FDA, EU and Global Guidance for CSV, Data Integrity, Cloud Computing and Mobile Applications

December 1, 2015

Ludwig Huber
E-mail: Ludwig_Huber@labcompliance.com

Today's Agenda

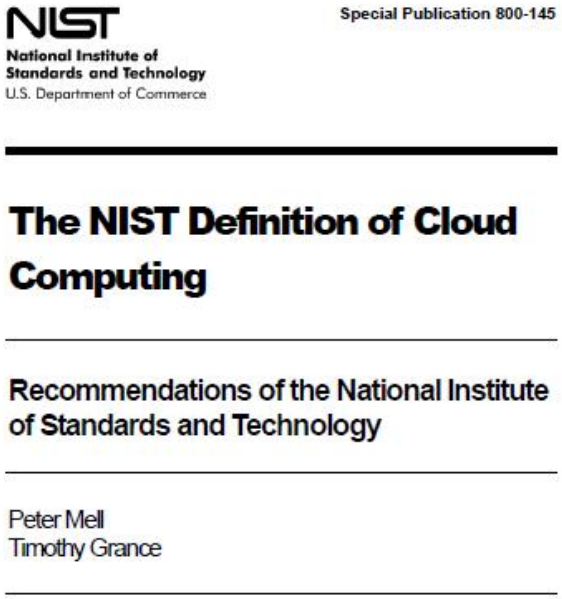
- Cloud Computing
  - Expectations to FDA
  - Industry guidance
- Mobile (medical) applications
  - FDA and Industry Guidance
  - Regulatory approach
- Part 11 and data Integrity
  - History and future of Part 11
  - Key inspection issues
- EU/PICS GMP Annex 11
  - Similarity, difference to Part 11

Cloud Computing

- Industry expectations
- Advantages and risks
- Deplyoment and service models
- FDA task force on Cloud Computing
- Industry Guidance
  - ISPE/GAMP publications

NIST Cloud Definition

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


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance

NIST 800-145

National Institute for Standard and Technology

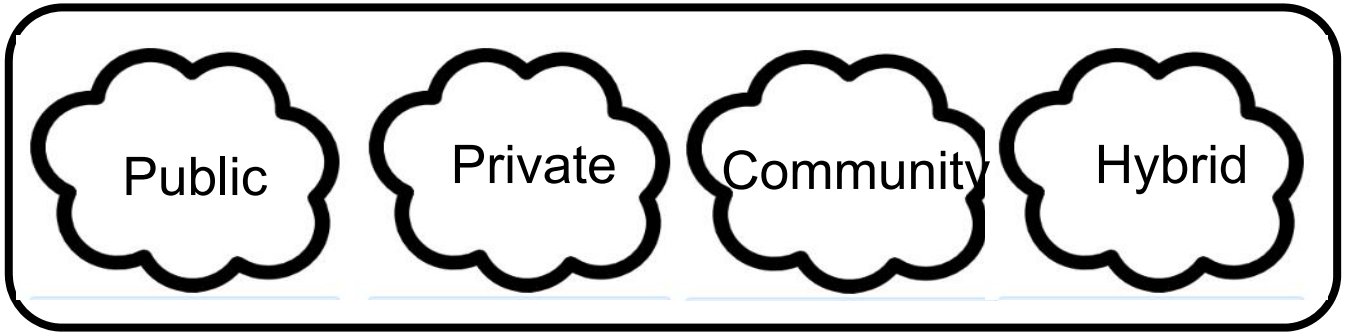
Cloud Computing - Advantages

- Elastic capacity
  - Based on actual demand
- Economic
  - Pay what you use
- Lower investment cost
  - Reduced IT resources
  - Reduced IT hardware / software cost
- Increased availability
  - (Close to) 100%
- Faster Project deployment

