Welcome to our E-Seminar:

Risk-based Approach to Part 11 and GxP Compliance
Common Discussion

• Q: Do I really need to do this?
• Possible Answers
• A: Of course! (QA)
• B: Who cares, I have work to do! (Engineering)
• C: No way! (IT)
• D: It depends! (FDA)

Pharmaceutical cGMPs for the 21st Century

• Announced August 21, 2002
• Two year program
• Merges science-based risk management with an integrated quality system approach
• Will not interfere with current enforcement
• Will be implemented in multiple steps
• Changes to part 11 were pre-announced in late 2002

Goal: Optimize FDA resources
Part 11 is NOT Going Away!!

- **Risk-based compliance approach** – FDA will scrutinize areas with high impact on product quality according to existing GxP
- *FDA will continue enforcing predicate rules (GxP)*
- *Validation, change control and training* are required for GxP-relevant systems
- *Access security, device checks, operational checks* for trustworthy and reliable records are still mandatory technical controls
- *Audit trail, copies of electronic records, record retention, legacy systems* are not a key focus area for FDA enforcement
- *Electronic signature requirements* are unchanged
<table>
<thead>
<tr>
<th>Description</th>
<th>Category</th>
<th>Predicate Rule Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production, control, laboratory records to assure that drug products</td>
<td>GMP</td>
<td>21 CFR 211.180</td>
</tr>
<tr>
<td>adhere to established specifications. Records for components, drug</td>
<td></td>
<td></td>
</tr>
<tr>
<td>product containers, labeling etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment cleaning and use log</td>
<td>GMP</td>
<td>21 CFR 211.182</td>
</tr>
<tr>
<td>Master production and control records</td>
<td>GMP</td>
<td>21 CFR 211.186</td>
</tr>
<tr>
<td>Batch production and control records</td>
<td>GMP</td>
<td>21 CFR 211.188</td>
</tr>
<tr>
<td>Production record review</td>
<td>GMP</td>
<td>21 CFR 211.192</td>
</tr>
<tr>
<td>Laboratory records</td>
<td>GMP</td>
<td>21 CFR 211.194</td>
</tr>
<tr>
<td>Protocol for a non-clinical laboratory study</td>
<td>GLP</td>
<td>21 CFR 58.120</td>
</tr>
<tr>
<td>Reporting of non-clinical laboratory results</td>
<td>GLP</td>
<td>21 CFR 58.185</td>
</tr>
<tr>
<td>Raw data, documentation, protocols, final reports, QA inspection records,</td>
<td>GLP</td>
<td>21 CFR 58.195</td>
</tr>
<tr>
<td>job descriptions, training records, instrument maintenance, calibration and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>inspection records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supporting records for INDA and records described by ICH GCP Guidelines</td>
<td>GCP</td>
<td>21 CFR 312.57</td>
</tr>
<tr>
<td></td>
<td></td>
<td>21 CFR 312.62</td>
</tr>
<tr>
<td>Ensure that the systems are designed to permit data changes in such a</td>
<td>GCP</td>
<td>ICH GCP 5.5.3 c)</td>
</tr>
<tr>
<td>way that the data changes are documented and that there is no deletion of</td>
<td>GMP</td>
<td>European GMP Guide Annex 11 §10</td>
</tr>
<tr>
<td>entered data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>List of individuals authorized to make data changes</td>
<td>GCP</td>
<td>ICH GCP 5.5.3 e)</td>
</tr>
</tbody>
</table>
### Part 11 Requirements

