



21 CFR Part 11, FDA's Guidance for Electronic Records & Electronic Signatures (ER/ES) for Regulated Computer Systems & Data

Carolyn Troiano

November 8, 2023

3-Hour Webinar (1:00pm – 4:00pm ET)

Part 1:

- ***21 CFR Part 11 Overview***
- ***Part 11 Compliance***
- ***“GxP” Systems***
- ***FDA Regulatory Oversight***
- ***Computer System Validation***

AGENDA (continued)

Part 3:

- ***Waterfall and Agile Methodologies***
- ***Computer Software Assurance (CSA)***
- ***Software and Medical Devices***
- ***COTS Packages***
- ***Cloud Services***
- ***Software-as-a-Service (SaaS) Solutions***
- ***10-Minute Break***

AGENDA (continued)

Part 5:

- ***Vendor Audit***
- ***FDA Inspection Trends***
- ***Industry Best Practice***

Wrap-Up:

- ***Q&A***
- ***Follow-up Items***

Part 1:

- ***21 CFR Part 11 Overview***
- ***Part 11 Compliance***
- ***“GxP” Systems***
- ***FDA Regulatory Oversight***
- ***Computer System Validation***

- **21 CFR Part 11** is a section in the Code of Federal Regulations (CFR) that sets forth the United States Food and Drug Administration's (FDA) guidelines on using:
 - ***Electronic Records (ER), and***
 - ***Electronic Signatures (ES)***



Key Takeaway:

Part 11 essentially allows any paper records to be replaced by an electronic record, and allows any handwritten signature to be replaced by an electronic signature

21 CFR Part 11 Overview (continued)

_____ public
safety in a *cost-effective* manner

Definitions:

- **Electronic Record:** Any combination of text, graphics, data, audio, or pictorial information represented in digital form that is created, modified, maintained, archived, retrieved or distributed by a computer
- **Electronic Signature:** A compilation of any symbol(s), when executed are the ***legally binding equivalent*** of an individual's handwritten signature and are used to verify:
 - ***Identity*** of the ***signer***
 - ***Intent*** of the ***signing***
 - ***Integrity*** of the ***data, document, or record***

- The regulation ***raised concerns*** about potentially ***restrictive use of technology*** & an ***increased cost of compliance***
- Industry concerns & confusion about the ***applicability, implementation, and enforcement*** led FDA to issue other guidances and documents
- In particular, the ***“Scope and Application” Guidance*** was released by FDA in 2003, but some aspects contradicted the 1997 rule

- **In 2010**, FDA began conducting **assessments** to evaluate industry's ER/ES application, understanding and compliance
- Software and instrumentation **vendors falsely claim** their **products are Part 11 "compliant"**
- A vendor can only provide **features and functions** of the system that will support a client's ability to validate the system in compliance with Part 11, but the **client** company **must validate** the system

Part 11 is a **law** that ensures that organizations define the **criteria** under which electronic records and signatures are **considered**:

- **Accurate**



- **Secure**



- **Authentic**



- **Trustworthy**



- **Reliable**



- **Confidential, if Personally Identifiable Information (PII)**

REQUIREMENT	ACCEPTANCE CRITERIA	CONTROLS (Technical & Procedural)
ACCURATE	Data must be correct, exact in all details, free from error, in accordance with fact and truth	Audit trails (structured data); version control (unstructured data)
SECURE	Data must be free from risk or harm	Role-based access; Users qualified; anti-virus/malware software; firewall; encryption for transmission; monitoring
AUTHENTIC	Data must be real or genuine, true, and accurate, not copied or false	Contemporaneously recorded; user authentication/access; audit trails; version control
TRUSTWORTHY	Data must be worthy of confidence, and dependable	Thoroughly tested all aspects of data flow; multiple rounds of testing
RELIABLE	Data must be suitable and fit for its intended purpose	SMEs define requirements, thoroughly test in simulated production environment following defined procedures
CONFIDENTIAL	Personally Identifiable Information (PII), must be kept private and identifying information unique to a person protected	PII identified/ protected through data workflow, reporting, transmission, viewing through access control/ security

REQUIREMENT	ACCEPTANCE CRITERIA	CONTROLS (Technical & Procedural)
CONFIDENTIAL	Personally Identifiable Information (PII), must be kept private and identifying information unique to a person protected	PII identified/ protected through data workflow, reporting, transmission, viewing through access control/ security

Data Privacy laws:

- ***General Data Protection Regulation (GDPR; EU)***
- ***Health Information Portability and Accountability Act (HIPAA)***
- ***California Privacy Rights Act (CPRA)***
- ***More than 700 privacy laws are currently in place globally***

Key Takeaways:

- ***Quality and Compliance built into everyday programs leads to inspection readiness***
- ***Think about how you treat compliance with paper systems before you take any action with ER/ES***



- For each record required to be maintained under predicate rules, ***determine in advance*** whether the electronic or paper record is the one to be used for ***decision-making***
- The determination should be ***documented*** (e.g., SOP) and included in ***training***
- ***Discuss with the vendor a range of features*** that must be in place to manage electronic records and processes



- ***There must be assurances for:***
 - Audit trail functionality
 - Identity management and assigned roles
 - Segregation of duties
 - Physical & logical security
 - Data integrity
 - Backup, restore, and archive
 - File format and record retention
 - System Change Control
 - Training
 - FDA Inspection and Audit



WHO
ARE
YOU?



Audit Trail:

- Know which ***user*** did what ***action*** and ***when***
- Know when ***records*** are created, modified, deleted, deactivated, or changed
- Record all ***events*** with the exact username, date, and time
- Enter a ***reason for the change***
- Part 11 is intended to provide ***fraud detection*** and know when changes have been made
- The ***audit trail*** allows the FDA to review your system and be provided ***proof*** of everything that has happened

- Prevent users from being able to ***modify or delete*** any audit trail

NEVER DELETE, only DEACTIVATE, and MUST HAVE DOCUMENTED JUSTIFICATION

- ***Synchronize*** the system date and time to an international standard (Meridian time; Greenwich Mean Time (GMT))
- ***Prevent users*** from being able to change the date or time
- ***Include*** the time zone, year, month, day, hour, and minute in the date and time stamp
- For legacy systems with software installed on a local device, must completely lock down the ability to change date/ time

Identity Management and Assigned Roles:

- These identify who reviewed and/or approved any information
- Access must be role-based, never name-based
- Access privileges assigned must be limited to those required to perform the authorized role
- There are ***multiple ways*** to comply; for example:
 - Biometric, e.g. fingerprint or retinal scan
 - Digital signatures
 - Scanning
 - Handwriting capture in software

Segregation of Duties:

- Users must have ***clearly defined and separate roles*** in their actions
- ***Review and approval*** should be done by someone ***independent*** of the user creating and/or modifying data
- The audit trail should identify the ***unique set of user credentials*** being used to take any action

Security:

- ***Restrict access*** to computer system and data via external software applications by encrypting data as it is transferred and/or using a firewall
- Maintain a ***cumulative record*** with the names of authorized personnel, their titles, and a description of their access privileges
- Never reuse a userID; when a user leaves the company, ***deactivate*** their account, ***never delete it***
- Prevent, detect and mitigate effects of ***viruses*** and other harmful software code (e.g., malware, ransomware)

21 CFR Part 11 Compliance (continued)

- **May apply** numerous levels of security to ensure authenticity of each user in the system
- **May require** users to establish a signature password on first log in
- **May require** use of an “approval” signature (same or different from login password) to sign off on controlled documents

_____ **require 2-factor
or multi-factor authentication**



Data Integrity Controls:

- Use prompts, flags, and other help ***features*** to encourage ***consistent*** use of ***terminology***
- Specify ***valid vs. invalid ranges*** and alert the user with a prompt for data out of range
- Require specific ***character types or numbers*** to assist users
- Force a valid entry in a field by making it a ***“required field”*** that cannot be bypassed
- Do not allow the system to automatically enter ***default data*** if a required field is bypassed

- Allow the system to populate a field with ***data duplicated*** from another field, but only after analyzing potential risk
- Design the system to attribute each record to an ***individual***
- Be able to reconstruct source documentation for ***FDA review***
- Be prepared to ***fully describe*** to FDA how data was obtained and managed over its life cycle
- ***Document*** what software and hardware are used
- A hybrid situation is when a company uses ***handwritten signatures*** to execute ***electronic records***, then ***scan*** the signed record into the system as a ***pdf; MUST VERIFY ALL***

Backup, Restore, Archival

- Use a ***full backup/recovery system*** to protect against data loss
- ***Test backup and restore*** functionality during validation
- Consider ***archival*** for data that does not need to remain online, but is still under retention
- Ensure that backup system maintains ***data integrity***
- Store backup records at a ***secure offsite*** facility
- Maintain backup and recovery ***logs***



Record Retention & File Format

- Treat an electronic record as a ***source document*** and retain according to the required ***retention period***
- Ensure copies preserve the content and meaning of the record, including all ***metadata***, or data that **puts it in context**
- Preserve copies in an appropriate ***format*** such as XML, PDF, or hardcopy
- The records must be available in ***“human readable” format*** for inspection

Change control:

- Maintain ***data integrity*** when making changes to the computer system, such as software upgrades, security and performance patches, equipment repairs, etc.
- Carefully ***evaluate*** effect of change before & after being made
- Determine the ***type and level of testing*** to perform, based on a risk assessment to ***evaluate the potential risk*** that may occur if the requirement is not met
- Consider ***regression testing*** to ensure other code not affected
- Use an ***IT Change Control SOP*** & document the revalidation

Training:

- Individuals who develop, maintain, and support the system in a validated state
- ***Users*** who will perform an ***authorized role*** using the system
- ***Quality*** should be trained to ***conduct mock audits***
- ***Document*** computer education, training, and experience
- Conduct training sessions as needed on a ***continuing basis*** for ***new personnel*** to learn the system functionality
- Provide training for ***everyone involved in validation***, including users, technical resources, and quality personnel

FDA Inspection and Audit:

- All records are subject to inspection in accordance with ***predicate rules***
- Provide an investigator with ***reasonable and useful access*** to records during an inspection
- Produce ***copies of records*** held in common portable formats when records are maintained in these formats
- Use established automated ***conversion or export methods*** to make copies in a more common format

- The copying process must produce copies that ***preserve the content and meaning*** of the record
- If you have the ability to ***search, sort, or trend*** part 11 records, copies given to the Agency should provide the ***same capability*** if it is reasonable and technically feasible
- Allow inspection, review, and copying of records in a ***human readable form*** at your site using your hardware and following your ***established procedures and techniques*** for accessing records

Standard Operating Procedures (SOPs):

- To provide the FDA with documented evidence that your system is Part 11-compliant, a set of ***system-specific*** standard operating procedures (SOPs) should be prepared in support of validation

Three Key SOPs:

- User Administration and Management
- System Administration and Configuration
- Document Control

User Administration and Management SOP:

- Create user ***accounts*** and user ***account types***
- Assign and approve user/workgroup ***security rights***
- Ensure the ***access privileges*** provided are ***limited*** to only those required to enable the user to perform their role
- ***Deactivate*** accounts
- Establish rules for ***password format*** and ***content***
- Establish rules for ***frequency*** of changing ***passwords***
- Define the procedure for ***electronic signature manifestation***

System Administration and Configuration SOP:

- System ***configuration*** settings and ***security*** administration
- ***Audit trail*** functionality
- ***Change control*** to design configuration of system
- Define ***ownership*** of system and system issues resolution

Document Control SOP:

- Include a ***usage*** statement
- Include ***revision*** numbering, approvals, document numbering
- Define controlled document ***distribution***
- Describe records ***retention*** and define a document ***lifecycle***

- *Who is authorized to **input and/or change** data?*
- *How can you tell who **entered** the data?*
- *How do you know **which data** was changed?*
- *When do you lock down data input as **final**?*
- ***Can you show me some data, the history of the data, and how the data life cycle is controlled?***
- *Is the system **validated** and are the **requirements met**?*
- *Can you show me the **results of the validation activities**?*
- *Are the **validation documents locked down**?*

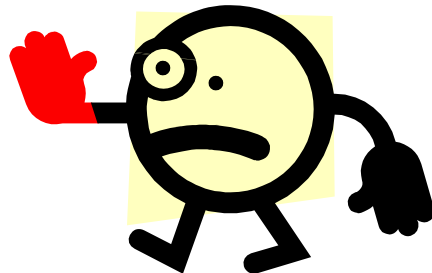
- ***Do the validation test results include:***
 - *Pre-defined acceptance criteria*
 - *Pass/fail*
 - *Signature*
 - *Date/time stamp*
 - *Deviation management*
 - *Objective evidence:*
 - *screen shots*
 - *audio-video recording*
 - *page printouts with a link to the source of the generated output?*

***“GxP” is defined as “Good-**variable-Practice**,” based on FDA
“Predicate Rules”***

- **GMP** = Good **Manufacturing** Practices
- **GLP** = Good **Laboratory** Practices
- **GCP** = Good **Clinical** Practices

The FDA operates on two key premises:

- If you didn't document it, you *didn't* do it
- If you could have committed fraud, you *did* commit *fraud*



- There is *no recourse*, since the following notion does not hold up when dealing with FDA

“You are innocent until proven guilty”

- **FDA can:**
 - issue *fin*es
 - **confiscate** materials and/or products, and
 - **shut down** some, or all, of your operations
- The classic example is **Schering-Plough's** Consent Decree issued in 1998:
 - cost **\$500MM** in fines
 - resulted in the **shut-down** of more than one manufacturing plant
 - required **10 years to recover** from the losses
 - They were **taken over** by Merck Sharpe & Dohme in 2010



An IT and/or automated system:

- ***“touches”*** an FDA-regulated product (pharmaceutical, biological, medical device, tobacco, etc.) during the process
- is used to collect, analyze, report, transmit or otherwise ***process FDA-regulated data***
- must be ***validated*** in accordance with Agency requirements for Computer System Validation (CSV)
- must be ***maintained in a validated state*** through the system’s life

Examples:

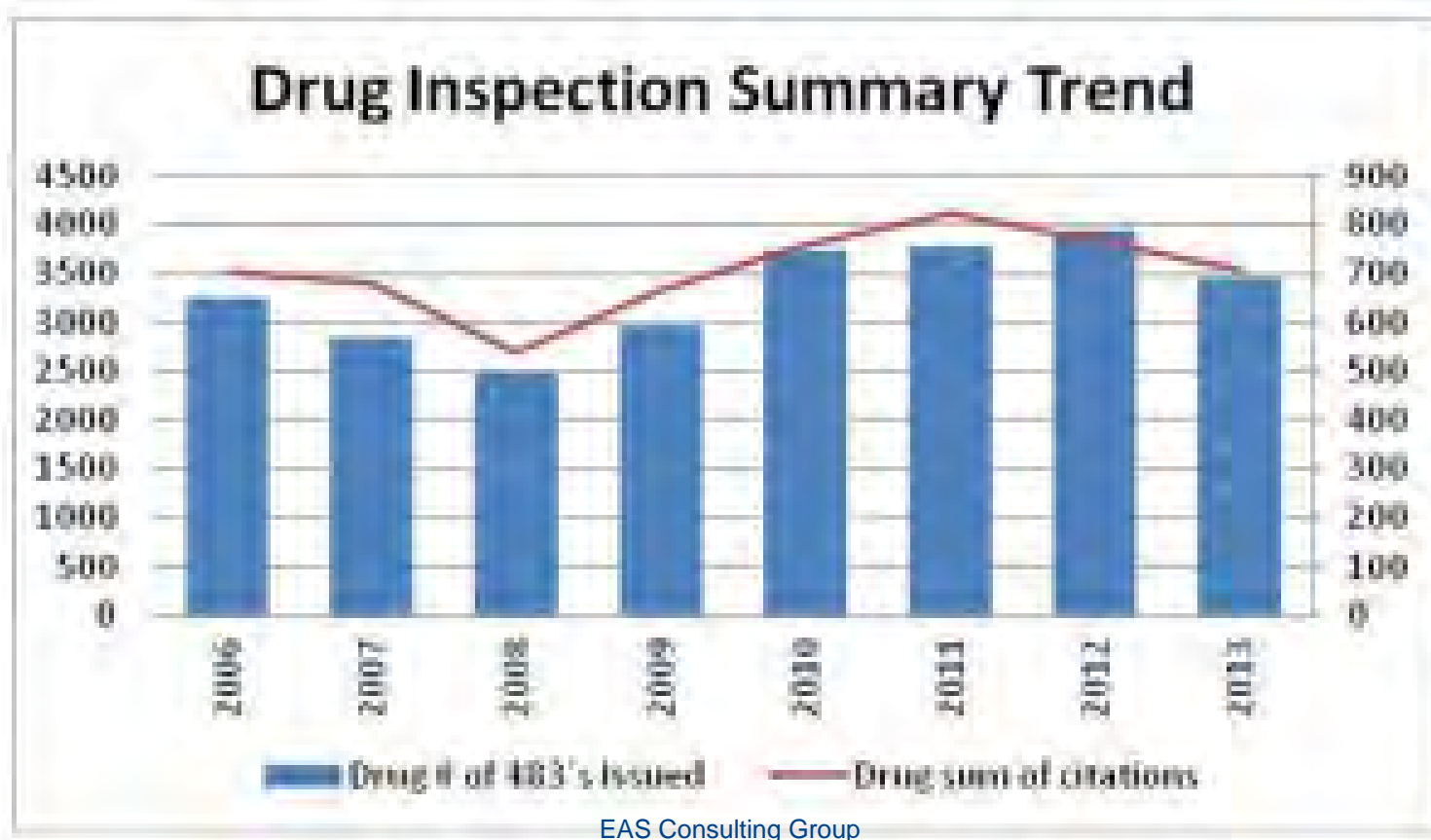
- Lab data acquisition systems (LAS)
- Lab information management system (LIMS)
- Clinical data management systems (CDMS)
- Room environmental monitoring systems
- Animal observation data recording/reporting systems
- Manufacturing automation systems
- Enterprise resource planning systems (ERP)
- ***Note interfaces and integration of systems***

Companies regulated by FDA have good reason for ***meeting compliance guidelines*** issued by the Agency:

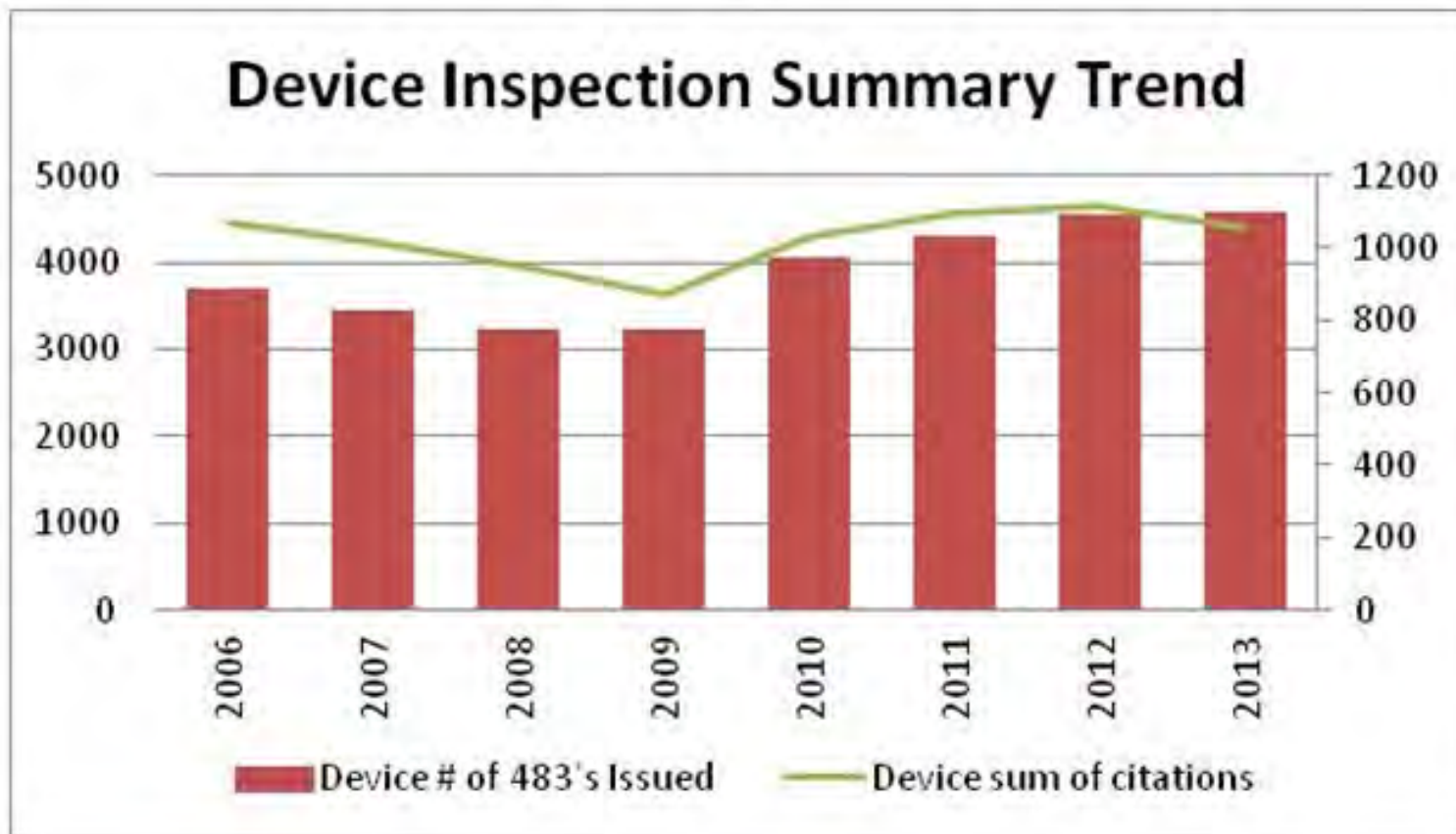
- Focus on ***data integrity, product quality and customer safety***
- Continued ***efficient business operations*** without unnecessary time and effort to respond to issues and concerns
- ***Good relations with FDA*** and any other regulatory agency
- Positive company ***image and reputation***



FDA Regulatory Oversight (continued)



FDA Regulatory Oversight (continued)



The FDA Guidance for Computer System Validation (CSV),
also known as the FDA ***“Blue Book,”*** was issued in 1983

CSV is:

- is the process of assuring that a system ***does what it purports to do***, and has been thoroughly tested and validated in order to prove this
- is based on the standard ***System Development Life Cycle*** (SDLC) methodology for computer systems

WHAT does FDA require? You must prove 4 things...

1. The system ***does what it purports to do*** and has been thoroughly ***tested*** to prove it
2. The system is ***suitable for its intended use*** and has been thoroughly ***tested*** to prove it
3. A ***risk-based approach*** is taken and documented
4. The system is ***maintained in a validated state*** through its entire life under formal ***change control***

Key Takeaway:

Companies must determine **HOW** to validate any GxP system

MYTHS Dispelled:

1. FDA tells you “WHAT” is required and **will never instruct** you as to “HOW” you should accomplish it
2. There is **NO** published, prescriptive, step-wise approach to validation that is endorsed or otherwise condoned by FDA
3. A company is **NOT** required to follow **any particular SDLC**, including “waterfall” to implement/ validate a GxP system
4. FDA does not require any company to follow **GAMP[®]5**, or **ANY** other published **principles** or industry best **practices**

More MYTHS Dispelled:

5. A lack of **FDA guidance** on any technology **does NOT** mean you **CANNOT** use it (e.g., cloud, SaaS, automated testing, AI, etc.)
6. The **requirements** for validating a system do **NOT** need to be completed/**approved before starting design/ development**
7. Many **design/configuration specifications** are vendor documents, and the **client may NOT** be able to view them
8. A vendor **CANNOT** claim a system is “**FDA-compliant,**” “**validated,**” or “**Part 11 compliant**”- client **MUST** do the work

More MYTHS Dispelled:

9. **GAMP®5 Category 3 software MUST BE validated**
10. **CSV does NOT mean you are following any particular methodology, such as waterfall**
11. **CSA does NOT mean you are following any particular methodology, such as agile**
12. **CSV and CSA ARE:**
 - Validation **methodology**-agnostic
 - System **platform**-agnostic
 - System **validation tool**-agnostic

More MYTHS Dispelled:

13. **Documentation prepared** by a **vendor** for a system **MAY** be **leveraged** when developing a validation plan (e.g., test scripts)
14. Documentation ***prepared by a vendor*** for a **CANNOT** be referenced as the sole source of confidence in the system, without doing validation independently; don't point at the vendor
15. You **CANNOT** feign ignorance and point to an internal IT organization, contractor, or vendor as being the responsible party for validation; the **SYSTEM OWNER** is responsible for this
16. FDA will ask the system owner to defend their case of an adequately validated system

Who should care?

- Resources involved in computer system validation need to be concerned and trained to perform their role:
 - *Develop/Configure and Test*
 - *Maintain the System (IT and Business)*
 - *Users (Functional Experts)*
 - *Quality Auditors (Oversight)*

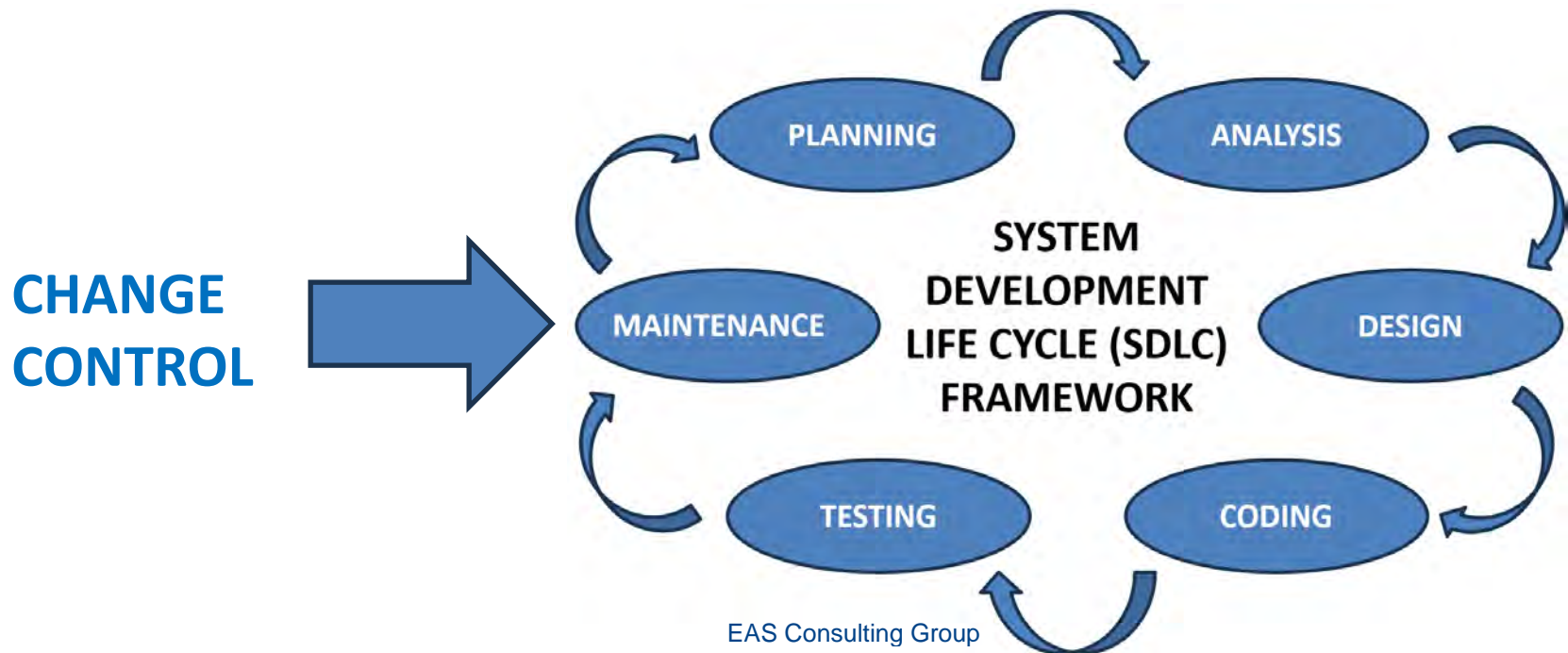


SDLC:

- Supports FDA requirements for GxP system validation
- Is integral to the CSV methodology or any methodology applied during development, testing, and validation
- Is the framework used for selecting, implementing, maintaining and retiring a system (“cradle to grave”)
- Includes a series of life cycle “**phases**”

IT CHANGE CONTROL SOP:

- Formally request change
- Include impact on validated state of the system
- Recommend appropriate testing (change, regression)



Any change to the functionality must be captured through a standard, documented change control process, which must include:

- A ***record of the change*** to the code or configuration
- The ***name*** of the person who implemented the change
- The ***date*** and ***time*** the change is moved to production
- ***Thorough testing*** of the changed functionality and related documentation

Validation Planning

Once a system is selected, a ***strategic approach*** should be developed for validation

- Is there an overall ***company approach***?
- ***What rationale*** will be used to demonstrate the system is fully tested and validated to meet FDA compliance?
- ***What SDLC phases and steps are required*** for this system, and how specifically will they be determined and rationalized?
- Who will be involved in the ***validation process***?
- What approach will be taken for ***testing***?
- How will the ***documentation and approvals*** be completed?