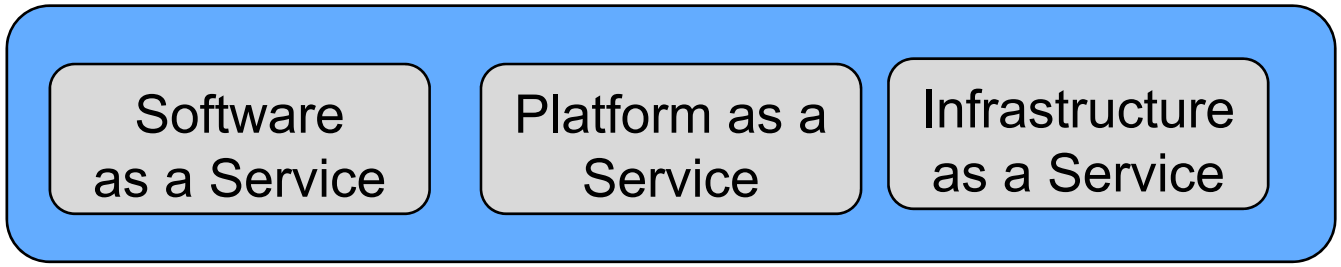
Cloud Computing – Issues and Risks

- Dependent on service provider
  - Confidentiality
  - What happens with ‘deleted’ data, are they ever fully destroyed?
- Regulatory requirements not clear
  - Unknown location of regulated data
- Need live internet connection
  - Availability, cost, speed, uptime
- Reported problems with external services
  - Availability of Cloud applications,
  - Data loss
  - Access to data
- Problems with data migration
  - When changing the cloud provider

NIST Models of Cloud Computing



Deployment Models



Service Models

- **On demand self service**
- **Broad network access**
- **Rapid elasticity**
- **Measured service**

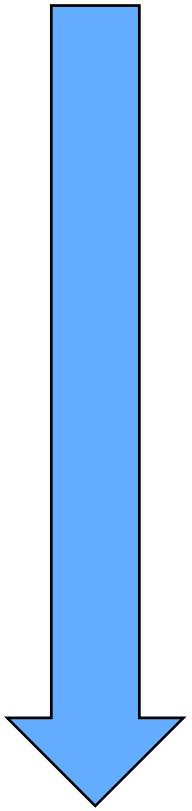
Resource Pooling with minimal management effort

Essential Characteristics

Ref: Visualized based on text in NIST Guide 800-145

Cloud Deployment Models

- Internal private cloud
  - Cloud is within the user company
  - Administrated by the user
- External private cloud
  - Administrated by external service provider exclusively for the user
- Community cloud
  - Administrated and exclusively used by community with shared interest
- Public cloud
  - Administrated by provider company
  - Available to the public (everybody)
- Hybrid cloud
  - Combination of 2 or more of the first 3 models



Cloud Services

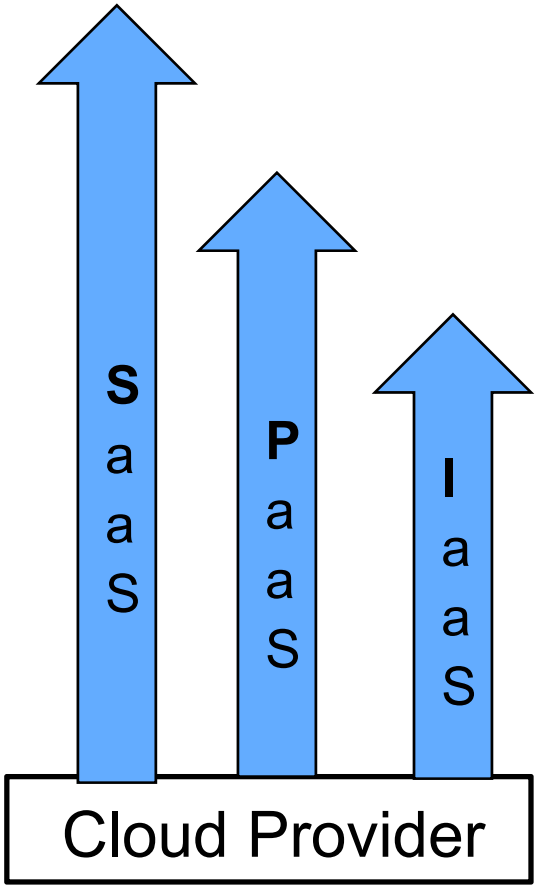
- Software as a Service (SaaS)
  - User uses the providers software and platform running in the cloud
  - User does not manage or control the underlying infrastructure and software
  - User can configure the software for special needs

