, etc.) and control frameworks (NIST 800, ISO 27000, Cobit, etc.)
- **Audits* -** Likely to have one or more types of control reports that have been independently tested by a third party (PCI, HIPAA, FISMA, SSAE 16, etc.)

* You are still Accountable and must do your Due Diligence

Risks... (Due Diligence and Accountability)

- **Data Security**
- **Data Backup and Recovery**
- **Data Disposal**
- **Data Discovery** (eDiscovery)
- **Data Backup and Recovery**



- **Location of the data –** Geographic locations and applicable regulations
- **Multi-Tenancy –** Co-mingling data with other cloud customers
- **Data aggregation and inference** – Data aggregation and inference that could result in breaching the confidentiality of sensitive and confidential information
- **Compliance** – Lack of controls that meet Regulatory and Industry Requirements
  - HIPAA, PII (State Regulations), PCI DSS, etc…

What are healthcare organizations doing?

Cloud vendors are not yet fully trusted:

Many healthcare organizations trust the security controls in their own systems more than a cloud provider’s.

KLAS research revealed:

Two-thirds of the hospitals that were interested in the cloud, preferred “private clouds” that were dedicated to their data and applications.

HIMSS focus group of senior health IT executives:

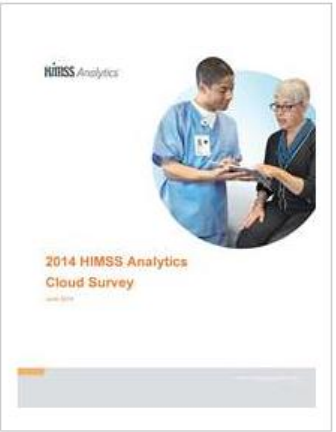
“…they were more comfortable using a private cloud than the public cloud and were more likely to store administrative data than clinical data in the cloud.”

Overall cloud trends

A HIMSS Analytics study published in mid-2014 showed healthcare providers’ cloud usage accelerating:

- Of the 150 survey respondents— most of them hospitals and health systems—83% were using the cloud in some way.
- Half of those organizations had clinical applications in the cloud, and 73% used cloud services for administrative or IT functions.
- Three quarters of respondents were using private or hybrid cloud services that gave them more control over their data than if they’d put everything in the public cloud.
- Just 23% said they were relying on the public cloud.

Source: **2014 HIMSS Analytics Cloud Survey**



HIMSS Analytics

2014 HIMSS Analytics
Cloud Survey

Reasons for not using the cloud

- ***Security (62%)***
- A continuing focus on in-house IT operations (42%)
- Availability and uptime concerns (39%)

However…

- 27% of healthcare cloud users went to the cloud partly because they thought it would improve security.

Source: **2014 HIMSS Analytics Cloud Survey**

Top reasons for adopting cloud

- Cost (56%)
- Speed of deployment (53%)
- Lack of internal staff/expertise (52%)
- Disaster recovery (50%)
- Need for a scalable, always-on solution (45%)
- Regulatory compliance (42%)
- Security (27%)
- Workforce mobility (27%)

Source: **2014 HIMSS Analytics Cloud Survey**

Move to the Cloud- Things to Do

- Identify the data to be moved to the cloud
- Identify risks- Impact to the organization if the data was modified, lost or accessed by an unauthorized individual
- Identify availability risks
- Identify applicable regulatory and compliance requirements, restrictions and regulatory concerns
- Identify a suitable deployment model to meet your needs
- Identify service providers that offer services in the deployment model
- Confirm the presence of a ***robust vendor management program*** within your organization
- Business Associate Agreements

Risk Assessment is Critical!

About Logicworks

20+ Years Keeping Critical Websites + Internet Applications Up & Running

HEALTHCARE

HIPAA compliance capable IaaS and Managed AWS

With our clients we host:

- 30 US States' Health Information Exchanges (HIE)
- The largest Health Insurance Exchange (HIX) in the United States
- The industry's leading Clinical Software-as-a Service (SaaS) providers
- Global Healthcare Systems Integrators
- Healthcare Analytics Platforms

LEGAL

- Largest e-Discovery / Digital Courtroom Platform in the World
- 40,000 Law Firms and Every Court in Washington DC

FINANCE

- SaaS Infrastructure for Top 5 Global Banks
- Investment/Portfolio, 401k, Mortgage Management

- 24x7x365 Monitoring
- Support & Escalation to Expert Engineers
- 100% SLA with High Availability Services
- Managed Security Services
- Database Services
- Custom Runbooks
- DR/Backup & Recovery
- Dev-Ops/Automation
- Dedicated Named Account Manager