Validation Planning (continued)

- Will there be a ***business process re-engineering*** component to the effort?
- Will the system be integrated with a ***legacy system*** that is/is not validated?
- How will ***organizational change management*** be handled?
- How will ***policies and procedures*** be evaluated, updated, remediated and/or created?
- How will ***training*** be incorporated into the project?
- How will the system be transitioned into ***production?***
- How will the system be maintained in a ***validated state?***

The SDLC Methodology includes Key Elements:

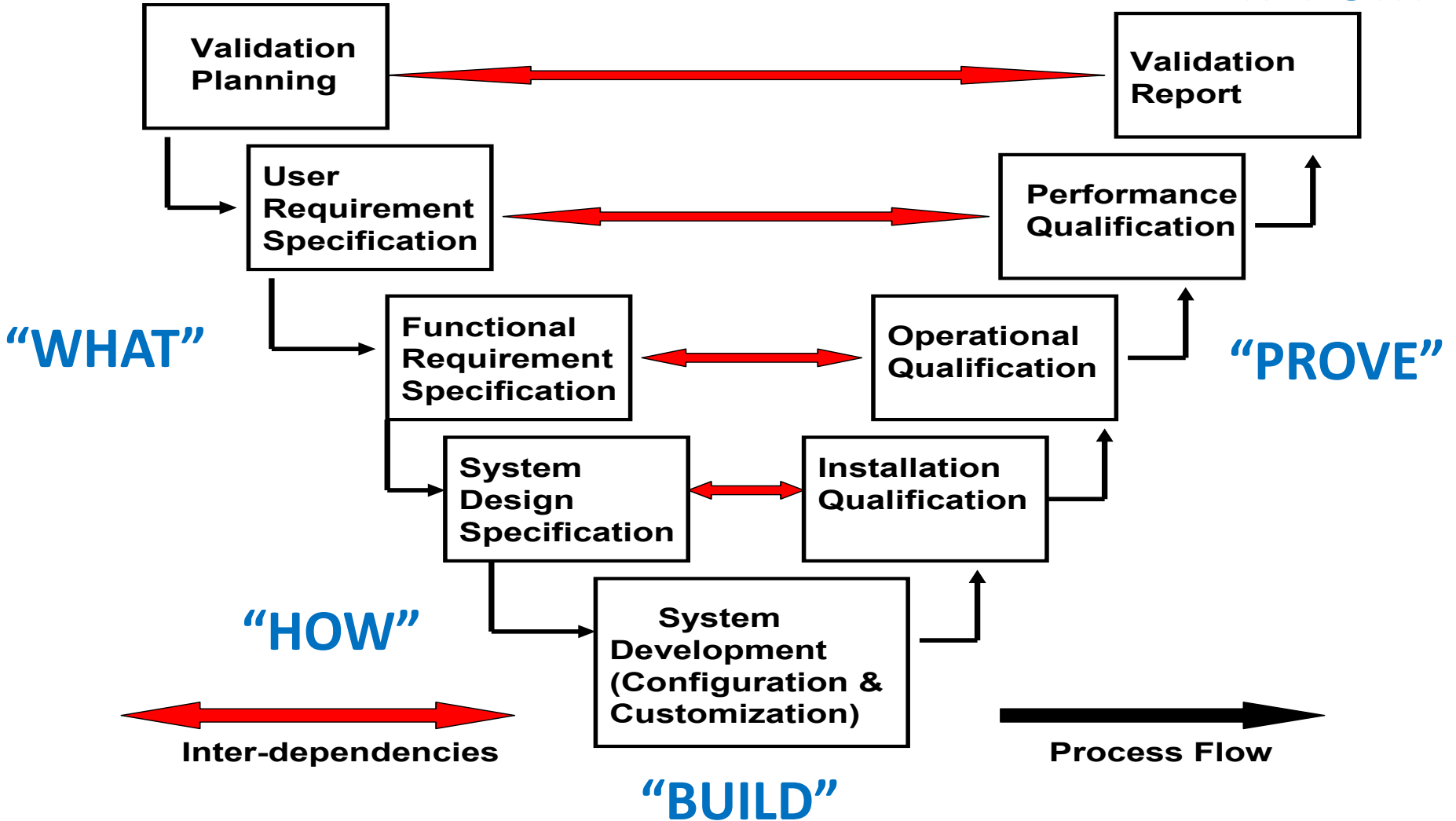
- Validation Planning
 - User Requirements Specification (URS)
 - Functional Requirements Specification (FRS)
 - System Design Specification (SDS) and/or Configuration Management Specification (CMS)
 - Implementation (Custom Development, Configuration, Out-of-the-Box Solution)
- “WHAT”
- “HOW”
- “GAMP®5 Category”

- Installation Qualification (IQ) } **“Verifies Design”**
 - Operational Qualification (OQ) } **“Verifies Requirements”**
 - Performance Qualification (PQ)* } **“Verifies Suitability”**
 - Test Summary Report(s)
 - Validation Summary Report
 - System Acceptance Report (System “Owner”)
 - System Release Notification (System “Steward”)
- *User Acceptance Testing (UAT) Testing

Validation Planning (continued)

“PLAN”


“REPORT”



- Develop a ***validation approach/rationale*** to address the ***type and level of testing*** that will be required

- **Five (5) Key Factors to Consider in the Validation Plan:**

1. System ***Size***
2. System ***Complexity***
3. System ***Business Criticality***
4. GAMP[®]5 System ***Category***
5. System ***Risk Assessment***



The first 3 are subjective & needed to gauge resources & time for robustness of testing based on risk

Document in the Computer System Validation (CSV) Plan

4. *GAMP[®]5 System Category*

We can implement and manage an automated system using the ***Good Automated Manufacturing Practice[®] (GAMP[®]5, Second Edition)*** guidelines published by the International Society for Pharmaceutical Engineering (**ISPE**)

- ***Focus*** on patient safety, product quality & data integrity
- ***Effective governance*** to achieve and maintain GxP compliance
- ***Scalable*** approach to GxP compliance based on risk and complexity
- ***Improving*** GxP compliance ***efficiency*** and ***effectiveness***
- ***Enabling*** continuous improvement

Source: <https://ispe.org/>

- GAMP®5 concepts can **improve** your existing **methodology**
- GAMP®5 guidance aims to achieve computer systems that are **fit for intended use** and meet regulatory requirements by building on **industry best practices** in an efficient and effective manner
- The GAMP®5 guidance is **not a prescriptive** method or standard, but...
 - » Pragmatic guidance
 - » Approaches
 - » Tools for the practitioner
- Applied with **expertise** and good **judgment**

Validation Planning (continued)

GAMP®5 CATEGORY	DESCRIPTION	REQUIREMENTS
1	Infrastructure Software (Operating System, Database Software, Tools, Utilities)	Vendor Audit, IQ
2	Firmware	N/A* Moved to Category 1 or 3
3	Non-configured (functionally) Software (COTS packages)	Vendor Audit, IQ, OQ
4	Configured (functionally) Software	Vendor Audit, IQ, OQ, PQ
5	Custom Applications (New Code)	Vendor Audit, IQ, OQ, PQ

Source: [GAMP®5 Guide: Compliant GxP Computerized Systems](#) International Society for Professional Engineering (ISPE)

5. A Risk-Based Approach to Validation:

- FDA ***does not have adequate staffing*** to inspect every system in every company visited
- FDA expects companies to ***prioritize*** their regulated systems based on risk
- ***A standard risk approach is an industry best practice*** that should be developed for the company and used consistently

Risk Assessment:

- The ***risk assessment*** is performed in accordance with a written procedure that includes forms and checklists to support documentation of the results
- Results are typically ***documented*** in a ***matrix format***, much like a failure modes and effects analysis
- Using the likelihood and consequences of failure, a ***level of risk is assigned***
- The ***validation plan*** uses the system (high-level) risk assessment results to drive the scope and extent or rigor of validation activities

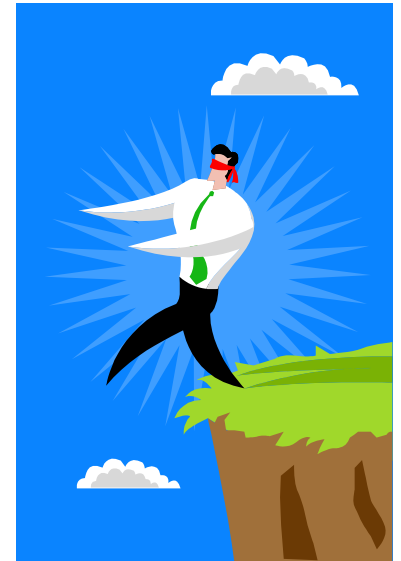
All risks should be evaluated collectively to create a *risk profile* for the system

- ***You need to ask the question:***

If the system were to fail, what

impact would that have on the

process, product or patient/consumer?



A system may fail in many different and unrelated ways





Ask the following questions:

1. What are the ***functions*** performed or data used?
2. What is ***affected*** by the function?
3. How can it ***fail?***
4. What is ***probability*** of failure, given vendor's development process, experience and system complexity?
5. What is the ***severity of consequences*** of failure; focus on risk to consumer?
6. How likely will failure be ***detected*** by system design or controls?

- Identify ***risk scenarios*** based on typical system processes and operations
- ***For each risk scenario:***
 - Assess ***probability*** each risk scenario will occur
 - Assess ***severity*** of impact to system
 - Assess how ***detectable*** it would be, if it occurred
 - Identify ways to ***mitigate*** using ***technical and/or procedural controls***
- Determine the ***priority*** of addressing each risk, then assign an overall risk rating to the system

Using failure probability & consequences, assign risk rating:

PROBABILITY 

CONSEQUENCES 

RISK RATING	LOW (Highly Improbable)	MEDIUM (Credible/ Not Very Probable)	HIGH (Credible/ Probable)
HIGH (Serious Injury or Death)	MEDIUM	HIGH	HIGH
MEDIUM (Non-serious Injury)	LOW	MEDIUM	HIGH
LOW (No Injury)	LOW	LOW	MEDIUM

Validation Plan uses risk assessment results to drive scope, extent, & rigor of activities

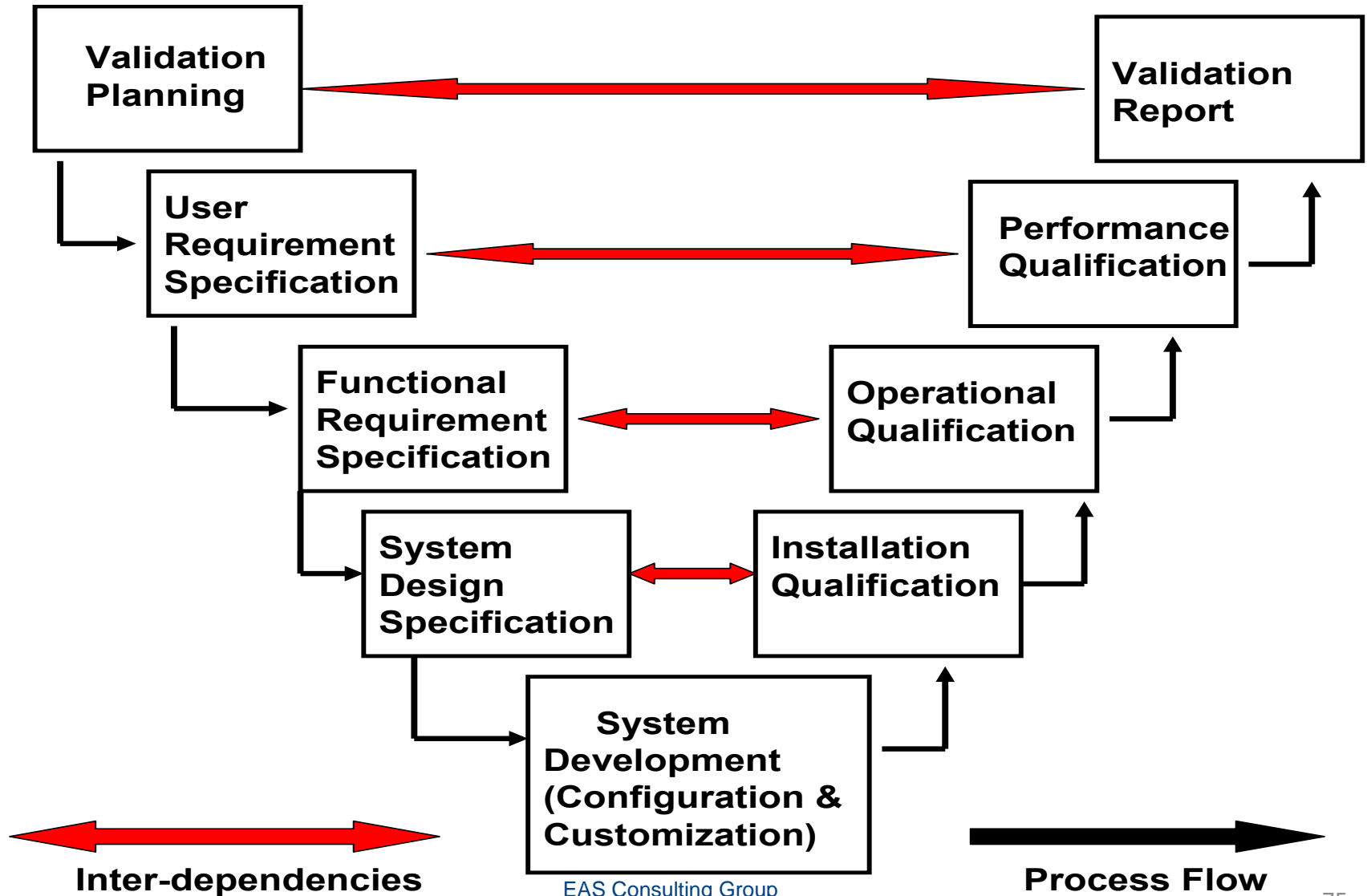
- ***Perform a Risk Assessment for each Requirement***
 - For each defined requirement determine the following:
 - ***Probability*** it will not be met
 - ***Severity*** of impact if it is not met
 - ***Detectability*** if it is not met
 - ***Technical*** and/or ***procedural controls*** that may mitigate the risk
 - For each requirement the ***risk rating*** should be assigned based on a ***standard risk assessment procedure*** used for all GxP systems

Validation Planning (continued)

- **Create a System Inventory for Inspection:**
 - *a **prioritized list** of the company's GxP-regulated system inventory*
 - *the **level of risk** assigned to each **system***
 - *the **approach to validation** that will be done to assure risk is **minimized***

System Name	Risk Rating (H/M/L)	Description	Business Criticality
System A	M		
System B	L		
System C	H		

Validation Execution



User Requirements Specification (URS):

- Needed system functionality, defined by SME at a ***high level and in business terminology***
- ***URS*** should be the ***basis*** for developing a detailed ***Functional Requirements Specification (FRS)***
- Requirements should be ***maintained as current***

Detailed Functional Requirements Specification (FRS):