<table>
<thead>
<tr>
<th>Section</th>
<th>Requirement</th>
<th>Responsibility*</th>
</tr>
</thead>
<tbody>
<tr>
<td>§11.10a</td>
<td>Systems must be validated</td>
<td>Proc.</td>
</tr>
<tr>
<td>§11.10b</td>
<td>Accurate and complete copies</td>
<td>Tech.</td>
</tr>
<tr>
<td>§11.10c</td>
<td>Protection of records</td>
<td>Proc., Tech.</td>
</tr>
<tr>
<td>§11.10d</td>
<td>Access limited to authorized individuals</td>
<td>Proc., Tech.</td>
</tr>
<tr>
<td>§11.10e</td>
<td>Secure, computer-generated, time-stamped audit trail</td>
<td>Tech.</td>
</tr>
<tr>
<td>§11.10f/g/h</td>
<td>Checks (device, authority, system checks)</td>
<td>Tech.</td>
</tr>
<tr>
<td>§11.50</td>
<td>Signature Manifestations</td>
<td>Tech.</td>
</tr>
<tr>
<td>§11.70</td>
<td>Signature/Record Linking</td>
<td>Tech.</td>
</tr>
<tr>
<td>§11.100</td>
<td>Uniqueness of e-sig to the individual</td>
<td>Proc., Tech.</td>
</tr>
<tr>
<td>§11.200</td>
<td>E-Sig Components and Controls</td>
<td>Proc., Tech.</td>
</tr>
<tr>
<td>§11.300</td>
<td>Controls for identification codes and passwords</td>
<td>Proc., Tech.</td>
</tr>
</tbody>
</table>

* Proc. = Pharmaceutical company is usually responsible to develop procedural controls  
Tech. = Supplier is usually responsible to implement technical controls

---

**Agilent Technologies**  
Chairperson: John Vis

---

= Enforcement Discretion (August 2003 Guidance)
New Part 11 Guidance - Summary

- **New guidance is most relevant for low risk systems** (e.g. word processor - “typewriter excuse”)
- **Minor changes for high risk systems,** e.g. Chromatography Data Systems
- **Requirement for long term reprocessing** (>5 years) may go away
- **Users are required to perform risk assessments for just about everything**
When Part 11 Applies

Guidance Aug-27, '03

.Predicate Rule Requirements + Regulated Activity + Business practices

GxP Requirement?

yes

Used for regulated activity?

yes

Maintain e-records for business?

yes

PART 11

Out of scope

Out of scope

Out of scope
The regulatory concern is product quality and safety.

The regulations specify the data and records required to assure product quality.

The validation and qualification of systems assures data and record quality.

The validation and qualification of infrastructure assures system reliability.
• “...We recommend that you base your approach on a justified and documented risk assessment and a determination of the potential of the system to affect product quality and safety and record integrity...”

• For instance, a word processor used only to generate SOPs would most likely not need to be validated.

Validate all automated computer systems that affect GxP type records (old and new systems).
Audit trail is required by some predicate rules.

- **We recommend that** your decision on whether to apply audit trails, or other appropriate measures, be based on the need to comply with predicate rule requirements, a justified and documented risk assessment, and a determination of the potential impact on product quality and safety and record integrity.

- **Audit trails are particularly important where the users are expected to** create, modify, or delete regulated records during normal operation.
The ... program runs across a LAN... The firm presented a diagram in support of the validation status for this LAN. The diagram provides graphical representation of the current I/O wiring (node lists) for each of the various devices of this LAN. Regarding this diagram

- The diagram lacks review by the quality unit
- The diagram has not been maintained following established document control procedures
- The diagram has been produced using I/O data contained within the non-validated excel node list database, which ... is not a controlled record

Ref: O.Lopez, Philadelphia 2002
• **The firm utilizes a Wide Area Network (WAN) to connect all Local Area Networks (LAN’s). The WAN is not validated as described below.**
  
  • The Quality unit has failed to ensure that procedures are in place, *which define all system definition documentation, which must be maintained for the WAN.*
  
  • The Quality unit has failed to ensure that complete WAN system definition documentation is included in WAN documentation. For example, the Quality unit has *failed to ensure that the WAN validation documentation includes WAN site diagrams.*
  
  • When requested, the firm could produce no approved WAN site diagrams. The Quality unit has failed to put in place procedures, which define that WAN site diagrams are maintained.
(Networked) system testing was not conducted to ensure that each system as configured could handle high sample rates.

