

easy·street

Cloud
Computing in
a HIPAA-
Compliant
World

NRTRC Telemedicine
Conference

Dean Oswald

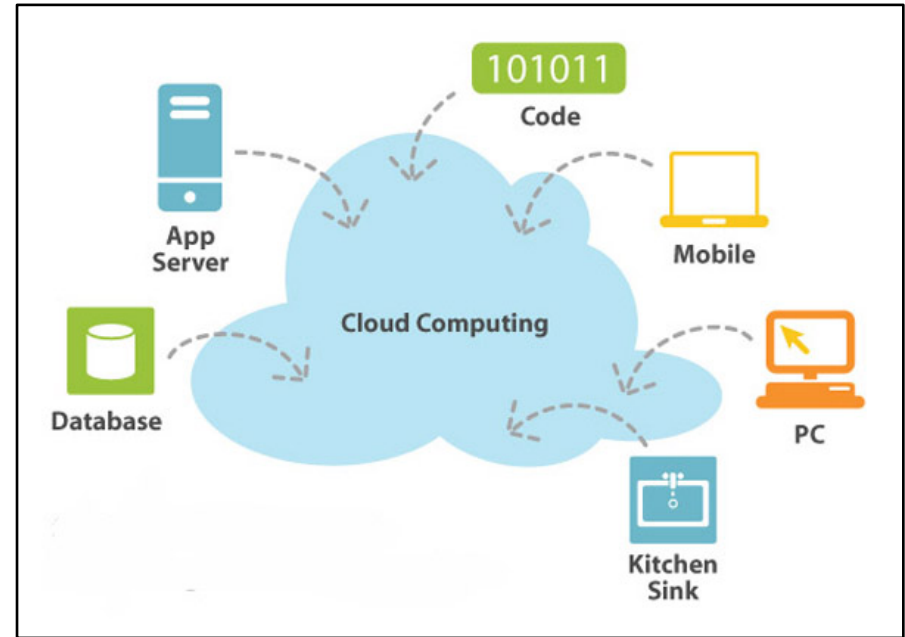
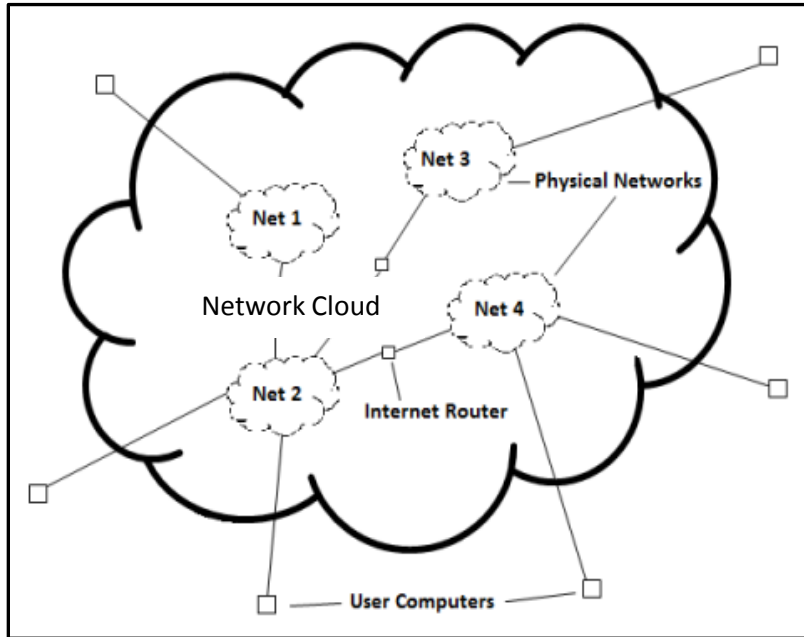
March 25, 2014

WHERE BUSINESS
LIVES
THRIVES
GROWS

Agenda

- Cloud overview
- Infrastructure-as-Service overview
 - HIPAA-compliant IaaS
- Risk – cost – speed tradeoffs
- Responsibility matrix for HIPAA requirements
- New technologies
- Customer Examples
- Recap

Why is it called “the cloud”?