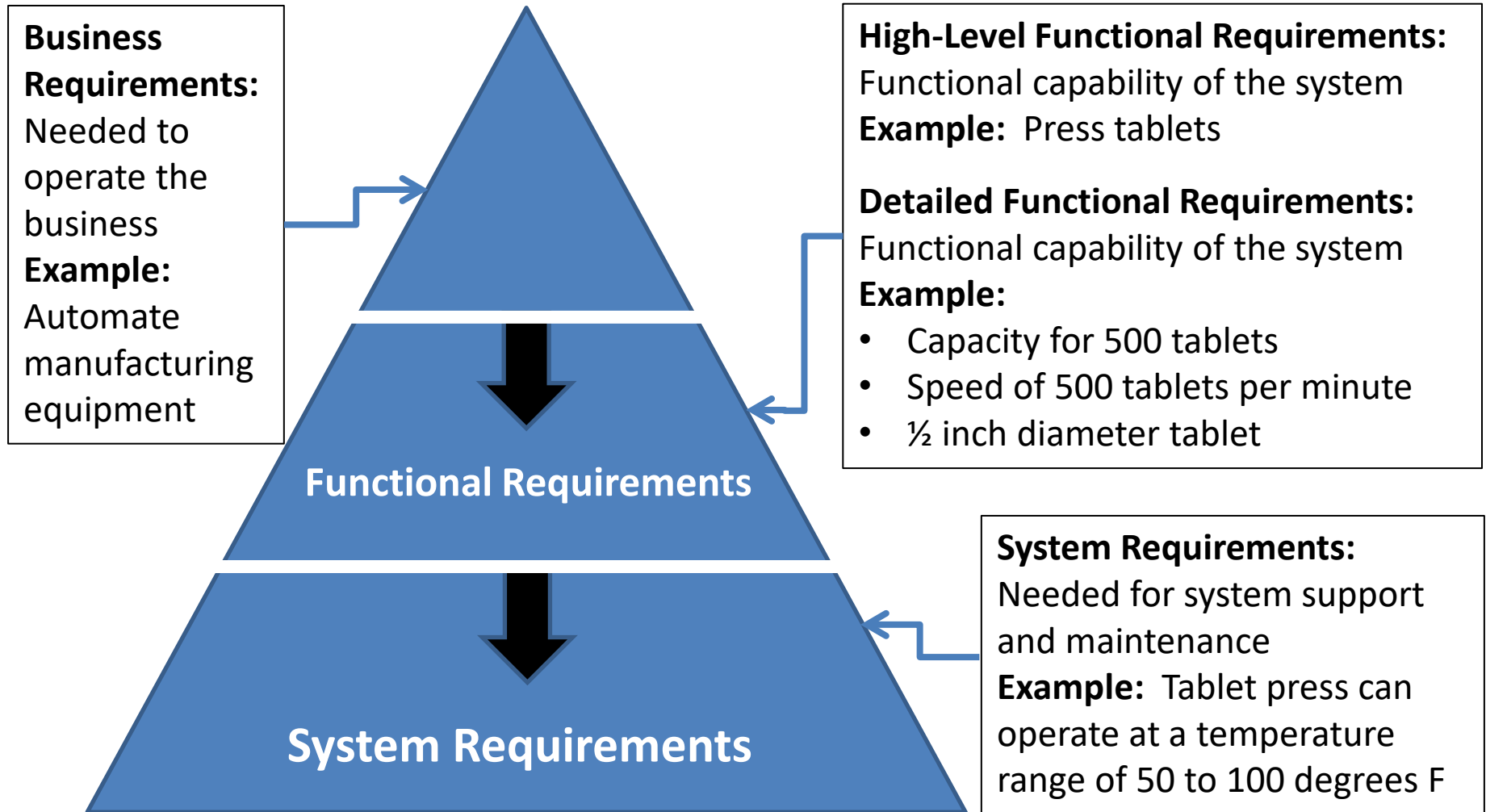
- Must address all system functionality in ***detail***
- Users ***must*** define & approve functional requirements

Requirements:

- ***What*** the software does is directly perceived by its users, either human users or other software systems that are ***integrated***
- When a user ***performs some action***, the software responds in a particular way; when an external system submits a request of a certain form, it ***gets a particular response***
- Therefore the ***users must agree*** on actions they can perform and the response they should expect

- **Requirements must be:**
 - Unique, and have a unique identifier
 - Able to be tested
 - Technically feasible
 - Able to support a business process
 - Clearly understood
 - The basis of a user commitment
- Include ***only requirements that represent functionality that will be used***, as each will require specific testing, which can become time-consuming

Validation Execution (continued)



Functional Requirements specify what the system should do

High-level Example: Allow entry of product information

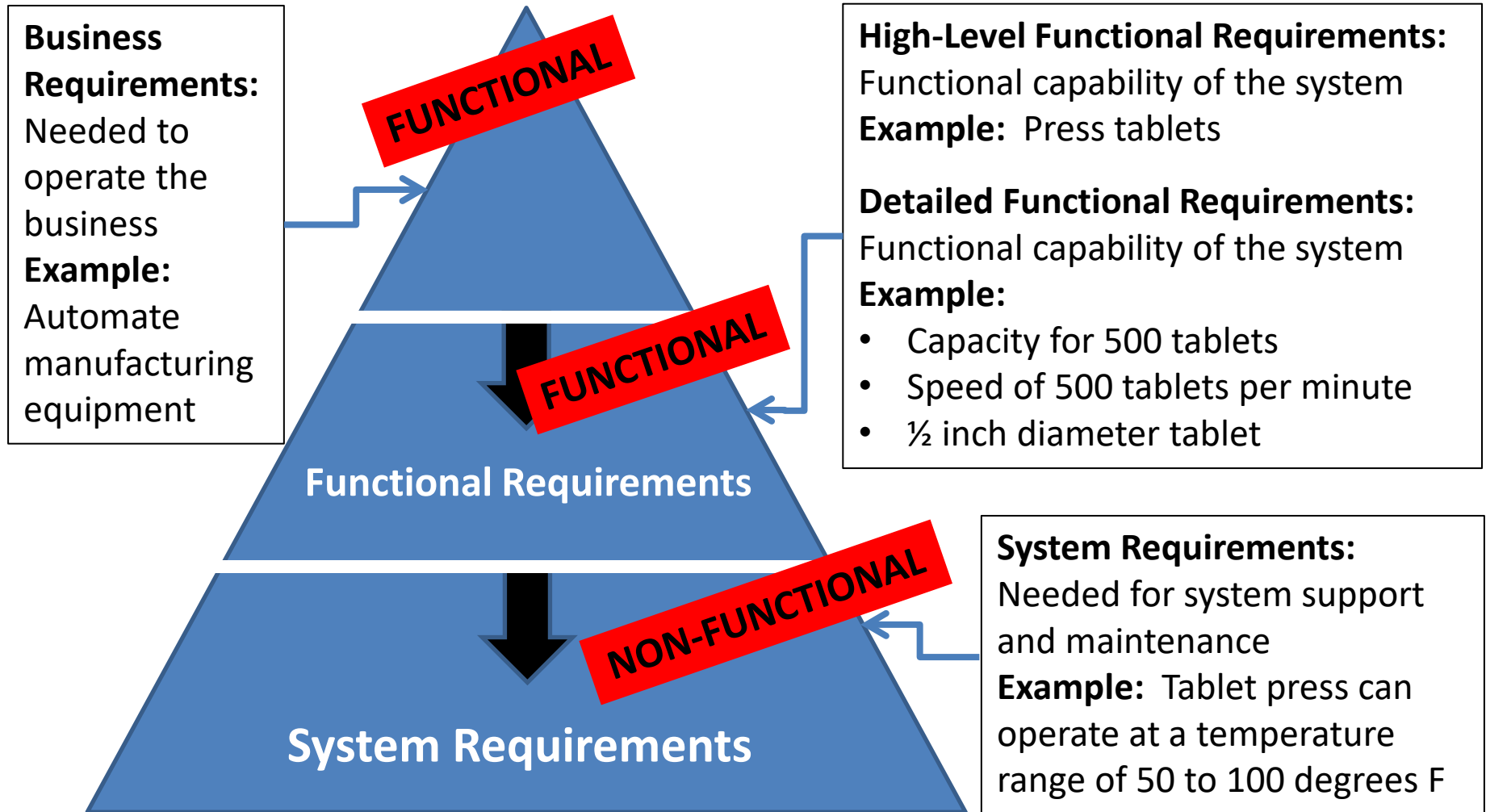
Detailed Example: Allow entry of a product number as an 8-character numeric (plus many more)

- ***Types of requirements include:***

- Business rules
- Transactions
- Authorization levels
- Data entry functions
- Administrative functions
- Reporting functions
- Archival of historical data
- Regulatory rules
- Certification functions

- **Non-Functional Requirements:**
 - How the system should *behave; enables* functionality
 - *Criteria* that judge the operation of the system
 - **Example:** Allow authorized users to access an application
 - *These include:*
 - Performance
 - Scalability
 - Capacity
 - Availability
 - Reliability
 - Recoverability
 - Maintainability
 - Security
 - Data Integrity
 - Environmental
 - Interoperability
 - Quality

Validation Execution (continued)



- Know ***who*** asked for the requirement and track their name along with it
- There are ***key requirements*** that should never be missed:
 - Security permissions
 - Error messaging
 - Error logging
 - System shutdown
 - System overload handling

Design Specification:

- **How** software responds to agreed upon request is in the design specification (screen layouts, database schemas, descriptions of communication layers, etc.)

Example:

- A **requirement** for a lab application is to allow the user to open a data file for which they have access
- A **design** issue is whether to build a customized or use a platform standard file selection tool

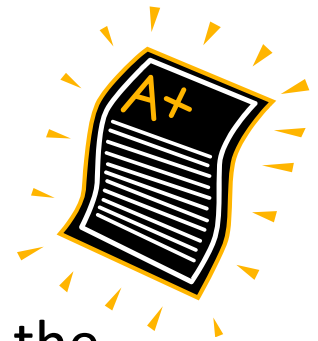
Detailed *System Design Specifications (SDS)*:

- Must address all defined functional requirements
- Users *must* sign off on them
- Design specifications should be *maintained as current* (“living” document)
- In the case of a COTS (computer off-the-shelf software), the design will be replaced with a *configuration specification*

Testing is one of the most critical steps required before placing a system in production:

- ***Installation Qualification (IQ)*** - for hardware, operating system, database, tools, utilities, etc.
- ***Operational Qualification (OQ)*** - for any code (unit & integration testing)
- ***Performance Qualification (PQ)*** - to confirm the intended use; must be executed by users

- Develop a ***detailed test plan***, including test scenarios and scripts
- Include ***positive and negative scenarios***, and ***boundary and stress testing***
- Follow up on all ***defects*** and resolve these
- ***Segregation of duties*** should be followed
- Prepare a written ***Test Summary Report*** for each of the phases of testing



- ***IQ and OQ testing packages*** can be purchased from and executed by a vendor or contractor
 - ***Shortens*** time to prepare testing documentation
 - ***Alleviates*** need for internal resources to plan/execute tests
 - ***Cost*** needs to be included in the budget
- ***PQ*** must be executed by users; if external resources prepare test scenarios and scripts, ***user input*** is required
- A software package provided by a ***mature vendor*** will likely have fewer faults than one from a new vendor due to a more robust and mature Quality Management System

Test Results Matrix Example

Step No.	Description	Expected Results	Actual Results	Result (P/F)*	Discrepancy No.	Signature	Date
3.1.2	Enter the sample number by clicking on the "Enter Sample No." field	The sample no. appears in the field and matches the vial					
3.1.3	Enter the number of vials by clicking on the "Enter No. Vials" field	The number of vials appears in the field correctly					

***P = Pass, F = Fail**

Test Results Matrix Example

Step No.	Description	Expected Results	Actual Results	Result (P/F)	Discrepancy No.	Signature	Date
3.1.2	Enter the sample number by clicking on the “Enter Sample No.” field	The sample no. appears in the field and matches the vial	The sample no. is “truncated” and only 7 of 9 characters appear in the field	F	5	<i>John Doe</i>	5/14/2023
3.1.3	Enter the number of vials by clicking on the “Enter No. Vials” field	The number of vials appears in the field correctly	The number of vials appears in the field correctly	P	N/A**	<i>John Doe</i>	5/14/2023

***P = Pass, F = Fail**

**** N/A = Not Applicable**

Test Results Matrix Example

Step No.	Description	Expected Results	Actual Results	Result (P/F)	Discrepancy No.	Signature	Date
3.1.2	Enter the sample number by clicking on the "Enter Sample No." field	The sample no. appears in the field and matches the vial	The sample no. is "truncated" and only 7 of 9 characters appear in the field	F	5-6 <i>JD</i> 5/14/2023 Incorrect number entered	<i>John Doe</i>	5/14/2023
3.1.3	Enter the number of vials by clicking on the "Enter No. Vials" field	The number of vials appears in the field correctly	The number of vials appears in the field correctly	P	N/A**	<i>John Doe</i>	5/14/2023

*P = Pass, F = Fail

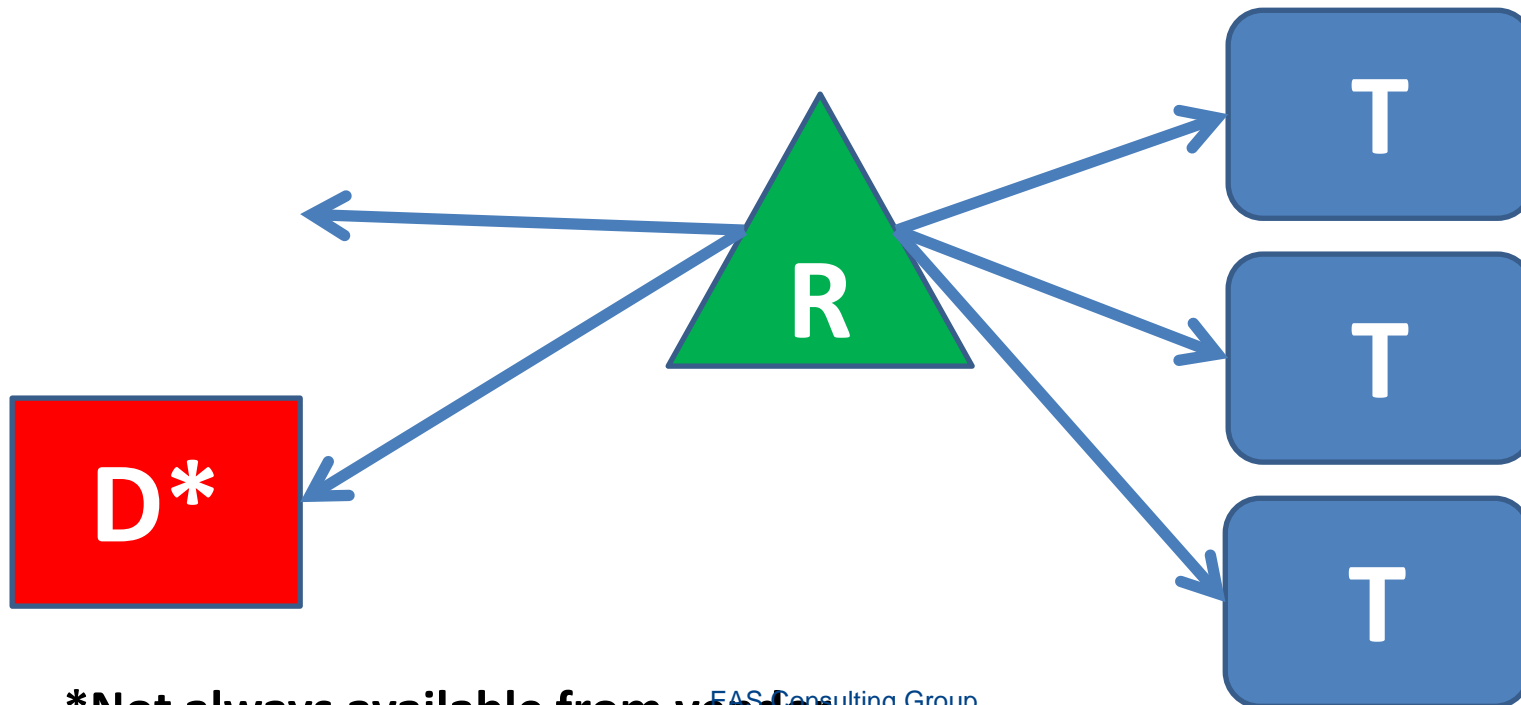
** N/A = Not Applicable

Every deviation from an expected result:

- Assign a ***consecutive number***
- ***Investigate*** the ***root cause***
- Note as a ***system error***
- Correct a ***tester or script error immediately***, with the reason for the change, initials, and date
- If a ***tester*** or ***script*** error, requires a ***re-test*** to ensure
- If a system error or defect, ***stop testing*** until resolved; may contact vendor to ***remediate***, then ***retest***
- ***Record the resolution*** on the test ***Deviation Log***
- All defects must be ***resolved*** prior to final review

Validation Execution (continued)

The requirements, design specifications and test scripts that are linked together should be documented in the ***Requirements Traceability Matrix (RTM)***



***Not always available from vendor**

Once the **test results** and **RTM** are **approved**, a **Test Summary Report** is prepared for **each phase**, or one for **all phases**

- All test scripts **executed accurately** & all defects identified, remediated, & retested; all **documentation** meets GDPs
- It should be clear when **testing was stopped**, what issues were analyzed/ resolved, and when testing was re-executed
- It should **detail the chronological path** followed for all testing
- The Test Summary Report should lead one to conclude the system is **fit for production**



- ***Operational and support manuals, scripts, & other documents*** should be ready before moving to production
- Details including ***log books & electronic files*** for recording
 - *System Configuration*
 - *Backup, Restore, & Archival*
 - *Environmental Requirements*
 - *Security & Controls*
 - *User Guides*
 - *Incident Reporting System*
 - *Policies & Procedures*
 - *Change Control*
 - *System Maintenance*
 - *Disaster Recovery Plan*
 - *Business Continuity Plan*
 - *Data Governance*
 - *Training*
 - *Retirement Plan*

- ***Disaster Recovery*** is the process of bringing back vital technology, infrastructure and systems after a disaster
- DR focuses on the IT components that support ***critical business functions***
- The objective in executing the disaster recovery plan is to quickly and effectively ***resume operations*** in the event of an unanticipated emergency or disaster that disrupts information systems and business operations
- ***Cloud service & SaaS vendors*** have this responsibility; refer to ***contract*** and/or ***vendor website***

Business Continuity:

- is the process of planning, preparing and conducting activities to ensure an organization's ***critical business functions*** continue with minimal or no interruption, despite the occurrence of a serious incident or event causing operations to be hindered
- enables organizations to ***recover operations*** needed to maintain regulatory compliance; for example, systems monitoring animal rooms during toxicology testing to support an NDA

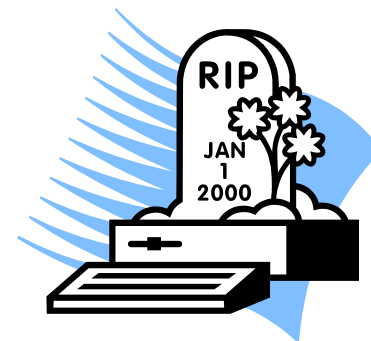
Once in production, a Governance Board should oversee the validated system:

- It should be organized ***prior*** to going live with a computer system regulated by FDA
- ***Roles and responsibilities*** should be defined clearly
- The board must ***control all changes*** to the system that might have an impact on its validated state



Every system regulated by FDA must be managed from “cradle to grave”:

- At the end of system’s useful life, an approach must be taken to archive data and ***retire the system***
- All ***system & validation documentation*** should be retired & retained through retention period
- ***Expired*** data and system documentation should be disposed of securely to avoid liability



To ensure users are ready to ***fully embrace*** and use it:

- A detailed ***Training Plan*** should be completed
- Training should be carefully ***timed*** to keep material fresh
- Training should be ***documented & available online*** for refresher and new employee training
- Training should be ***mandatory & enforced*** to ensure success

An ***Organizational Change Management Plan*** should be developed to detail how progress will be communicated

- Identify “***quick adopters***”
- Identify “***laggards***”
- Identify “***resisters***”
- Disarm those who “***obstruct***”
- Communicate ***profusely*** and keep everyone in the loop as to how the project is progressing
- ***Listen*** to your customers



- Any effort to add ER/ES capability to systems should include an ***organizational change management*** component designed to:
 - Ensure the changes are clearly ***understood***
 - ***Engage*** stakeholders to be part of the process
 - Ensure that system functionality will be ***used correctly***
 - Allow for ***feedback*** from stakeholders to ensure the process is optimized

What are “GxP” Documents:

- Written records of **GxP** processes and procedures
- **Legal documents** that can be requested or subpoenaed by a court of law to prove GxP Compliance
- Provide a **full data trail** of process events
- **Demonstrate** work was conducted in compliance
- Critical documentation for the **planning & execution of** GxP system **validation**
- **Training** and skill **qualification** documentation

- Critical documentation included in the ***maintenance of a “GxP” system in a validated state***
- ***Policies and procedures*** that support CSV activities
- All recording of ***original “GxP” documentation*** must be ***reviewed*** by a second person and ***approved*** by a third person, per the requirement for ***segregation of duties***
- Any ***deviation*** from a ***documented CSV plan or protocol*** is a deviation even if ***fully justified***
- ***Deviating*** from an approved ***procedure*** because it is not updated is a ***violation of GxPs***

GDP (continued)

- Existing policies and procedures must be ***updated*** to account for all ramifications of the use of electronic records and signatures in an FDA-regulated system environment
 - ***Identify*** policies and procedures
 - Perform ***gap analysis***
 - ***Update and/or create*** applicable policies and procedures



Policy **Topic** Checklist for GxP Compliance:

- Computer Validation
- IT Change Control
- IT Asset Management
- Physical/Logical Security
- GDPs & Data Privacy
- Electronic Records/Signatures (ER/ES)
- Risk Management
- Data Governance
- Disaster Recovery
- Business Continuity
- Vendor Management

Procedure **Topic** Checklist for GxP Compliance:

- Functional Requirements Specification (FRS)
- System Design Specification (SDS)
- Installation Qualification (IQ) Testing
- Operational Qualification (OQ) Testing
- Performance Qualification (PQ) Testing
- Operational Maintenance
- Data Backup, Recovery and Archival
- System Release

- System Configuration Management
- System Retirement
- Disaster Recovery
- Business Continuity Planning
- System Change Control
- Electronic Records & Signatures (ER/ES)
- Data Integrity
- IT Asset Tracking
- Good Documentation Practice (GDP)
- Training Tracking and Management

Agile Model:

- An agile project is broken into “***sprints***” to deliver a ***working product*** (Minimum Viable Product (MVP) after each sprint
- Produces ***ongoing releases*** with small, ***incremental changes*** from a prior release
- Each iteration is ***tested***
- Emphasizes ***interaction of customers, developers & testers***
- ***Depends*** on ***customer interaction*** to provide clear direction
- It may be ***difficult*** to ***identify*** the ***final cost***
- ***New requirements*** may ***conflict*** with existing ***architecture***

Waterfall and Agile Methodologies (continued)

- The **GAMP[®]5 “V” Model** can be ***mapped effectively*** for use with an ***agile***, or **any approach**
 - The ***same documentation*** used in waterfall can be ***adapted*** for use through agile ***“sprints”***
 - The ***timing*** for ***completion & review/approval*** cycles for documents ***will vary***

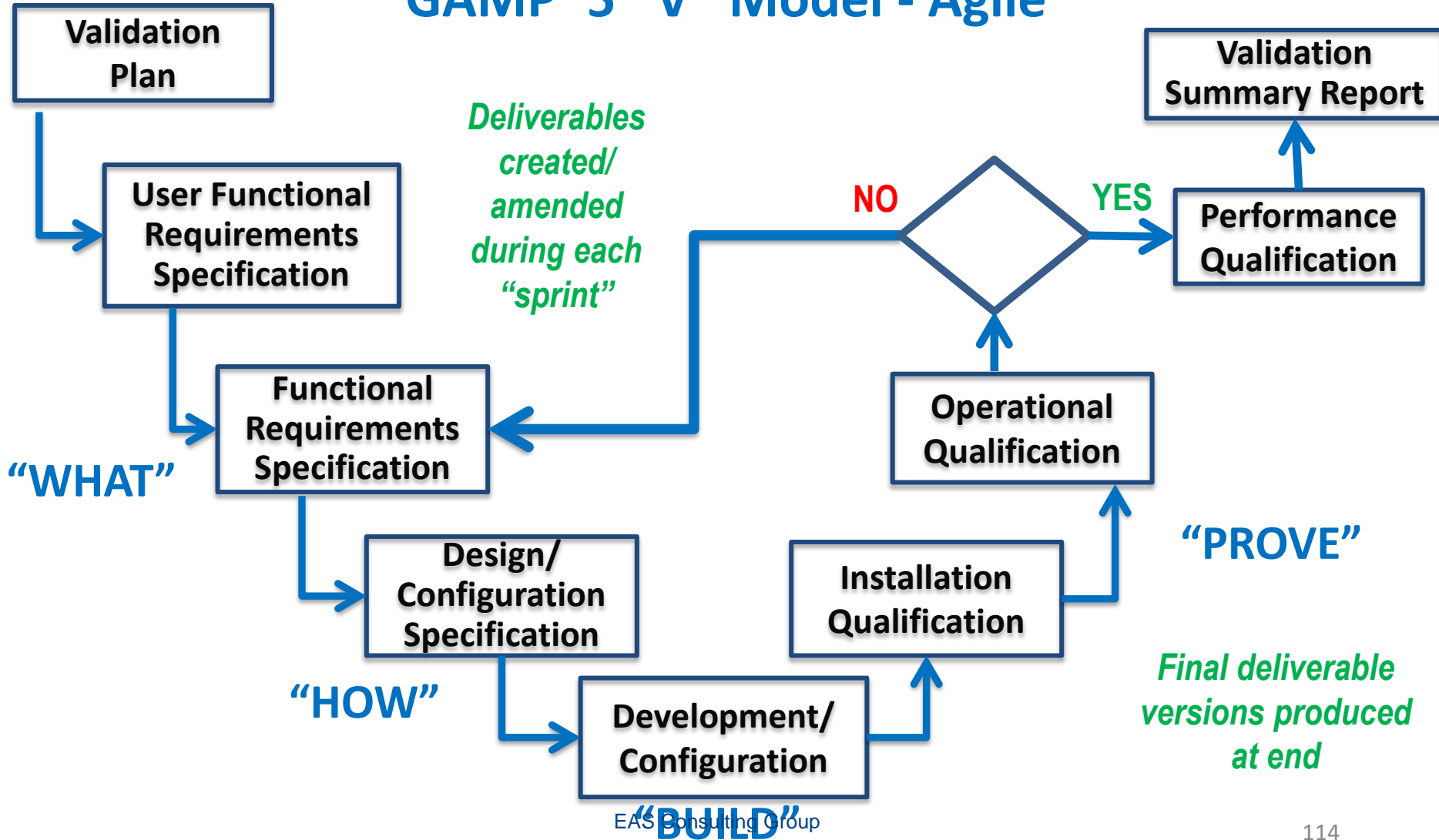
Key Takeaway: If a validation approach ***other than waterfall*** is used, this is **NO EXCUSE** for ***not doing a thorough job***

Waterfall and Agile Methodologies (continued)

- As **GAMP[®]5, Second Edition** guidance was issued in July 2022
- As **GAMP[®]5** includes the “**V**” model, or **waterfall approach**, many **believe** this is a **requirement**
- GAMP[®]5, however, **promotes a risk-based approach** and **does not require** any particular development methodology
- A **Special Interest Group (SIG)** was established to provide **guidance** on understanding how to **apply agile** development to **GxP system software**
- The SIG is focused on a **risk and critical thinking based** approach in an effort to **remove aspects that do not add value**