Validation of the (networked) system did not include critical system tests such as volume, stress, performance, boundary, and compatibility.

Ref: www.fdawarningletter.com
Examples From Network Related 483 Observations

- Wide Area Network diagrams (WAN) with appropriate definition documentation identifying corporate sites on the network that use XXX have not been included in any XXX validation documents
- Validation of the system did not include critical system tests such as volume, stress, performance, boundary, and compatibility
- Validation documentation failed to include complete and updated design documentation, and complete wiring/network diagrams to identify all computers and devices connected to the ... system
Before August 2003
• **Part 11 applies to all systems that manage e-records in a regulated firm**

After August 2003
• **Predicate rule requirements, documented risk assessment and business use determine whether Part 11 applies**
• **Low risk systems may fall out of scope for Part 11**

<table>
<thead>
<tr>
<th>High risk</th>
<th>Medium risk</th>
<th>Low risk</th>
<th>No risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Key Focus Areas for FDA Enforcement**

**Guidance Aug-27, ’03**
Break Number 1

Question & Answer Session

Please type your question into the Question Box at any time during the presentation.
A “risk” is a potential problem, but a “problem” is a risk that really happened.
Risk Management

Risk Management Plan

Risk Analysis

Risk Evaluation

Risk Mitigation/Control

On-going Evaluation

- Identify the system
- Identify hazards and possible harms
- Estimate, justify and document risk level (probability/severity)
- Estimate costs of mitigation vs. non-mitigation
- Define and take actions for mitigation
- Monitor for new harms
- Monitor risk levels
- Update plan and take actions

Key criteria: product quality (public health), business continuity
www.labcompliance.com/books/risk

Chairperson: John Vis
• Use tables with description of risks, severity, probability and the rationale behind
• Calculate overall risk factor (severity, probability)
• Classify factors in high, medium and low

<table>
<thead>
<tr>
<th>Risk description</th>
<th>Severity</th>
<th>Justification</th>
<th>Probability</th>
<th>Justification</th>
<th>Risk factor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk Prioritization Example: QC Lab Data System

Production control Records

Sample receipt and log in
Sample analysis
Review and approval

Impact on product quality: DIRECT
Regulated activity based on: E-Records

High Risk

Agilent Technologies

Chairperson: John Vis
## Infrastructure Risks and Mitigation

<table>
<thead>
<tr>
<th>Risk (Cause)</th>
<th>Mitigation</th>
</tr>
</thead>
</table>
| Data Loss (network failure) | • Redundant setup  
• Continuous health monitoring |
| Data Corruption (operational errors, transmission errors due to out-of-spec components) | • Compliance with technical standards  
• Physical and logical segregation of subnets |
| Data Insecurity (inadequate controls) | • Security procedures (security policies, password policies)  
• Technical security (firewalls, virus protection, access control lists) |
### Example: GAMP Risk Level Categories

#### Likelihood

<table>
<thead>
<tr>
<th>Severity</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td></td>
<td></td>
<td><strong>WAN</strong></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Probability of Detection

<table>
<thead>
<tr>
<th>GAMP Risk Level</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td><strong>WAN</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: ISPE GAMP Forum