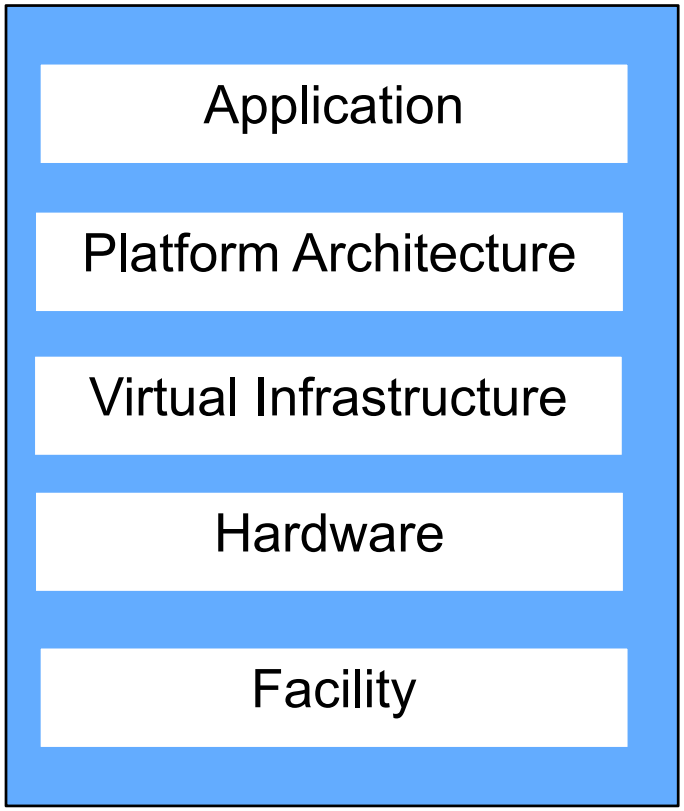
- Platform as a service (PaaS)
  - User owns and controls application software and data
  - Software runs on platform and infrastructure owned and administrated by the provider

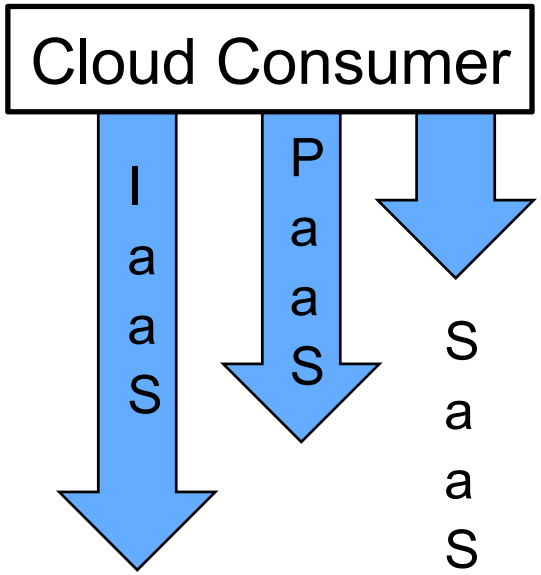
Cloud Services

- Infrastructure as a service (IaaS)
  - The user uses the provider's hardware and fundamental computing resources, e.g., memory, storage devices, firewalls, networks
  - The user owns, deploys and runs operating system and application software
  - User does not manage or control underlying infrastructure
  - User has control over operating system, storage and deployed applications

Scope and Control







Ref: NIST

The higher the level of Support from the cloud provider, the more narrow the scope and control the cloud consumer has over the system

S,P,I - Software, Platform, Infrastructure as a Service

Risks in SaaS and Cloud

- Risks involved
  - Login security
  - Access to audit trails
  - Data storage location
    legal issues, dependent on external laws
  - Data recovery
- Perform risk assessment to address all risks
- Qualify vendor and determine how the vendor handles risks

GMP Requirements

- Network infrastructure must be qualified (Annex 11)
- Applications must be validated (Part 11, Annex 11)
- Infrastructure hardware must be identified
- Data must be ‘readily’ available, at any time
- Location of data must be known
- Data security and integrity must be ensured
- Changes must be handled under change control procedures
- IT administrators need to be formally trained on GMP

Users must have control over IT infrastructure and software applications supported by the infrastructure either directly or through agreements

FDA Checklist (incomplete)

#	Check	Yes/no
1	Is there a design specification for the software and system?	
2	Has the software and system been developed in a QC environment?	
3	Is there a system inventory with serial numbers etc.?	
4	Are changes to the infrastructure made following a change control procedures and are the changes recorded in a change log?	
5	Is access to system and data limited to authorized individuals?	
6	Is the location of all regulated data known to the user?	
7	Is there a documented maintenance program?	
8	Is the service provider staff trained on GMP?	
9	Has the selected cloud service been qualified	
10	Are there service level agreement with FDA regulations in mind?	