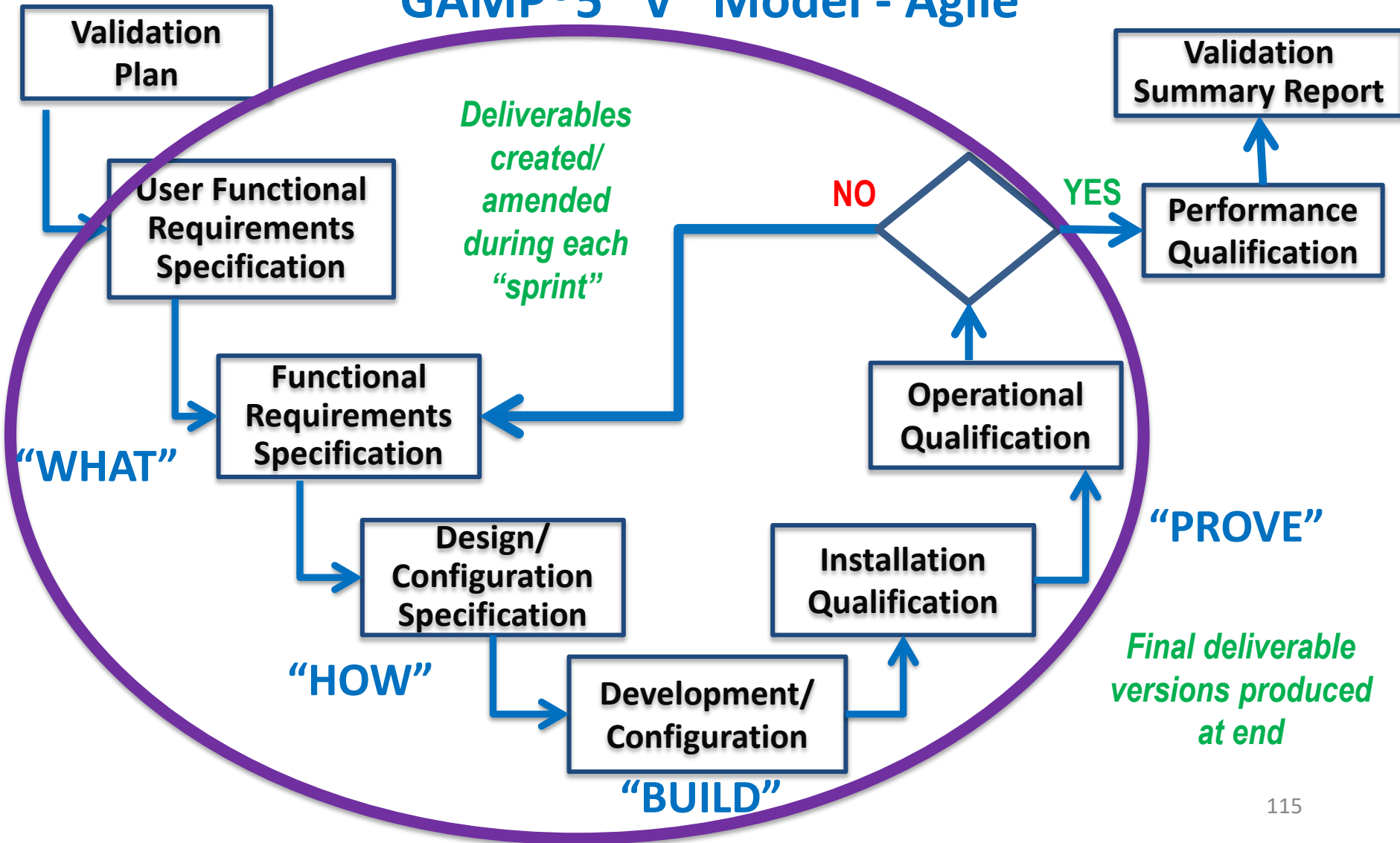
Waterfall and Agile Methodologies (continued)

GAMP®5 “V” Model - Agile



Waterfall and Agile Methodologies (continued)

GAMP[®]5 “V” Model - Agile



- Do what *makes sense*
- Use a *risk-based approach* & test each requirement accordingly
- If it *doesn't* seem to add value, *question* doing it
- Use *critical thinking* & ask “why” you are doing validation
- Documentation should be the final “*proof*” rather than the “*driver*” of validation

- CSA will require an effort to ***ask “why” software is being developed*** rather than focusing on the mechanics of code development
- A ***risk-based approach*** will be required to minimize risks in code application
- The focus will be on ***appropriate testing*** and then ***documentation***, still required, but the ***purpose*** becomes to ***prove all activities have been done effectively*** rather than driving the software development processes
- ***Critical thinking***, instead, becomes the ***main focus***

- How the CSA approach ***addresses critical thinking***, and ***how requirements are classified by risk and tested*** will be different
- The use of ***cloud services*** will require a ***different approach for IQ*** during CSA, with documentation from the ***vendor's website*** comprising a good portion of the Test Protocol; IQ testing will be more of an ***"IQ reporting"*** type of exercise
- ***Automated testing*** will likely be a considerable part of the CSA approach, and the ***documentation for that will differ*** from test documentation created using CSV (heavily manual) and will ***depend on the tools used***
- Moving from CSV to CSA ***requires a shift*** from documentation to critical thinking

- In some cases with ***low risk***, a ***simple test*** can be appropriate, while in others with ***high-risk/high-impact***, you might consider ***negative testing*** to be sure certain processes can account for different potential risk of failure
- By ***testing a higher-level process***, can ***automatically qualify*** the ***underlying systems*** and ***save*** a tremendous amount of ***time and effort***
- For example, is it necessary to spend time ***qualifying*** installation of ***servers, operating systems, and database setup*** ***when these are heavily used throughout industry?***

How to Think Critically:

- 1. *Ask*** Basic Questions
- 2. *Question*** Basic Assumptions
- 3. *Be Aware*** of Your Mental Processes
- 4. *Try*** Reversing Things
- 5. *Evaluate*** the Existing Evidence
- 6. *Remember*** to Think for Yourself
- 7. *Understand*** No One Thinks Critically 100% of the Time

- Software used in conjunction with a **medical device** to control or monitor activity must be thoroughly validated
- The **extent of validation evidence** needed for software used with a medical device depends on the device manufacturer's documented **intended use** of that software
- **For example:**
 - a device manufacturer who chooses not to use all the vendor-supplied capabilities of the software **only needs to validate those functions that will be used**
 - The **potential risk** of device failure must be considered when determining the type and level of testing to conduct

- When software is ***upgraded*** or any ***changes*** are made, the device manufacturer should consider how those changes may ***impact the "used portions"*** of the software and must ***reconfirm the validation*** of those portions of the software that are used
- However, ***high risk applications*** should not be running in the same operating environment with non-validated software functions, even if those software functions are not used
- ***Risk mitigation techniques*** such as memory partitioning or other approaches to resource protection may need to be considered

- **COTS** is configurable/ commercial, off-the-shelf software
- Software vendors **test/validate** COTS packages to meet industry standards
- Companies with end users of COTS software **cannot assume** the software was developed or validated in accordance with current Good Manufacturing Practices (cGMPs)
- They **must validate** these to meet FDA standards
- FDA is **increasingly concerned** that companies are not doing enough

- For a **COTS application** used in an automated process, assess the **audit the vendor & review their SDLC methodology**
- For **COTS tools** (e.g., compilers, linkers, editors, operating systems, & databases), exhaustive **black-box testing may be impractical**
- Validation of tools may be **inferred** by validating the **application usage requirements** that are traceable & indirectly implemented by the COTS tool functions
- **Software tools** are frequently used to design, build, and test the software for an automated medical device

- The main ***compliance-related purpose*** of validation is to ***ensure accuracy and integrity of data*** created, modified, maintained, archived, retrieved, or transmitted by the computer system
- In addition, validation is typically a ***pre-requisite for reliable system operation & maximum uptime***
- Depending on the ***complexity & functionality***, validation of computer systems can be a ***huge task***

- Adoption of ***new technologies*** by the life science industry remains conservative, but is ***loosening up***
- The approach includes ***identifying and mitigating risk*** to protect public safety
- The increase in usage of cloud technology has brought it into the ***mainstream*** and is now considered to be a ***viable and secure*** option
- The ***approach to validation*** and effort to maintain the system in a validated state must be ***tailored*** accordingly

- Needs for ***mass processing and management of data*** is escalating, increasing demand for scalable and fast-delivery solutions, while reducing costs
- ***Cost-effective solutions*** are needed to minimize IT management and maximize capacity for data and growth
- ***SaaS solutions*** fit this model perfectly, but create concerns about compliance and security, specifically related to HIPAA and FDA regulations
- The key is ***understanding the risks*** and the technical and procedural ***controls*** that need to be implemented

- Requires a ***comprehensive compliance framework***, with a view of intended purpose of the solution & how it's controlled
- Requires a ***robust validation strategy***, a QMS with enterprise-wide ***controls***, & a ***secure application infrastructure*** with ***encryption*** of PHI communications
- ***Maintaining a SaaS solution*** requires a repeatable way to ***minimize*** requirement & test tasks
- ***Simplifying*** validation & maintenance of a SaaS solution requires ***risk assessment*** with a strong ***defensive case***
- ***Level of testing & documentation*** is based on ***risk appetite***

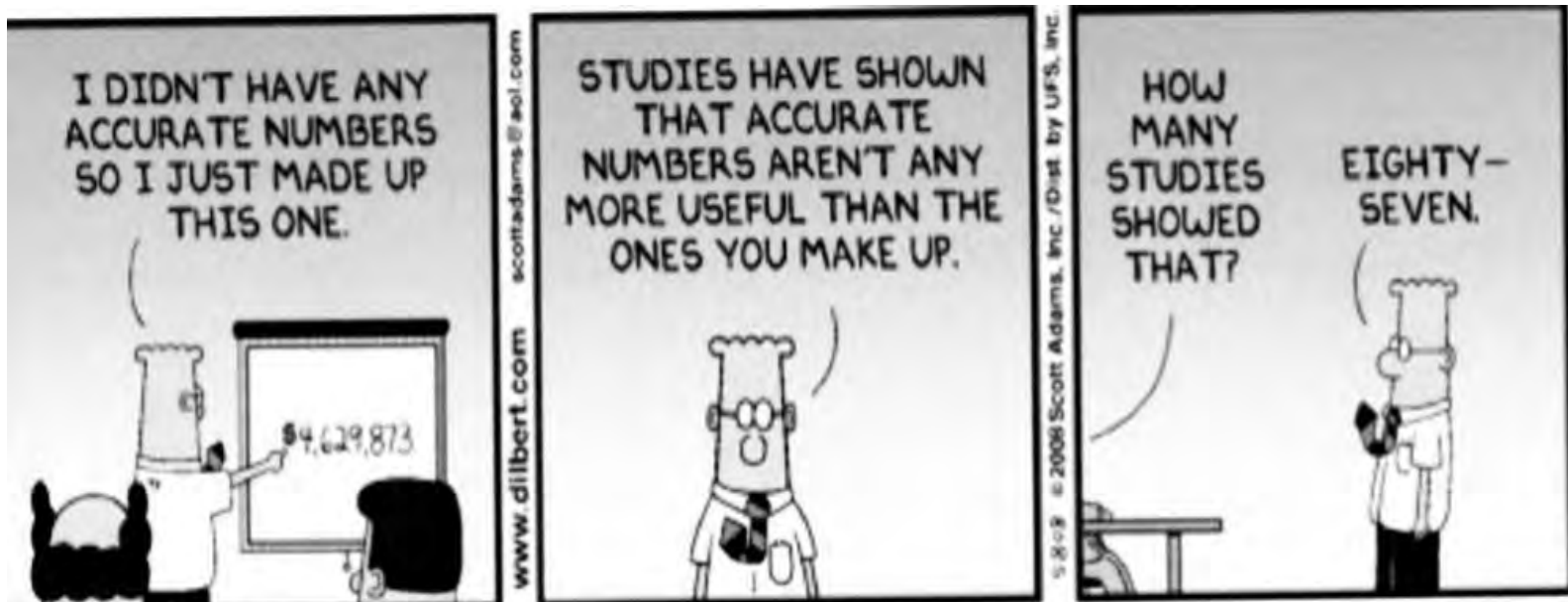
- Discuss with the provider their ***responsibilities related to IT & compliance***, & put in contract to hold them accountable
- ***Clients ultimately own compliance*** on their solution instance
- There is ***opportunity*** to streamline requirements, if the provider thoroughly complies with regulations
- A cloud/SaaS provider must be ***SOC 2 certified***
- Ensure you can ***retrieve your data from the cloud*** if the ***vendor ceases support***



Data Integrity

Why is Data Integrity Important?

- Data integrity problems ***break trust***
- We ***rely largely on trusting the firm*** to do the right thing when we are not there
- It's very difficult to ***regain trust*** once it is lost



Data Integrity and Compliance with cGMP Guidance for Industry, December 2018:

21 CFR Parts 211 and 212

- Requirements with respect to data integrity include:
 - **211.68** – “backup data are exact and complete,” and “secure from alteration, inadvertent erasures, or loss”
 - **212.110(b)** – data be “stored to prevent deterioration or loss”

- **211.100 and 211.160** – activities be “documented at the time of performance” & lab controls be “scientifically sound”
- **211.180** – records retained as “originals,” or “true copies,” or other “accurate reproductions of the original records”
- **211.188, 211.194, and 212.60(g)** – “complete information,” “complete data derived from all tests,” “complete record of all data,” and “complete records of all tests performed”

Must address the **ALCOA** data integrity components:

- **ATTRIBUTABLE**
- **LEGIBLE**
- **CONTEMPORANEOUS**
- **ORIGINAL** or **“TRUE COPY”**
- **ACCURATE**

Data Integrity (continued)

Must address the **ALCOA+** data integrity components:

- **ATTRIBUTABLE**
- **LEGIBLE**
- **CONTEMPORANEOUS**
- **ORIGINAL** or **“TRUE COPY”**
- **ACCURATE**

PLUS

- **COMPLETE**
- **CONSISTENT**
- **ENDURING**
- **AVAILABLE**

	REQUIREMENT	ACCEPTANCE CRITERIA	CONTROLS (Technical & Procedural)
A	ATTRIBUTABLE	The identity of who performed the action & when; If record is changed, who did it, when, and why?	User authentication, password security, audit trail, automated versioning
L	LEGIBLE	Data must be recorded permanently in durable medium and must be readable	Must be in “human readable format”
C	CONTEMPORANEOUS	Data must be recorded at the time work is performed	Work must be recorded in real time
O	ORIGINAL OR “TRUE COPY”	The information is an original record or verified & documented “True Copy”	Must identify as original or must have evidence it is a “true copy”
A	ACCURATE	No editing can be performed without documented evidence	Audit trails (structured data) & Automated versioning (unstructured data)
P L U S	COMPLETE	All data including repeat or reanalysis performed sample (21 CFR 211.94)	Must include ALL data & investigate & document if not
	CONSISTENT	Consistent application of date & time stamps in expected sequence	Automated date/time stamp on audit trail & versioning
	ENDURING	Recorded on controlled worksheets, bound/numbered lab notebooks or media	Must be on medium that is durable and lasting
	AVAILABLE	Available and accessible om “human readable format” on screen or paper	Must be available for the lifetime of the record

Metadata:

Describes attributes of data, provides ***context & meaning:***

- Audit trails (old/new values, who, when, why)
- Processing information
- Methods

Static: Fixed record or print-out

Dynamic: Electronic record a user can interact with & modify

Backup: Editable data, with metadata & configuration settings

System validation: including backup & recovery process

Frequent Data Integrity Citations:

- Excluding cGMP data from ***decisions*** without justification
- Workflow not ***end-to-end*** tested/validated
- Access ***restrictions*** not appropriate
- Concerns with ***shared*** login accounts, passwords
- Controls for ***blank forms*** not in place
- ***Audit trails*** not reviewed
- Electronic copies ***not compared*** with paper, if scanning
- Paper printouts ***not compared*** with screen copy
- Electronic signatures ***not defined or secured***
- Electronic cGMP records ***not secured***

Examples:

Your firm failed to ensure that ***laboratory records*** included complete data derived from all tests... (21 CFR 211.194(a))

- ***Raw data*** (sample preparation) not maintained
- ***Discarded*** data in the trash

Your firm ***failed to exercise appropriate controls*** over systems to assure ***only authorized personnel institute changes*** in master production and control records... (21 CFR 211.68(b))

- ***Lack of basic controls*** to prevent changes to electronic data
- ***Audit trails*** turned off
- ***No control*** over substituting, deleting, overwriting data
- ***Sharing*** user names and passwords

- Manufacturing & product testing data ***not secured***
- Data not attributed to a uniquely authenticated user
- Data ***falsified*** and ***inaccurate***
- Documentation not completed ***contemporaneously***
- ***Raw data*** not available
- Training file ***re-written*** to remove the original record
- QC created ***unauthorized*** computer folders
- Failure to record activities ***at the time they are performed***

- Failure to prevent ***unauthorized access*** or ***changes to data*** & provide ***adequate controls*** to prevent ***omission of data***
- Only included ***most favorable result*** from multiple results ***without*** justification (Testing into Compliance)
- ***Destruction*** of original records
- “Rough notes” (loose paper) used to capture ***original critical manufacturing data*** were ***destroyed after transcription*** into the batch production records
- ***Backdating*** of production records when personnel were not onsite to perform the activity

Typical Data Integrity observations:

- Alteration
- Fabrication
- Misrepresentation
- Omission
- Deliberate willful deception
- Fraud
- Inadequate data or documentation retention practices
- Questionable, poor, incomplete documentation practice
- Altering information on the certificate of analysis
- Is QA oversight lacking? Symptom of weak QMS?
- Why not found internally/previously?