Chairperson: John Vis
## Validation Rigor Increases with Vulnerability

<table>
<thead>
<tr>
<th>Class of System</th>
<th>Vulnerability/Validation Rigor</th>
<th>Plan/Report</th>
<th>Design Phases</th>
<th>Qualification Phases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Software Application</td>
<td>High</td>
<td>- Validation Plan and Report Development - SOPs Supplier Audit - Periodic Review - Change Control</td>
<td>- URS (business and regulatory needs) - FS (Full functionality of the system) - Design down to module specifications - Design Review Process -- Source Code Reviews Traceability Matrix</td>
<td>- Detailed Risk Assessment against operational aspects - Comprehensive positive functional testing - risk-focused negative functional testing</td>
</tr>
<tr>
<td>COTS Application</td>
<td>Medium</td>
<td>- Validation Plan and Report Development SOPs - Supplier Audit - Periodic Review - Change Control</td>
<td>- URS (business and regulatory needs) - FS (Full functionality of the system) - Design documents (application configuration aspects only) - Design Review Process -- Traceability Matrix</td>
<td>- High level Risk Assessment against operational aspects of processes - Positive functional testing - risk-focused negative functional testing</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Low</td>
<td>- SLA - Quality and Compliance Plan - Work SOPs - Periodic Review - Change Control</td>
<td>- Network topology diagram - Network definition (list of supported applications, network performance, security requirements)</td>
<td>- High level Risk Assessment against operational aspects of processes - risk-focused functional testing (e.g. Security controls, data integrity, backup and recovery)</td>
</tr>
</tbody>
</table>

Source: ISPE GAMP Forum (Pharmaceutical Engineering, May/June 2003, Volume 23 (3), page 24

Chairperson: John Vis
Example: Networks as System Components

- **Network Communication is Integral to Modern Systems Design**
- **Network Performance Directly Affects Application Performance**
- **Point Errors Can Affect Your Ability to Complete Critical Tasks**
- **If Critical Tasks Slowed There is a Business Cost**
- **Regulators View Data at Risk as Product Quality at Risk**

Business Impact can be High
Specifying a Networked System

To be answered by the anticipated users

- Operating environment
- Security requirements (physical and logical controls, authentication, encryption, biometrics?)
- Capacity (sites, users, volumes)
- Performance (response times, latency)
- Reliability (risks, up-time, redundancy, data integrity)
- Standards to be used: Protocols, cabling, design considerations, operating procedures)
Qualification Phases

- **Design Qualification**
  - User requirement specifications
  - Functional specifications
  - Vendor qualification

- **Installation Qualification**
  - Check arrival as purchased
  - Check installation of hardware and software

- **Operational Qualification**
  - Test of key functions
  - Requalification

- **Performance Qualification**
  - Test for specified application
  - Preventive maintenance
  - On-going performance tests


Detailed content and ordering: [www.labcompliance.com/books/validation3](http://www.labcompliance.com/books/validation3)
Example: Qualification Phases for Networks

**DQ**  The network is suitable for the applications
  – The design matches the intended use

**IQ**  Verifying and documenting static network topology
  – The implementation matches the design

**OQ**  Dynamic topology verification and capacity testing
  – The implementation operates properly

**PQ**  Measuring the network in use
  – Determining that the risk of failure in use is low
The Four Cs of a Quality Network

**Connection**
- Each device can connect as the application requires

**Communication**
- The devices can communicate through the connection

**Capacity**
- The network has sufficient capacity for quality communication

**Control**
- The network will continue to enable quality communication
• Direct Measurement Reduces Risk Faster than Documentation Alone
• Direct Measurement Verifies the Actual Network Quality
• End to End Communication Quality is the Key Metric

Look Inside Your Network!
Q: Do I really need to do this?

Possible Answers

A: Of course! (QA)
B: Who cares, I have work to do! (Engineering)
C: No way! (IT)
D: It depends! (FDA)

• **Part 11 is not going away**
• **You need to understand the regulatory requirements that affect your work-area**
• **You need to develop a gap and risk analysis**
  • Which Trouble Areas are the Greatest Risks
  • What Remediation is Required
• **The results affect your overall validation plan**
• **Validate applications, qualify infrastructure**
• **Ask your suppliers for help if you lack resources or expertise**
References and Recommended Reading

- [www.ispe.org](http://www.ispe.org) and [www.pda.org](http://www.pda.org): Good Practice and Compliance for Electronic Records and Signatures:
  - **Part 1:** Good Electronic Records Management (GERM), July 2002
References and Recommended Reading (2)

- Wolfgang Winter, Electronic records are here to stay, Biopharm Europe, Special Issue September 2002, 29-31
References and Recommended Reading (3)