Coalfire logicworks

Trends in Cloud Adoption

In practice we're seeing:

- Private cloud service adoption by CEs
- Private and Public cloud service adoption by Service Providers to the Healthcare Industry

Driving factors include:

- Space constraints of in-house datacenters
- Agility
- Increased Focus on Core Competencies
- Security Management
- Consultation
- High-Availability architectures and SLAs

PRIVATE CLOUD SOLUTIONS

MANAGED AMAZON WEB SERVICES

Coalfire logicworks

Shared Security Responsibility

Security in the cloud, whether private or public is a shared responsibility

The burden of responsibility can be weighted towards the provider or customer depending on the service model:

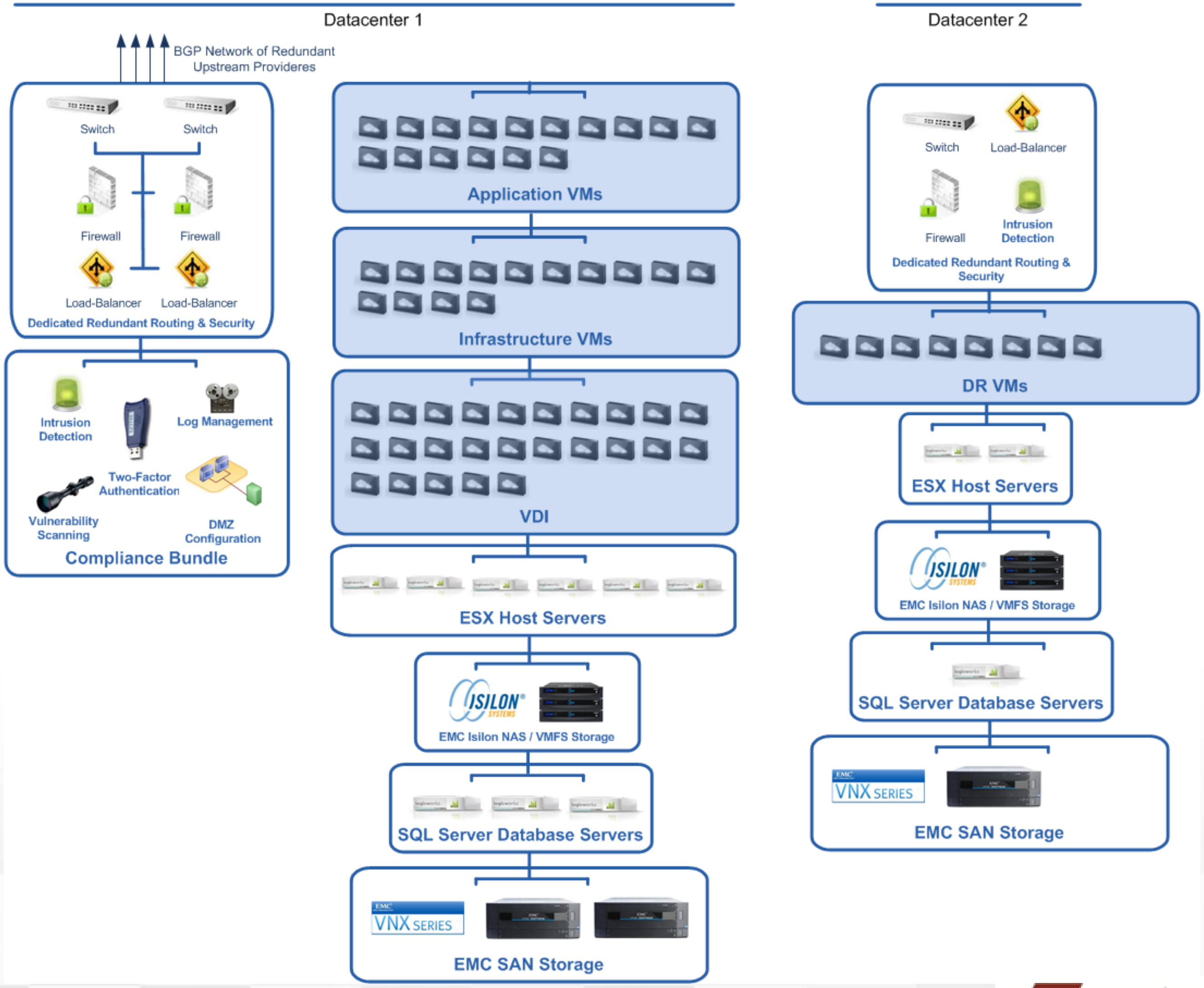
Self-service

Managed Service

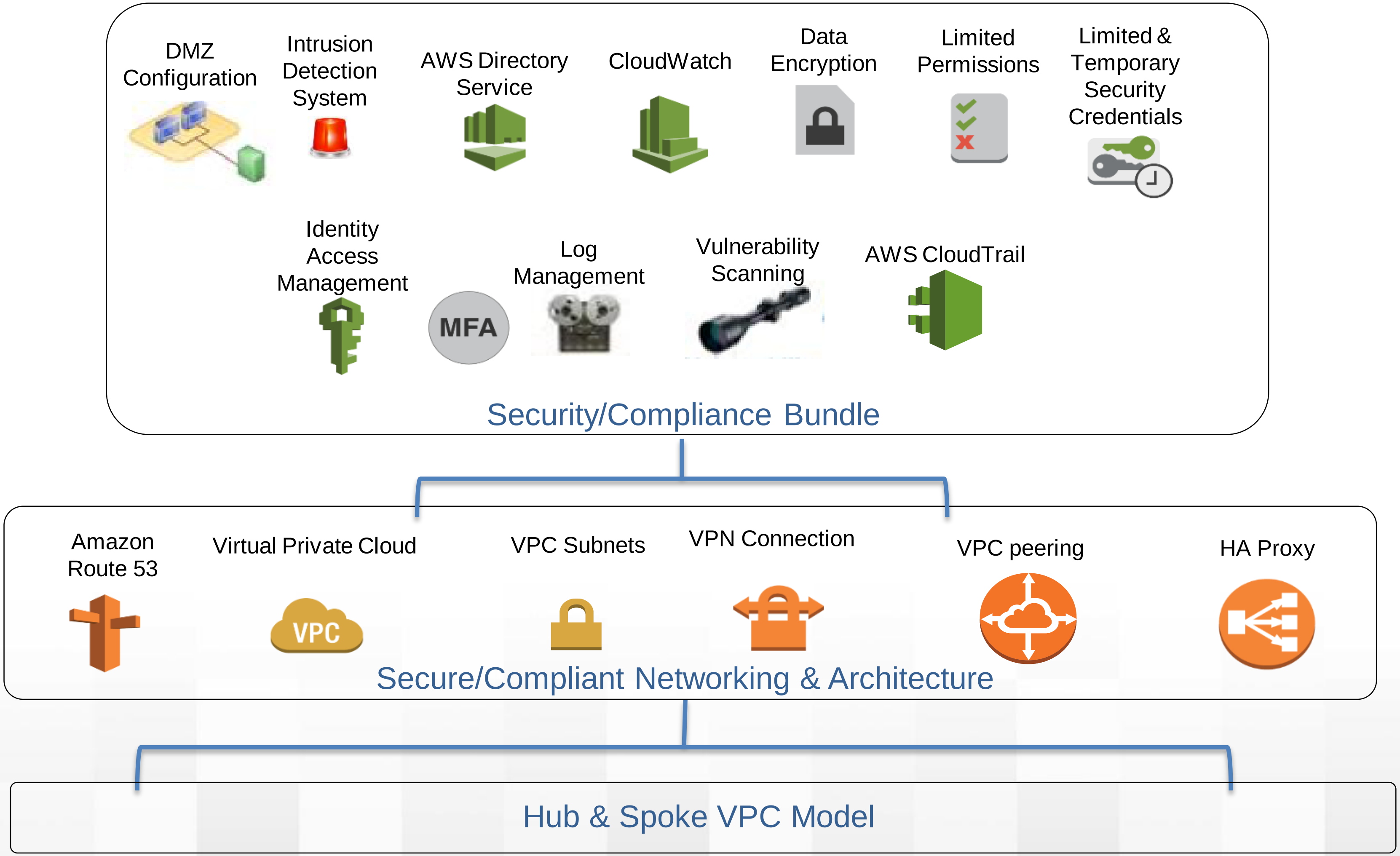
Have a common understanding of –

- Data Criticality
- The services
- Each Party's Responsibilities

Private Cloud Model



Public Cloud Model – Secure Architecture



DMZ Configuration

Intrusion Detection System

AWS Directory Service

CloudWatch

Data Encryption

Limited Permissions

Limited & Temporary Security Credentials

Identity Access Management

Log Management

Vulnerability Scanning

AWS CloudTrail

Security/Compliance Bundle

Amazon Route 53