Typical FDA Form 483 data integrity observations:

- “...trial injections.....”
- “...results failing specifications are retested until acceptable results are obtained....”
- “...over-writing electronic raw data.....”
- “...OOS not investigated as required by SOP....”
- “...appropriate controls not established for....”
- “....records are not completed contemporaneously”
- “... back-dating....”
- “... fabricating data...”
- “.... No saving electronic or hard copy data...”

- **Changes** to the chromatographic data or injection sequence should be **documented** in an **audit trail**
- **Aborted or incomplete** injections should be captured in **audit trails** and should be **investigated and justified**
- It is **not** acceptable to record data on **pieces of paper** that will be **discarded** after the data are **transcribed** to a permanent laboratory notebook
- It is **not** acceptable to store electronic records in a manner that allows for manipulation without creating a **permanent record**
- You may employ a combination of **technical and procedural controls** to meet CGMP documentation practice

- **All data** created as a cGMP record must be evaluated by Quality against release criteria and maintained
- Electronic data **includes relevant metadata** required to reconstruct the activity captured in the record
- **Invalidating test results** to exclude them from quality unit decisions about conformance to a specification requires a **valid, documented, scientifically sound justification**
- If legitimately invalidated, the **full cGMP batch record should include the invalidated data**, along with the investigation report that justifies invalidating the result

- Any cGMP workflow is an ***intended use*** of a computer system and ***must be validated***
- The ***extent*** of validation testing must align with the ***potential risk posed*** by the automated system, should it fail
- FDA recommends implementing ***appropriate controls*** to ***manage risks*** associated with each element of the system
- FDA recommends ***appropriate controls*** to assure only authorized personnel can make ***changes to records***
- The ***ability to alter*** specifications, process parameters, data or manufacturing/test methods should be restricted to ***technical teams*** only

- Authorization to ***alter files and settings*** should be assigned to a system administrator who is ***independent*** from users responsible for record content
- A method should be documented for ***authorization of access and associated privileges*** for FDA-regulated systems
- All sets of ***blank forms*** that are ***numbered*** should be ***issued and reconciled*** upon completion of them
- ***Incomplete or erroneous forms*** should be kept as part of the ***permanent record*** along with ***written justification*** for their replacement

- Audit trails should be **reviewed** by the same organization that would review notebooks or other hard copy data records
- **Audit trail review** should be at the **same frequency** as mandated by cGMPs for the records involved
- **Electronic copies** can be used as **true copies of paper or electronic records**, provided they **preserve the content and meaning** of the original, **including all metadata** to reconstruct the cGMP activity and the static or dynamic nature of them

- ***True copies of dynamic electronic records*** may be created and maintained in the ***format of the originals*** or in a ***format that preserves the content and meaning*** of the original if a ***suitable reader and copying equipment*** are readily available
- ***Paper printouts*** (static records) may be retained instead of ***original electronic records*** from stand-alone computerized lab instruments
- A ***paper printout*** (static record) may satisfy retention requirements if it is the ***original record or a true copy***, provided it is ***retained***

- If the electronic records are ***dynamic***, a printout (static record) ***does not preserve the dynamic record format*** that is part of the complete original record
- Electronic data becomes a ***cGMP record*** when ***generated***
- It must be documented, or saved, ***at the time*** of activity performance (contemporaneously)
- FDA expects processes to be designed so that data required to be created and maintained ***cannot be modified without a record*** of the modification (such as an audit trail)
- Chromatographic data should be saved to ***durable media*** after ***each step*** or injection, not at the end of an injection set

Many companies are cited for failing to:

- perform ***“systemic corrective action”***
- provide ***reasonable/responsive timelines*** for remedial action
- provide ***objective evidence*** of remedial action
- provide ***training*** for updated procedures
- ***assess*** all product adversely “affected”
- ***specifically*** address violation cited
- conduct ***retrospective*** reviews
- provide ***supporting evidence*** when disagreeing with FDA
- take a ***holistic view*** of deficiencies and act accordingly

Recent DI publications include:

- UK's ***Medicines & Healthcare products Regulatory Agency*** (MHRA) GMP Data Integrity Definitions & Guidance for Industry, March 2015; DI blogs: org behavior, ALCOA principles
- ***FDA*** Warning Letters and Import Alerts
- ***European Union Drug Regulating Authorities*** (EUDRA) GMDP database noncompliance
- ***Health Canada*** Feb 2015 stakeholders letter including DI notification
- ***Health Canada*** Inspection tracker for GMP & DI observations
- Expected guidelines from ***World Health Organization*** (WHO)

KEY TAKEAWAY:

*These requirements are **NOT NEW***

To prepare for inspection, ask these questions:

- Is the software and hardware ***suitable*** to perform the task?
- Have system ***incidents*** been recorded, root cause ***investigated, remediated, retested based on risk?***
- Is ***security monitored*** and the results recorded?
- Are audit trails routinely reviewed & is it documented?
- Are ***changes*** done by SOP; approved, recorded, & tested?
- Are ***records*** of all changes, including enhancements to hardware, software, or other critical component available?
- Can you show the system is ***maintained*** in validated state?

Data Life Cycle:

- Consists of **7 phases**
- Each phase has its own characteristics
- If we could follow a piece of data as it moved through the enterprise, we would understand the various phases and characteristics

1. Data Capture

- An item of data must pass within the enterprise firewalls
- The act of creating data values that do not yet exist and have never existed within the enterprise
- **Three main ways to capture data:**
- **Data Acquisition:** ingestion of existing data produced by an external organization; contract governs how it can be used
- **Data Entry:** creation of new data values for the enterprise by humans or devices
- **Signal Reception:** capture of data created by devices, typically in control systems, but also for information systems

2. Data Maintenance

- Once data ***captured***
- Supplying of data to points at which ***Data Synthesis/Usage*** occur, ideally in a form best suited for these purposes
- ***Processing data*** without deriving value from it
- Often ***involves*** movement, integration, cleansing, enrichment, changed data capture, and extract-transform-load (ETL)
- Focus of a ***broad range*** of data management activities
- A ***challenge is rationalizing*** how data is supplied to the end points for Data Synthesis/Usage, preventing proliferation of point-to-point transfers

3. Data Synthesis

- Creation of data values via ***inductive logic***, using other data as input
- ***Area of analytics*** that uses modeling, such as risk modeling, actuarial modeling, and modeling for investments
- Inductive logic requires some kind of ***expert experience, judgment, and/or opinion*** as a part of the logic, e.g. the way in which credit scores are created

4. Data Usage

- The application of ***data as information*** to tasks that the enterprise needs to run and manage itself
- Data is becoming more central to ***business models*** in many enterprises
- Data may itself be a ***product or service*** (or part of a product or service) that the enterprise offers
- ***Data Governance*** challenges include evaluating whether there are regulatory or contractual constraints on how data may be used, and must ensure these are met

5. Data Publication

- Sending data to a location ***outside*** of the enterprise
- Once data has been sent outside the enterprise it is ***de facto impossible to recall*** it
- Data values that are wrong ***cannot be corrected*** as they are beyond the reach of the enterprise
- Data Governance may be needed to assist in ***deciding how*** to handle this
- ***Data breaches*** also fall under Data Publication

6. Data Archival

- A single data value may experience ***many rounds of usage*** and publication, and eventually, it reaches the end of its life
- ***Copying of data*** to an environment where it is stored in case it is needed again in an active production environment
- This is followed by ***removal of this data*** from all ***active*** production environments
- A data archive is simply a ***place where data is stored***, but where no maintenance, usage, or publication occurs
- If necessary the data ***can be restored*** to an environment where one or more of these occur

7. Data Purging

- We now come to the actual ***end of life*** of our single data value
- Data Purging is the ***removal of every copy*** of a data item from the enterprise
- Ideally, this will be done from an ***archive***
- A Data Governance challenge is ***proving*** the purge has been ***done properly***

- Requires a ***framework*** for enterprise-wide integrity
- ***IT Security group*** is the assurance that information can be accessed and modified only by those authorized to do so
- ***Database Administrator*** for making sure data entered into the database are accurate, valid, and consistent
- ***Data Owner*** provides a measure of quality, with appropriate business rules and defined relationships between entities
- ***Regulator*** ensures data integrity is the quality of correctness, completeness, wholeness, soundness, and compliance, and intentions of data creators

- ***Impossible to eliminate*** all vulnerabilities to data integrity in the organization; ***controls should:***
 - be established to ***reduce*** the propensity for data integrity ***errors and vulnerabilities***
 - ***integrate and coordinate the capabilities*** of people, operations, and technology through a data integrity ***assurance infrastructure***
 - be part of a ***control framework*** designed to integrate capabilities, and molded to fit virtually any organization
 - ***Support this framework*** along with data management and governance to ensure ***enterprise-wide data integrity***

Build a Sound Data Integrity Strategy:

- Design and establish an infrastructure to manage data availability, usability, integrity, and security
- *Data management is execution of data architectures, policies, practices, and procedures*

At its core, data governance has four goals:

- *Meeting compliance* requirements
- Making data *visible* to *C-level* management
- *Improving operations*
- Assisting efforts to *fix data quality* at *department level*

Organize Governance Teams:

- Create a ***governance strategy*** and define decision rights (using a RACI chart) for the following activities:
- ***Developing*** and ***approving*** policies and procedures
- ***Monitoring*** compliance
- ***Establishing SLAs***
- Protecting ***system architecture***
- Managing raw ***metadata***
- Managing ***security and access***

Factors for Data Governance Success:

- Effectiveness of your strategy will be based on **key factors**:
 - Quality of company **culture** and **decision-making** process
 - Selecting the **right business stakeholders** in developing governance strategy
 - Considering industry **best practices**
 - **Executive management** providing **sponsorship**
 - Providing **ongoing funding and resources**
 - **Integration** with the company's **QMS** (no separate program)

Data Management:

4 Questions to Inform your Processes:

1. Why is data required?
2. How will you collect it?
3. How will you validate it?
4. How will you handle it?

Six ways to improve data integrity:

1. Conduct real-time quality reviews
2. Train for data and process management
3. Automate data capture
4. Drop spreadsheets for data storage
5. Map your entire process workflow
6. Adopt developing industry standards

Put these Best Practices to Work:

- ***Comprehensively assess*** computer system/data to ensure system requirements fully met and documented
- ***Evaluate*** data governance/management practices using risk-based validation strategies to protect data integrity and strengthen the Quality Management System (QMS)
- ***Comprehensively remediate*** compliance gaps identified during the assessment
- ***Thoroughly validate*** computer systems to ensure they stand up to scrutiny and assure data is safe, reliable, and available

Data Governance (continued)

1. Data Strategy

- Data Management Strategy
- Communications
- Data Management Function
- Business Case
- Funding

3. Data Quality

- Data Quality Strategy
- Data Profiling
- Data Quality Assessment
- Data Cleansing

4. Data Operations

- Data Requirements Definition
- Data Lifecycle Management
- Provider Management

5. Platform & Architecture

- Architectural Approach
- Architectural Standards
- Data Management Platform
- Data Integration
- Historical Data & Archiving

6. Supporting Processes

- Measurement & Analysis
- Process Management
- Process Quality Assurance
- Risk Management
- Configuration Management

2. Data Governance

- Governance Management
- Business Glossary
- Metadata Management

Data Governance provides a framework for dealing with the challenges around **data compliance and regulation**:

- **Aids** in management of the availability, usability, integrity, quality, consistency, and security of data
- Helps **meet compliancy** with laws and regulations
- Is a component of **Enterprise Data Management**, providing and enforcing:
 - Enterprise-wide data **standards**
 - Common **vocabulary** and **terminology**
 - Common **reports**
 - Standardized **processes**

- **Data Governance** can be leveraged in ***maintaining data integrity*** by managing data more efficiently/effectively to:
 - Establish and maintain ***consistent data definitions***
 - Measure and track the ***quality of transactional and analytical data*** used across the enterprise
 - More easily ***integrate, synchronize and consolidate data*** from different departments or across different systems
 - Exchange and transfer data in a ***common format*** allowing for faster decision-making

- **Coordinate communication** between business units and IT
- **Provide insight** into the data across the business applications through shared terminology and reporting
- **Coordinate activities** due to standardized processes and access to enterprise-wide data
- Improve **business intelligence** reporting
- **Reduce costs** by improving data quality and minimizing cleansing activities
- Provide a **single-source of data** to ensure accuracy and consistency across the organization
- Reduce costs by **eliminating redundant** data stores

There are ***six key elements*** of the Data Governance Framework, including:

1. Organization
2. Policies, Principles & Standards
3. Processes, Practices & Architecture
4. Investigation & Monitoring
5. Gap Analysis
6. Tools & Technology

Organization

- Representative ***participation and commitment*** from both IT and business stakeholders
- Senior level ***executive sponsorship*** from both areas
- ***Active consulting practices*** to drive and champion case

Data Governance Board:

- ***Oversees data assets*** that exist across the enterprise
- Is ***sanctioned through approved charter*** defining scope, objectives, authority, organization, procedures & metrics
- Sets and authorizes the ***direction*** of data governance
- ***Aligns*** business and IT goals

- ***Manages*** organizational data as a strategic asset
- ***Drives*** business priorities and regulatory compliance
- defines ***roles and responsibilities*** for data owners
- creates data ***policies, procedures and standards*** for the organization as a whole
- ***directs*** how data should be used, managed, and monitored across the organization

Policies, Principles & Standards

A policy must be developed for ***enforcing data standards and governance procedures*** that specify who is ***responsible and accountable*** for various segments and aspects of the data, including its:

- accuracy
- accessibility
- consistency
- completeness
- how it is updated

Processes, Practices & Architecture

- Processes must be ***established and formalized*** to guide principles for how policies, processes, and standards are created, collected, modified, implemented, and distributed across the organization
- ***Without*** formalizing the process, IT will constantly find itself having to ***demonstrate its value add*** to business stakeholders
- Setting formal processes and practices helps ***identify and document*** how the organization ***manages its data***