Originally network shorthand for: “Magic happens in here and we don’t know/care how it works.”

Evolution toward the cloud

Applications run on-premises



You own the hardware and perform maintenance and operation of the data center

Applications run in the IaaS Cloud



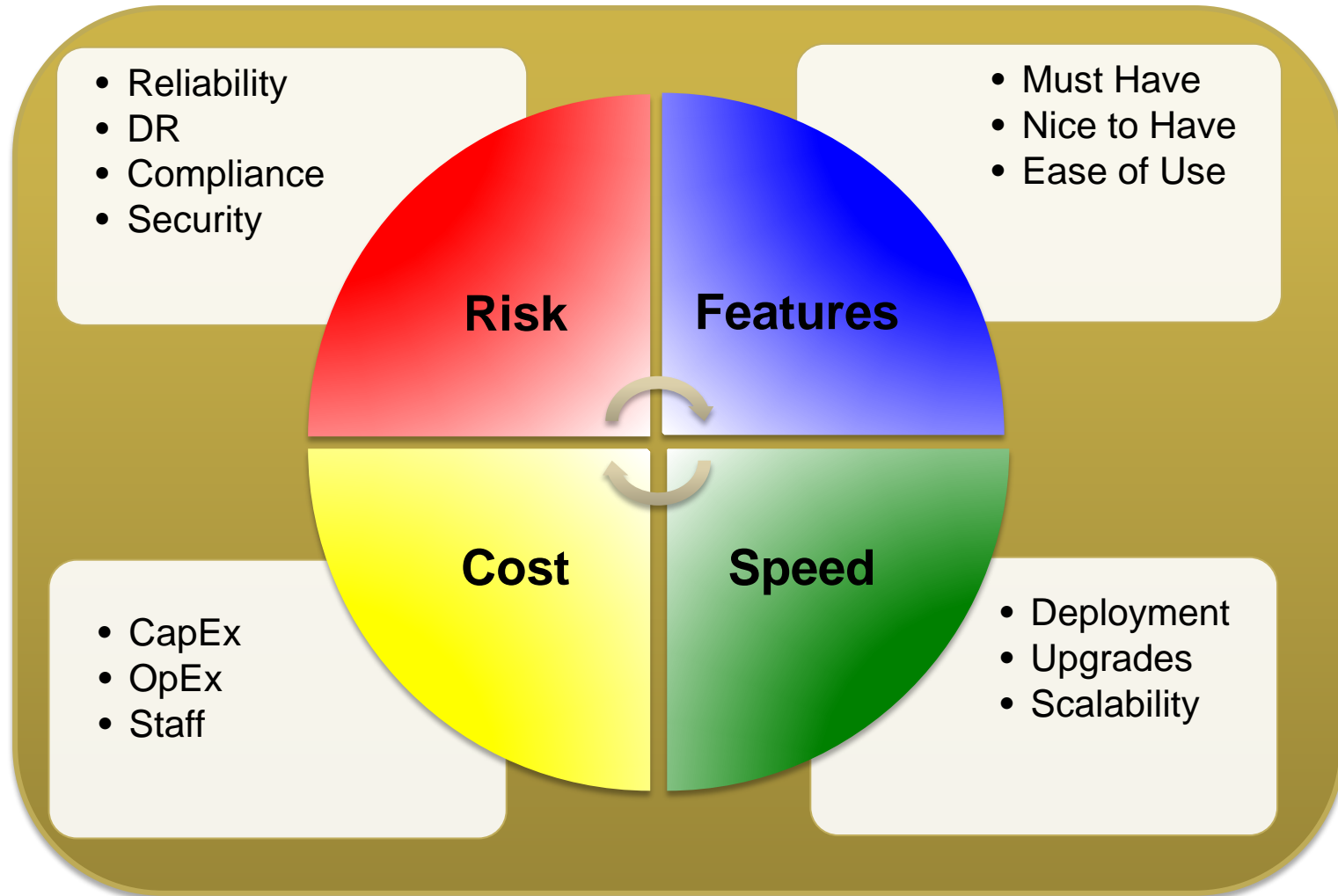
You pay someone to run your applications on hardware to your specification