Cloud Services – Summary Recommendations for Validation

- Software as a Service (SaaS)
  - Look at computer system validation practices
  - Look at Part11/Annex11 compliance for e-records
- Platform as a service (PaaS)
  - Check operating system and utilities and
  - Account, patch and configuration management
- Infrastructure as a service (IaaS)
  - Need good infrastructure qualification plan
  - Includes network hardware, software, topology, configuration, security

Cloud Computing and the FDA

- Task force from 2012-2015
- Task force leader
  Krishna Ghosh, Ph.D. FDA/ CDER/ Office of Compliance
- Two presentations from Krishna Gosh
- “Cloud Computing and Data Security A Regulatory Perspective”
  - ISPE Meeting, 2013
  - IVT CSV Conference 2014
- Emphasis on 21 CFR Part 211and Part 11
- Task Force discontinued in 2015
- Refers to the GAMP SIG with extension of GAMP5 to Cloud

Mobile Health Applications

- According to industry estimates, 500 million smartphone users worldwide will be using a health care application by 2015, and by 2018, 50 percent of the more than 3.4 billion smartphone and tablet users will have downloaded mobile health applications These users include health care professionals, consumers, and patients.

http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/default.htm#ahttp://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/default.htm#a

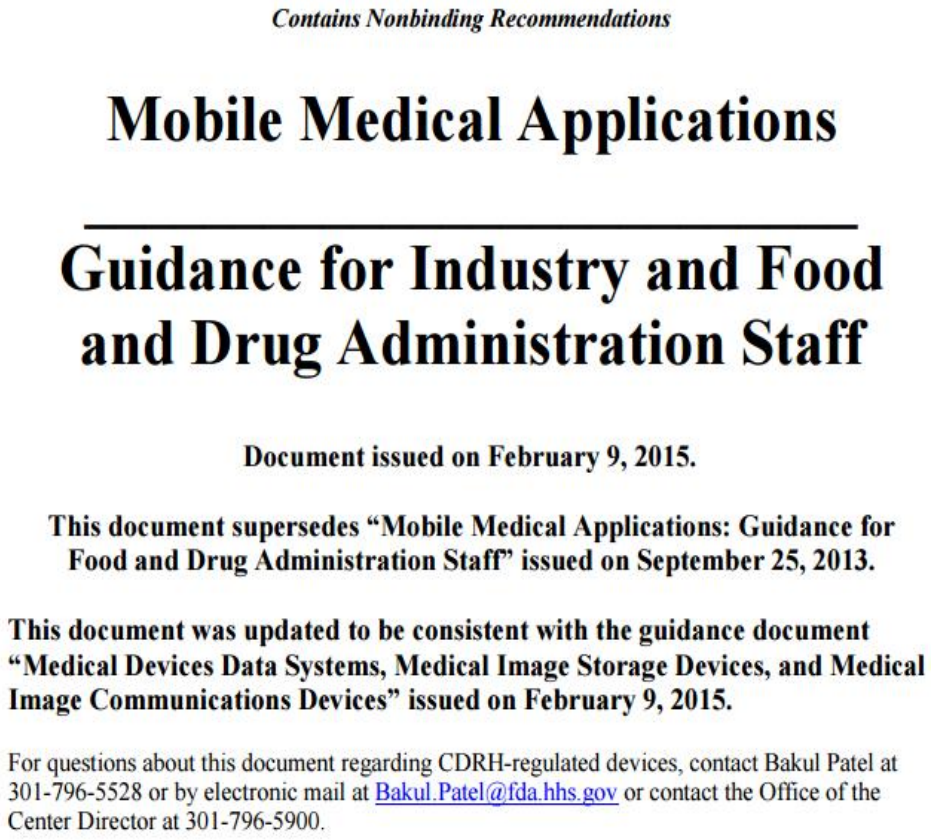
Mobile Apps

- Mobile apps are software programs that run on smartphones and other mobile communication devices. They can also be accessories that attach to a smartphone or other mobile communication devices, or a combination of accessories and software.