Virtual Private Cloud

VPC Subnets

VPN Connection

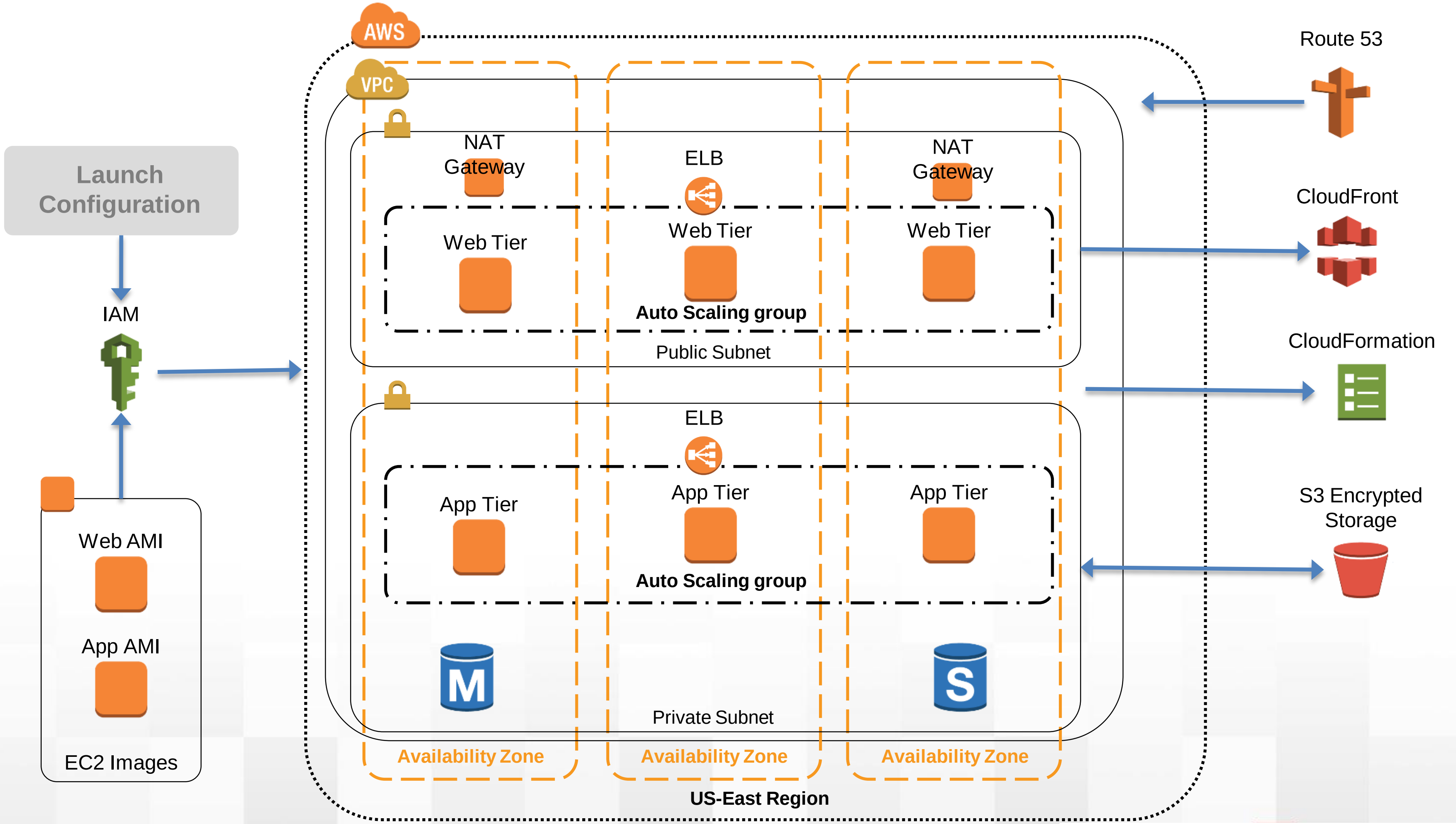
VPC peering

HA Proxy

Secure/Compliant Networking & Architecture

Hub & Spoke VPC Model

Public Cloud Model – Application Diagram



Understanding your Cloud Provider

Business Associate Agreements

- What limitations have been imposed?

Responsibilities Matrix

- Understand what each party is responsible for
- Review the OCR Audit Protocol with your provider

Bill Franklin
Director, Coalfire

Bill.Franklin@coalfire.com
www.coalfire.com

Stephanie Tayengco
VP, Logicworks

stayengco@logicworks.net
www.logicworks.net

Coalfire®

logicworks