Applications run in the Cloud

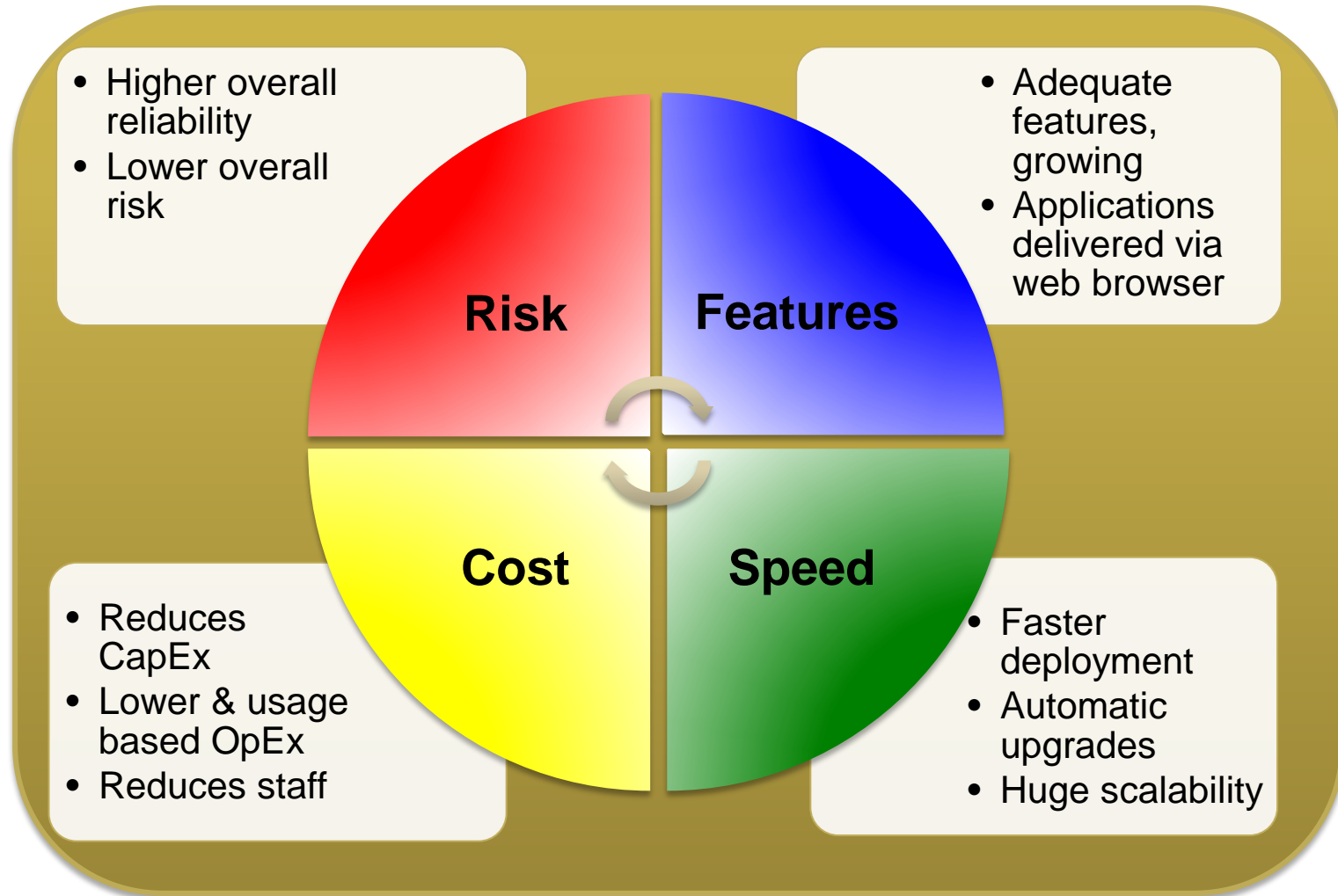


You pay for computing capacity that can be used for your applications