http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/default.htm#ahttp://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/default.htm#a

FDA Guide on Mobile Medical Applications

- Introduction
- Background
- Definitions
- Scope
- Regulatory approach for mobile Apps
- Regulatory requirements
- Appedix A:, B, C, D, E,F,G with examples
  e.g., examples for healthcare apps that are and that are not medical devices



Contains Nonbinding Recommendations

Mobile Medical Applications

Guidance for Industry and Food and Drug Administration Staff

Document issued on February 9, 2015.

This document supersedes "Mobile Medical Applications: Guidance for Food and Drug Administration Staff" issued on September 25, 2013.

This document was updated to be consistent with the guidance document "Medical Devices Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices" issued on February 9, 2015.

For questions about this document regarding CDRH-regulated devices, contact Bakul Patel at 301-796-5528 or by electronic mail at Bakul.Patel@fda.hhs.gov or contact the Office of the Center Director at 301-796-5900.

Regulatory Approach

- FDA intends to apply its regulatory oversight to only those mobile apps that are medical devices and whose functionality could pose a risk to a patient's safety if the mobile app were to not function as intended.
- The FDA strongly recommends that manufacturers of all mobile apps that may meet the definition of a device follow the Quality System regulation (Part 820)
- For mobile medical apps, manufacturers must meet the requirements associated with the applicable device classification

GAMP Good Practice Guide A Risk Based Approach in Regulated Mobile Applications

Purpose

- Intended to provide a risk based approach to implementing and supporting regulated mobile apps

Scope

- Mobile medical apps that meet the definition of a medical device
- Mobile apps that are used as part of GxP operations at a regulated company, as a component of a GxP regulated computerized systems, such as an interface to an instrument or control system

Data Integrity and Part 11

Pre-part 11 inspections

Part 11 history

- Release, changing approach
- Part 11 inspection assignment

Part 11 Inspections focus 2012-2014

Guidances

- Released: WHO, MHRA
- Under development PIC/S, GAMP SIG?

Pre-Part 11 Inspections

1994

- Operations that could affect the **integrity of chromatographic data files collected and processed by the data acquisition** system **are not controlled by electronic audit trails** that maintain who, why and what was changed to anygiven sample record.
- There are insufficient security measures in effect to ensure the integrity of chromatographic data housed in the Quality Control Laboratory.
- There is no post-login security to prevent users from accessing all data files.
- Data is not stored in personal accounts protected by operating systems access controls, and all users have read/write access to the data scored on each hard drive
- The firm lacks the controls necessary to **ensure the integrity of raw data** generated by the laboratory computer system

www.fdawarningletter.com W-283

Part 11 – Past, Present and Future

1997	Part 11 released
1999-2003	Heavy enforcement according to letters of the rule started in 1999
2003	New interpretation according to new guidance: Scope and Applications
2003	Announcement of the new Part 11
2003-2006	Enforcement stopped
2006-2010	Enforcement starts again
2010/2012	Part 11 Inspection assignments program
2013/2014	Focus on data integrity and security
2015	Lots of industry activities related to data integrity

2003 - FDA Changes Approach

- Part of FDA's 21st century drug CGMP initiative
- Documented in Part11 guidance: Scope and applications
- All existing Part 11 guides removed
- Narrow scope of Part 11
  - Narrowed from all electronic records to records required by predicate rules - risk based implementation
- Enforcement discretion for validation – audit trails – audit trails - copies of records record retention, legacy systems
- Warning letters to be approved by FDA headquarter
- New Part 11 announced for 2005

FDA Compliance Update

31st International GMP Conference - Athens, March 14, 2007

- Presentation from Edwin Rivera Martinez, Chief Investigations and Preapproval Compliance Branch

"Data Integrity and Fraud - Another Looming Crisis?"