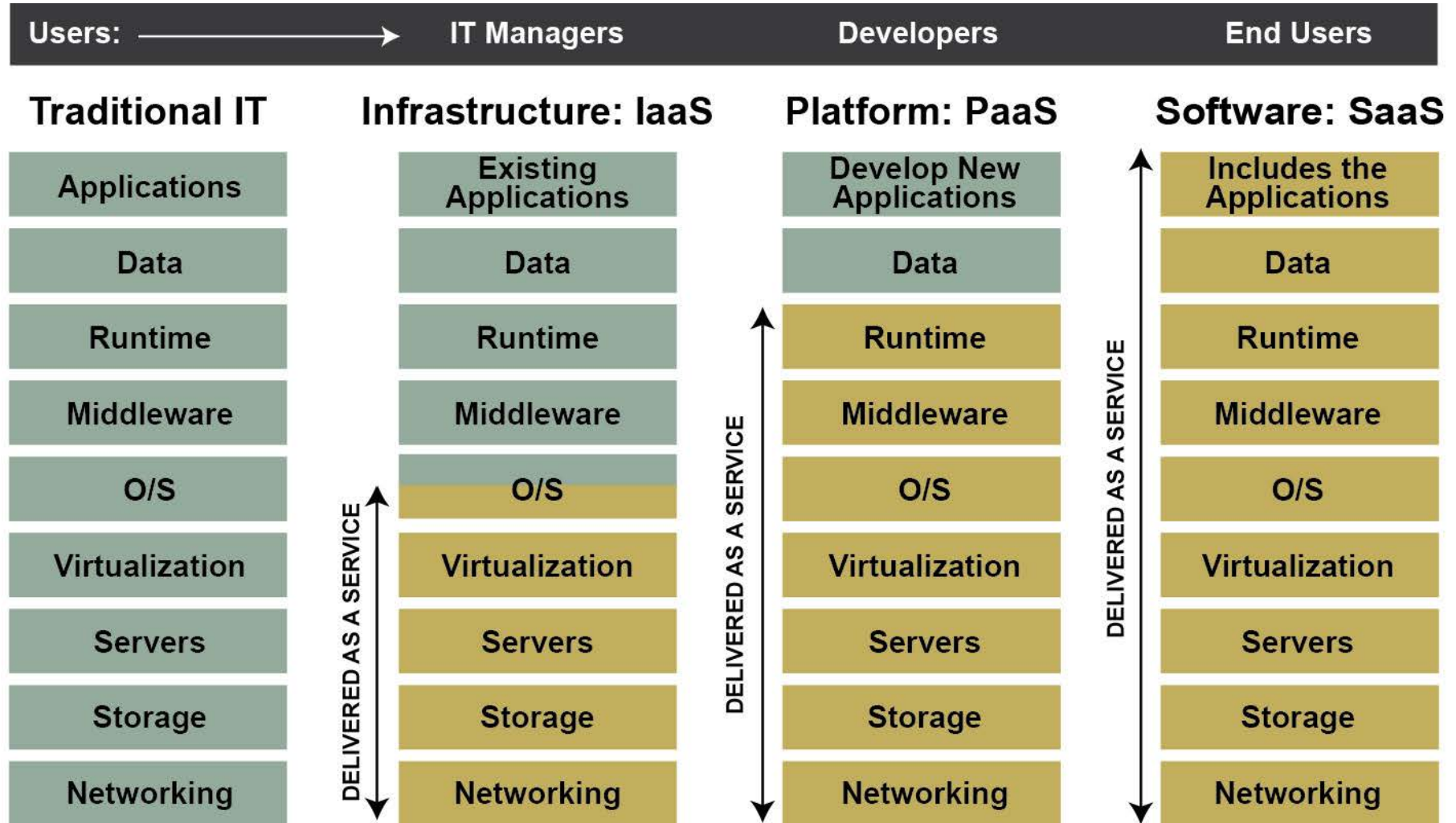
IT decisions balance conflicting goals



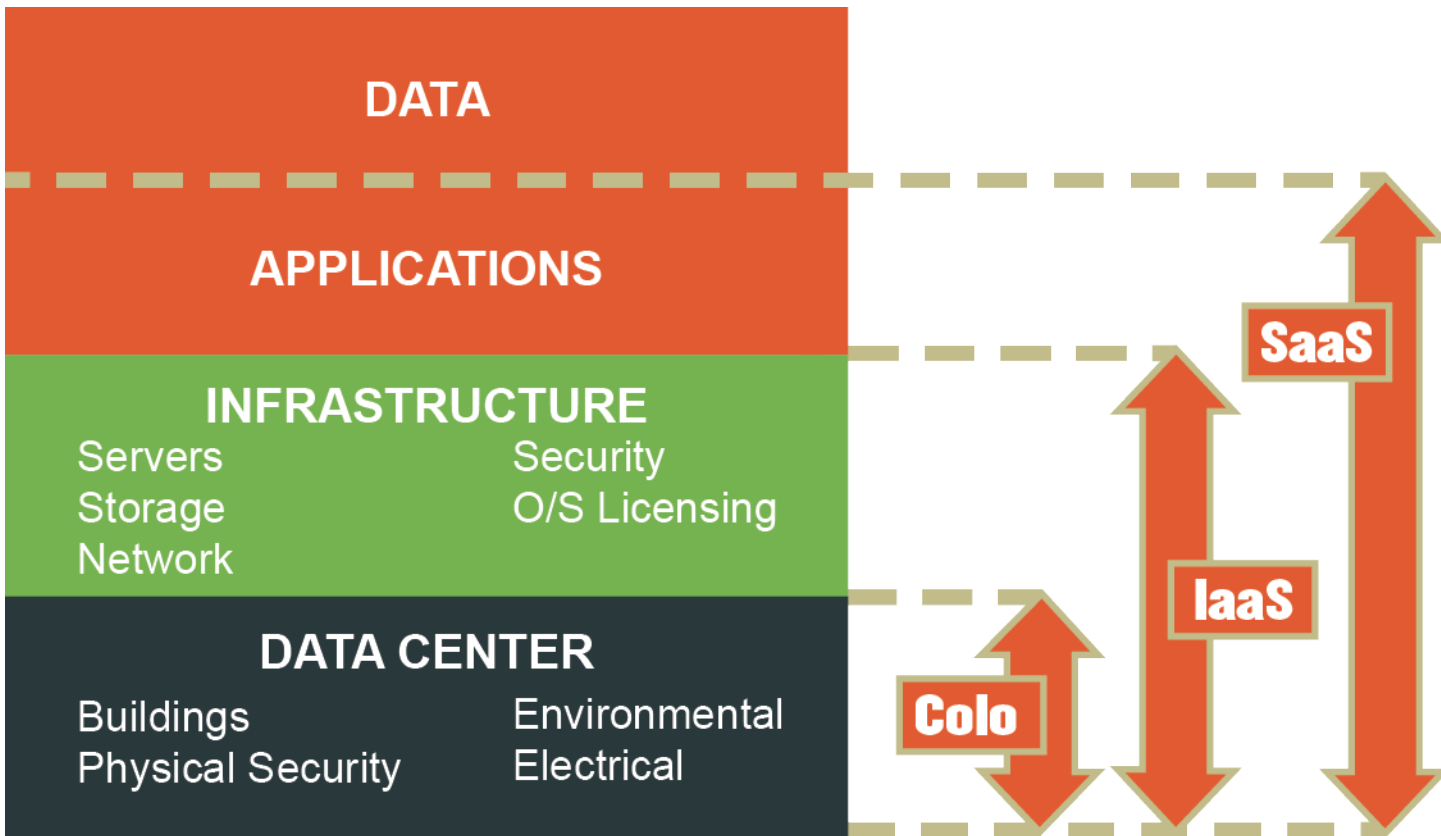
Cloud computing is like a miracle drug



Cloud computing service models



What is Infrastructure-as-a-Service (IaaS)?