Problems found in 2005

- Biased manipulation of study data resulting in the acceptance of failed runs
- **Intentional computer manipulations** of chromatograms by cutting and pasting chromatographic data so that initial out-of-specification test results are brought into specifications

FDA Compliance Update

Problems found:

- Altering weights of samples and standards in analytical calculations
- Changing chromatogram processing parameters
- **Manipulation of chromatograms by lab chemists** without justification and changing calculations **to bring out-of-specification results within specifications**
- The chemists then placed the in-specification assay results into the batch production and control record

- 31st International GMP Conference - Athens, March 14, 2007

Presentation from Edwin Rivera Martinez, Chief Investigations and Preapproval Compliance Branch

"Data Integrity and Fraud - Another Looming Crisis?"

FDA Compliance Update

- Ten audits were assigned to ORA field offices and completed
- Three of the ten audits revealed data of highly questionable reliability that are currently under review by CDER's OC
- Second audit assignment to be issued shortly

31st International GMP Conference - Athens, March 14, 2007

- Presentation from Edwin Rivera Martinez, Chief Investigations and Preapproval Compliance Branch

"Data Integrity and Fraud - Another Looming Crisis?"

What is the FDA Doing?

- Specialized training of investigational staff on uncovering data integrity, data manipulation and fraud
- PAIs to focus more on data integrity and fraud
- Agency committed to follow-up on leads or information regarding data manipulation and fraud

31st International GMP Conference - Athens, March 14, 2007

- Presentation from Edwin Rivera Martinez, Chief Investigations and Preapproval Compliance Branch

“Data Integrity and Fraud - Another Looming Crisis?”

What Industry can do

- Train employees on proper data handling and reporting
- Assure the reliability of data reported in applications and manufacturing records
- Emphasize that everyone in the company is responsible for data integrity

31st International GMP Conference - Athens, March 14, 2007

- Presentation from Edwin Rivera Martinez, Chief Investigations and Preapproval Compliance Branch

“Data Integrity and Fraud - Another Looming Crisis?”

FDA Warning Letter 2006

Hybrid system

- Operating parameters were maintained with the relevant xxx. However, electronic raw data was not saved (www.fdawarningletter.com W-167).

Electronic raw data not saved

21 CFR Part 211: (e) Complete records shall be maintained of all stability testing performed in accordance with Sec. 211.194 (e).

Predicate rule

Study regulation and check if the print-out has all records

Part 11 – Past, Present and Future

1997	Part 11 released
1999-2003	Heavy enforcement according to letters of the rule started in 1999
2003	New interpretation according to new guidance: Scope and Applications
2003	Announcement of the new Part 11
2003-2006	Enforcement stopped
2006-2010	Enforcement starts again
2010/2012	Part 11 Inspection assignments program
2013/2014	Focus on data integrity – is there a new regulation?
2015	Lots of activities related to data integrity - Guidance, literature, workshops, conferences -

Data Integrity Guidances

- MHRA, 16 pages, March 2015 (final)
- WHO, draft
- PIC/S proposal
- GAMP SIG (under disussion)

Comparison Annex 11with Part 11

Par.	Annex 11	Part 11
1	Risk Management throughout the lifecycle	Part 11 Guide
2	Personnel qualification and responsibilities	x
3	Supplier Management e.g., formal agreement	
4	Validation throughout the life-cycle	Less details
5 / 6	Built-in checks for data entry	
7 / 17	Data storage – Archiving – Back-up	x
8	Print outs	Part 11 Guide
9	System audit trails according to risk	x
10	Change/configuration. management	
11	Periodic evaluation	
12	Security through restricted access to systems &data	x
13	Incident management	
14	Electronic signatures	x
15	Batch release	
16	Business continuity	

Suppliers and Service Providers Annex 11

3. Suppliers and Service Providers

- 3.2 The **competence and reliability** of a supplier are key factors when selecting a product or service provider. The need for an **audit** should be **based on a risk** assessment.
- 3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.

For More information sign up for our one-hour on-demand recorded seminars

- Validation and Use of Cloud Computing in FDA&EU Regulated Environments
  www.labcompliance.com/seminars/audio/351
- FDA's New Enforcement of Part 11
  www.labcompliance.com/seminars/audio/364
- Ensuring Integrity of Laboratory Data for FDA/EU Compliance
  www.labcompliance.com/seminars/audio/366
- Understanding and Implementing the New EU Annex 11
  www.labcompliance.com/seminars/audio/350

All seminars come with PPT file, 10 best practice guides (SOPs, checklists) and script

LabCompliance