Infrastructure-as-a-Service benefits

- An excellent option for healthcare organizations that are:
 - Facing the expense of a technology or hardware refresh
 - Ready to implement EMR and EHR solutions that require complex environments
 - Short-staffed due to changing needs or loss of experienced IT professionals
 - Desiring a Disaster Recovery environment outside their own region
 - Concerned about ePHI security or other compliance issues (HIPAA-compliant providers)
 - Seeking a more predictable cost structure

HIPAA-compliant IaaS

- Added requirements based on HIPAA and/or HITECH-Act regulations
- External auditor assesses organizational, administrative, physical and technical controls
- Validation of compliance with policies and procedures by review of logs, configuration, records and interview of personnel
- Evaluation and validation of architecture, including interviews of personnel responsible for design and implementation, for Technical Safeguards
- Validation of physical controls deployed in the environment
- Privacy Rule requires Business Associate agreement

A common control design assessment model



1.	Strong	Exhibits strong design in every respect. Control design weaknesses are minor.
2.	Satisfactory	Exhibits safe and sound design but may demonstrate modest weaknesses, which can be corrected without major remediation.
3.	Less than Satisfactory	Exhibits some degree of concern due to a combination of weaknesses that may range from moderate to severe
4.	Deficient	Exhibits control design that would create an unsafe and unsound environment that may impair future viability of the entity.
5.	Critically Deficient	Exhibit critically deficient control design and in need of immediate remedial action.

Example requirements: Administrative Safeguards

Standard	Requirement	ES	Client	Both
Security Management Process HIPAA 164.308(a)(1)(i)	Risk Analysis and Management	■		
	Sanction Policy	■		
	Information System Activity Review	■		
Workforce Security HIPAA 164.308(a)(3)(i)	Authorization and/or Supervision	■		
	Workforce Clearance Procedures	■		
	Termination Procedures	■		
Information Access Management HIPAA 164.308(a)(4)(i)	Isolating Healthcare Clearinghouse Function	N/A	N/A	N/A
	Access Authorization	■		
	Access Establishment and Modification	■		
Security Awareness and Training HIPAA 164.308(a)(5)(i)	Security Reminders			■
	Protection from Malicious Software			■
	Log-in Monitoring			■
	Password Management			■

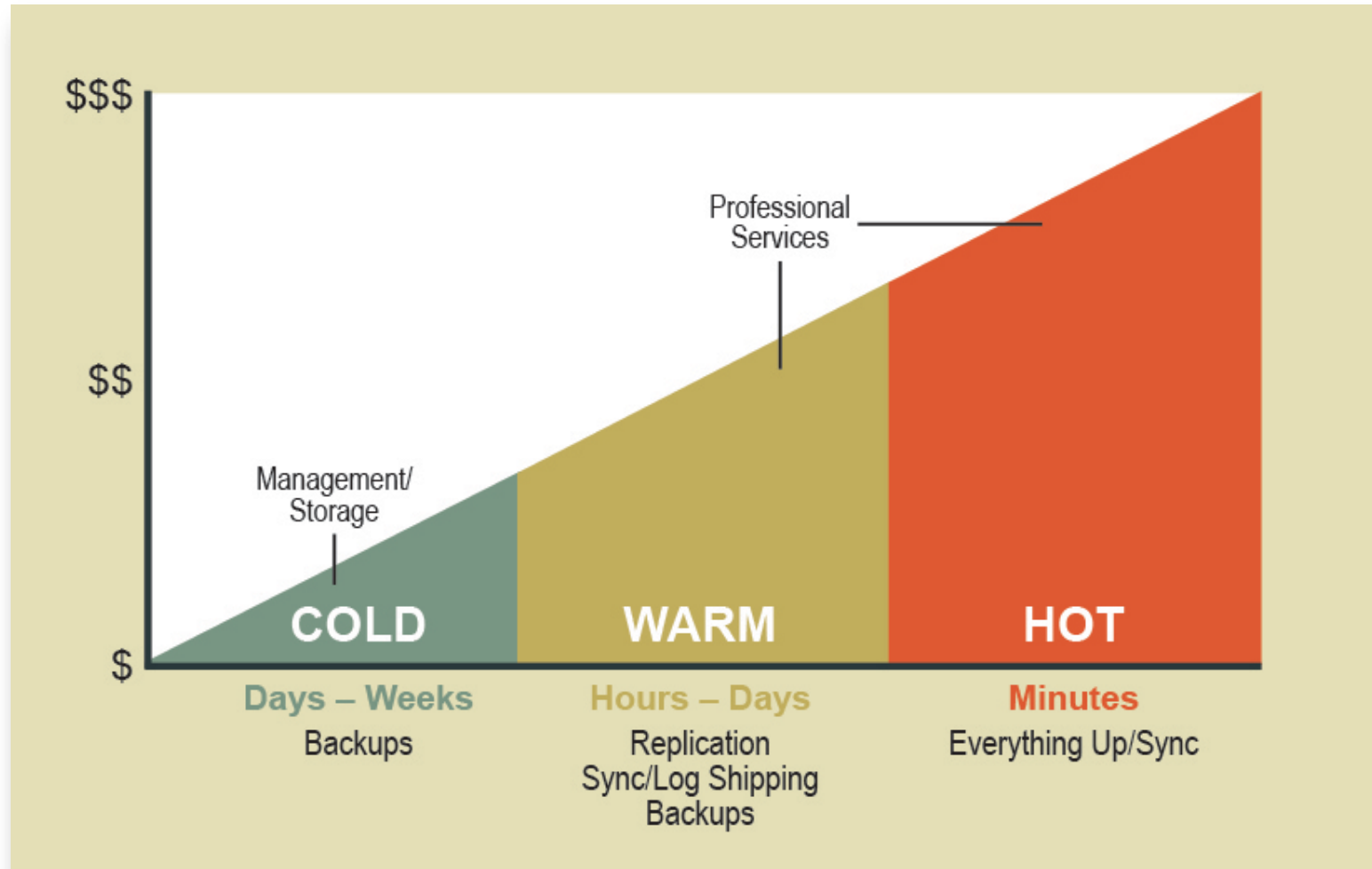
Example requirements: Physical Security

Standard	Requirement	ES	Client	Both
Facility Access Controls HIPAA 164.310(a)(1)	Contingency Operations	■		
	Facility Security Plans	■		
	Access Control and Validation Procedures	■		
	Maintenance Records	■		
Device and Media Controls HIPAA 164.310(d)(1)	Disposal	■		
	Media Re-use	■		
	Accountability	■		
	Data Backup and Storage			■

Example requirements: Technical Safeguards

Standard	Requirement	ES	Client	Both
Access Control HIPAA 164.312(a)(1)	Unique User Identification	■		
	Emergency Access Procedure	■		
	Automatic Logoff	■		
	Encryption and Decryption		■	
Integrity HIPAA 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information		■	
Transmission Security HIPAA 164.312(e)(1)	Integrity Controls			■
	Encryption			■

RTO decision drives your options

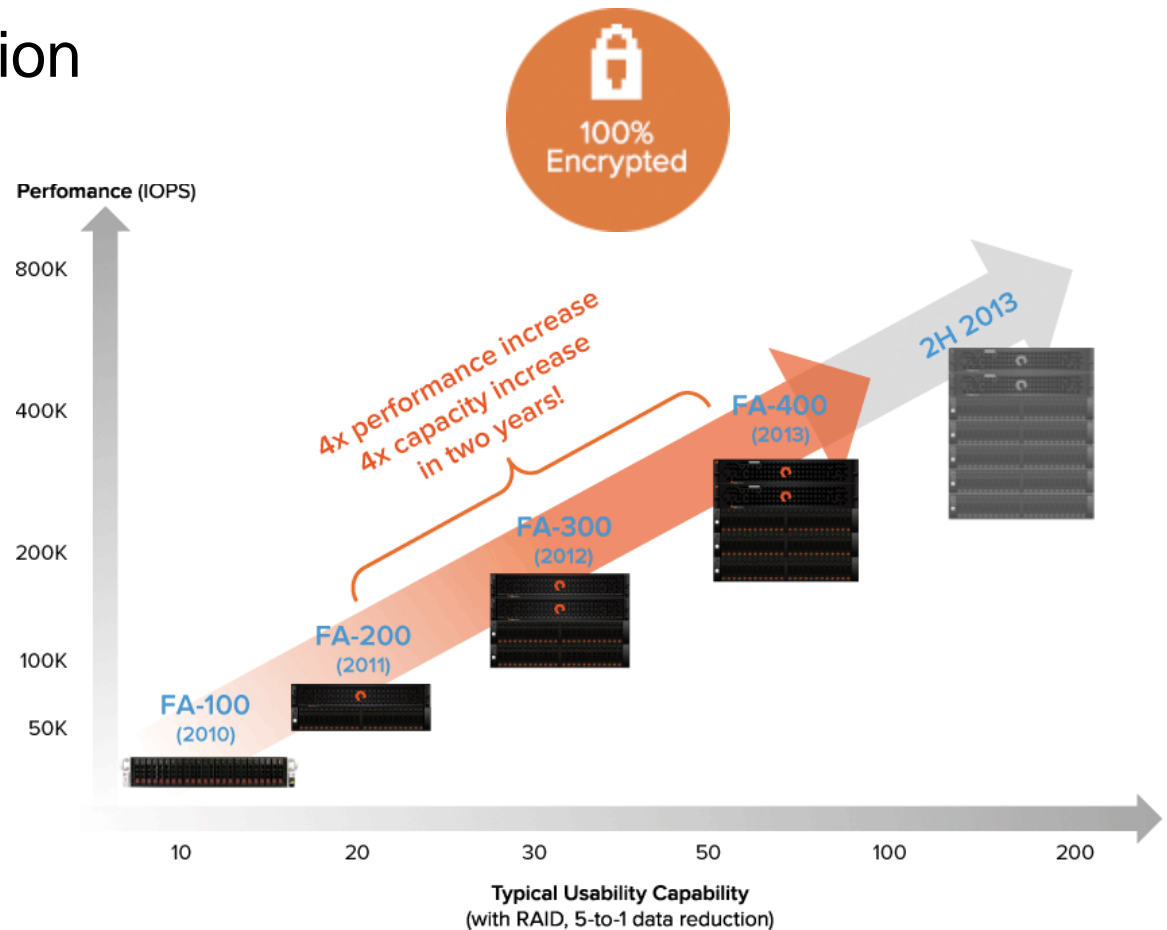


New technologies ease compliance

→ SSD with flash storage

→ Always on encryption

- Meets data-at-rest requirement
- Protects against drive theft or loss in transit or maintenance
- A combination of software-based and ASIC-accelerated encryption for no performance loss



Customer example #1

→ Oregon-based Hospital

- Large skilled internal IT staff
- Significant assets already in place
- Hardware refresh provided opportunity to improve DR

→ Solution

- Primary infrastructure in EasyStreet colocation
- 9-cabinet cage
- Redundant/diverse connectivity
- DR infrastructure located at hospital site
- Data replication/DR playbook managed by hospital IT



Customer example #2

- Arizona-based healthcare provider
 - New “green-field” clinical information system
 - Complicated modern application
 - Extremely high availability/performance required
- Solution
 - HOT/HOT Disaster Recovery Solution (RPO 1 hour, RTO 4 hours)
 - Identical dedicated private clouds in Beaverton and Phoenix
 - Multiple replication techniques used
 - Database / storage / hypervisor based
 - DR playbook jointly developed by customer and EasyStreet



Recap

- “The cloud” delivered as Infrastructure-as-a-Service is an excellent option for healthcare organizations
- Ensure you’re in compliance with your IaaS provider
 - Have them sign a Business Associate agreement
 - Request a Responsibility Matrix
- Your IaaS provider can help balance the risk/cost/speed or hot/warm/cold requirements that are right for your organization
- New technologies overcome risk/cost/speed limitations
 - Inline encrypted storage

Thank you!

- Call 503-671-1884
- Email gdoswald@easystreet.com