- The organization ***must define how*** the data is “to be” stored, archived, backed up, and protected
- ***Practice and procedures*** are also instituted to ensure compliance and government regulations and audits met
- ***Data Governance processes and practices*** help organizations face challenges of enterprise level data integration concerns and include enterprise standardization for data and systems

Data Architecture:

- addresses how the data is to be ***organized and integrated***
- includes ***enterprise*** data standards, data models, data flow diagrams, mapping spreadsheets, data definitions, and a metadata dictionary, in addition to ***security and privacy*** measures
- is ***essential*** for determining requirements and preparing the organization for efficient and effective data integration

Data Integration:

- involves the process of ***cleansing, transforming, merging and enriching*** data that is merged from multiple sources
- ***addresses*** error handling, scheduling, process restart capabilities, data administration, gaps in data and audit
- ***ensures data is integrated*** in the timeframes required by the business and outlined in the SLA

Data Cleansing:

- identifies ***data model schema differences*** (data types, length, value)
- ***validates rules*** based on business user roles and processes
- ***recognizes duplication*** of data, behaviors, and functionality

Data Quality:

- Involves problems with ***incorrect*** and/or ***inconsistent data***
- Requires ***creating and managing data models*** from the source system
- Requires creating ***enterprise standards***
- Can be aided using a ***data profiling tool*** to allow for:
 - Data to be ***assessing*** to identify cross-system data overlap & ***consistency***
 - ***Metrics*** to track the effectiveness across the enterprise
 - ***Continuous improvement***

- Allows for an examination of duplicate definitions, dissimilarities of definitions, and ***identifying consistent inconsistency***
- ***Becomes information knowledge sharing*** where definitions, data types, entity layouts, and domains are published

Data Governance (continued)

Metadata:

- ***Structured information*** and ***business rules*** about data
- ***Can include:***
 - Data Lineage
 - Business Rules
 - Business Term Definitions
 - Ownership/Stewardship
 - Transformation Rules
 - Data Mapping

When establishing a data model repository for metadata, keep in mind differences that may exist across the organization:

- ***Different*** applications and systems have been built using ***various*** platforms and databases
- The data contained across the different applications and systems might not be stored in a ***standardized method***
- There might be different ***meanings, data types, & naming conventions***
- Some information may be captured in ***manual format***

Investigation & Monitoring

- Identify the data ***quality issues***
- ***Prioritize the issues*** based on urgency, importance, dependency, and critical success factors
- Conduct ***root cause analysis*** to determine and identify the probable cause of the data issue
- Formulating a ***corrective action plan***
- Decide on the ***next steps***
- Implement the ***fix***
- ***Monitor*** the results

Gap Analysis

- Focuses on mapping the organization's governance policies and processes against ***industry standards and best practices***
- Allows the organization to have an understanding of ***where*** their organization is, what their ***target needs*** to be, and addresses ***plans*** to get there

Tools & Technology

- Includes ***tools*** to be considered and evaluated for use during and post implementation
- ***Examples include:***
 - Data Profiler
 - Data Modeling Tools
 - Modeling Repository
 - Workflow data management application to alert, track, notify, escalate and approve Data Governance standards and policies as the model matures

The Governance Board can then:

- Plan to identify the ***tools and technologies*** needed
- Make ***recommendations*** for best approaches in creating a ***standardized model*** that accommodates the requirements and organizational strategic objectives and initiatives
- Determine ***requirements*** for a “to-be” data architecture and enterprise information model, business impact for implementing Data Governance
- Identify ***possible actions*** to take to ***mitigate risk***
- Identify methods of effective ***communication and training*** with the business stakeholders

Part 5:

- ***Vendor Audit***
- ***FDA Inspection Trends***
- ***Industry Best Practice***

- GxP systems must be **validated** in accordance with specific requirements
- Vendor audits are needed to ensure **quality control** in an industry regulated more than any other industry in the world
- It provides a company with a means to verify a **vendor meets** applicable **FDA laws & regulations**
- The intent is to evaluate the **quality management** of the vendor by assessing the procedures and data system processes used to ensure all **products and services** your company purchases meet FDA compliance requirements

- For any computer system, the company must be able to demonstrate the use of appropriate ***technical and procedural controls***
- The vendor's ***documentation*** to support their quality program must be available, accurate, and must meet FDA requirements
- FDA-regulated companies typically ***leverage*** the expertise of other product and service organizations, rather than building the technical and automation capability internally, as part of their ***business strategy***

- By auditing vendors, an organization can **reduce its costs** and **improve quality control** specifically by:
 - Providing great value during validation by **reducing duplicate effort** (e.g., testing)
 - **Clarifying expectations** and reducing vendor/ client misunderstandings and risk
 - **Establishing relationships** with vendors to improve quality of their products and services over time
- Must audit at least **every two years** during the life of a product or period of the service delivered

- ***Several key areas*** must be evaluated during the course of a vendor audit:
 - ***Viability*** of the company
 - Assigned ***responsibility*** and ***accountability***
 - Accurate ***system performance*** in comparison with functional requirements
 - The ability of the system to maintain ***data integrity***

Viability:

- Review website news and available ***financial information*** to determine company stability
- Consider ***client base*** and history of ***user support***
- Assess the company's ability to be ***transparent***
- Determine whether products and/or services have been the subject of any ***FDA concern or citation***

Responsibility and Accountability:

- The vendor's assignment of ***responsibility*** for leadership, operational management and key decision making should be evaluated
- The vendor's company culture should be assessed in terms of ***accountability*** for all levels of the organization
- The ***user group*** associated with the vendor's product(s) should be contacted for additional insight

System Performance:

- The vendor of a hardware or software system must be able to demonstrate the system performs consistently, and in accordance with the ***functional requirements***
- The vendor should successfully execute an ***Operational Qualification (OQ)*** test and provide thorough documentation to support the conclusions

Data Integrity:

- The vendor of a hardware and/or software system must demonstrate that the functionality sufficiently ***maintains the integrity*** of all FDA-regulated data
- The system must include proper ***audit trails***
- The vendor should follow ***change control procedures*** and secure ***system and data access*** to ensure data integrity is maintained

The vendor must demonstrate that:

- Adequate ***unit & integration testing*** is done on all code
- ***Upgrades/changes*** meet compliance for ***change control***
- ***Patches/upgrades done periodically*** & client coordinated
- Vendor of ***data migration/ conversion*** services must ensure manual & automated procedures in compliance
- Vendor must demonstrate their ***processes, procedures & practices*** are based on a ***risk assessment & GAMP[®]5*** system categorization
- Work done by vendor must be ***appropriate***, based on these

- ***Risk is critical*** to the degree of a vendor audit:
 - ***Risk*** must be determined based on how a company will ***implement & use*** the product, or what will the potential ***impact*** be on your system, processes & organization
 - Risk should be determined based on the ***probability***, ***severity*** and potential for ***identifying*** it, along with the potential for ***mitigating*** it
 - Greater risk potential requires ***more in-depth*** auditing
 - ***Discuss assigned risk with vendor*** & document it in the ***audit report***

Send a vendor a Pre-Audit Questionnaire:

- Include questions ***relevant to quality*** that can be answered in advance to minimize on-site time
- Provide ***sufficient time*** for the vendor to respond
- Follow up and confirm the vendor's responses while on site;
trust and verify
- Refer to ***previous*** audit reports or experiences with the vendor

For cloud services & SaaS solutions:

- Research vendor questionnaire on the ***vendor's website***
- Understand the ***policies, procedures, practices, & certifications***

When preparing for the audit, put on your “FDA Hat:”

- Develop specific ***objectives & expectations*** before a visit, & provide the vendor with the ***scope***
- ***Assign clear responsibilities*** to audit team members, ***matching their expertise*** to specific target areas
- Identify one person as the ***point-of-contact*** to lead the team
- Focus on determining whether the vendor’s culture, processes, & practices would ***meet FDA scrutiny***

Refer to GAMP or PDA Technical Report 32 for guidance and make sure all of these key areas are covered during your audit:

1. Quality System
2. Project Management
3. Methodology
4. Testing and Traceability
5. Records Management
6. Quality Assurance
7. Security (physical/logical)
8. Configuration Management
9. Training
10. Maintenance/ Operations

Verify Key Areas:

- ***Policies and procedures*** should be adequately reviewed and ***approved***
- ***Evaluate training practices*** & ensure they are ***documented***
- Evaluate ***written records*** to ensure they are following procedures
- Ensure the vendor ***keeps current*** with all FDA/industry standards, requirements, & best practices
- Ensure documents are in ***human readable format***, decipherable, & legible on paper or screen

More best practices:

- Be ***objective*** and avoid personal judgments
- Gather ***factual*** evidence, documents, & data
- ***Verify*** information during interviews
- ***Ask questions while on site***, & be willing to follow up
- Deliver a professional, ***constructive*** report
- Focus on the vendor's ***quality management program***
- Understand the vendor's ***challenges and constraints***
- Make note of their ***continuous improvement efforts***

- Wrap-up review & results with vendor management; be ***honest, direct, & focus*** on key areas and concerns
- Be willing to ***compromise*** where feasibility and cost are issues, but quality management is not at risk
- Plan for ***follow-up questions*** and discussions; items may come to an auditor's attention post-audit
- Provide a ***draft report*** to the vendor with sufficient time to respond before finalization
- Provide ***specific dates*** for delivery of your report & their response; ***commitments*** should be realistic & measurable

Sample deficiency - weak testing process:

- ***Lacking*** in positive and negative scenario development to ensure thoroughness
- ***Lacking*** in boundary and stress testing
- Testing ***does not reflect*** your company's use of a product
- Testers are ***not trained*** or qualified, or it is ***not documented***
- Lack of understanding of ***FDA GxP*** requirements
- ***Documentation weak, missing*** dates, no segregation of duties
- ***Change control*** lacking or poor quality
- ***Subcontractors*** not under sufficient control

Options:

- Use vendor ***unconditionally***
- Use the vendor for ***certain*** products, product versions or services only
- Use the vendor subject to specific ***corrective actions***
- Agree to ***reexamine*** the vendor in the future
- ***Prohibit*** the use of the vendor

Companies regulated by FDA have several good reasons for *meeting compliance guidelines* issued by the Agency:



- Focus on *data integrity, process quality, product quality, and patient/consumer safety*
- Continued *efficient business operations* without time/effort to respond to issues/concerns; *do things right the first time*
- *Good relations with FDA* and any other regulatory agency
- Positive company *image and reputation*; FDA citations can be publicly consumed by consumers, competitors and other agencies

FDA has many tools available to them:

- 483 Observations
- Warning Letter
- Consent Decrees
- Seizure
- Import Alerts
- Injunction
- Criminal Prosecution & Fines



FDA Inspection Trends (continued)

An ***FDA 483 observation*** is about a ***condition*** the FDA inspector believes is significant and relates to a an ***observed or possible problem*** with:

- **Facilities**

- **Equipment**

- **Processes**

- **Controls**

- **Products**

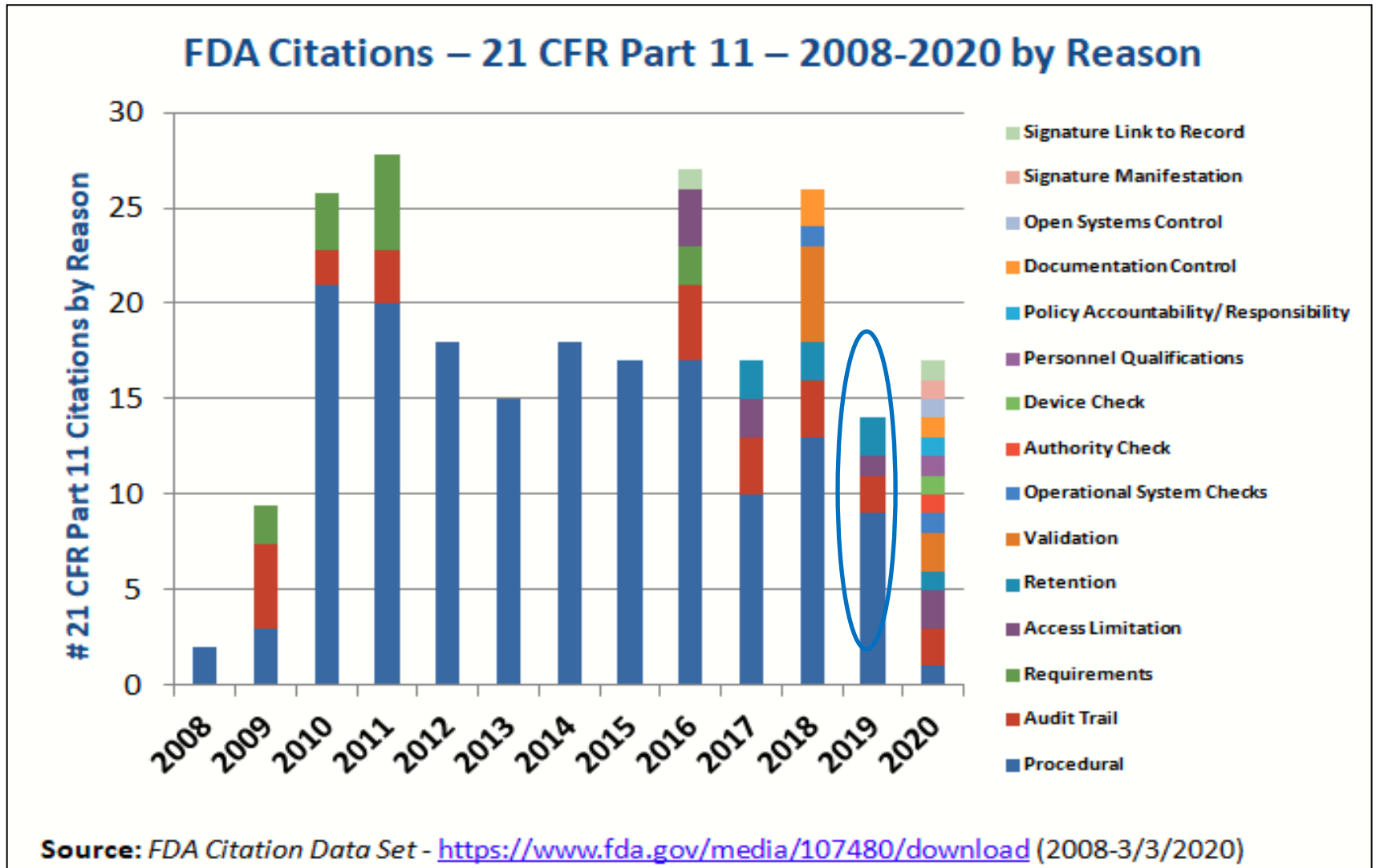
- **Employee practices**

- **Records (paper/electronic)**

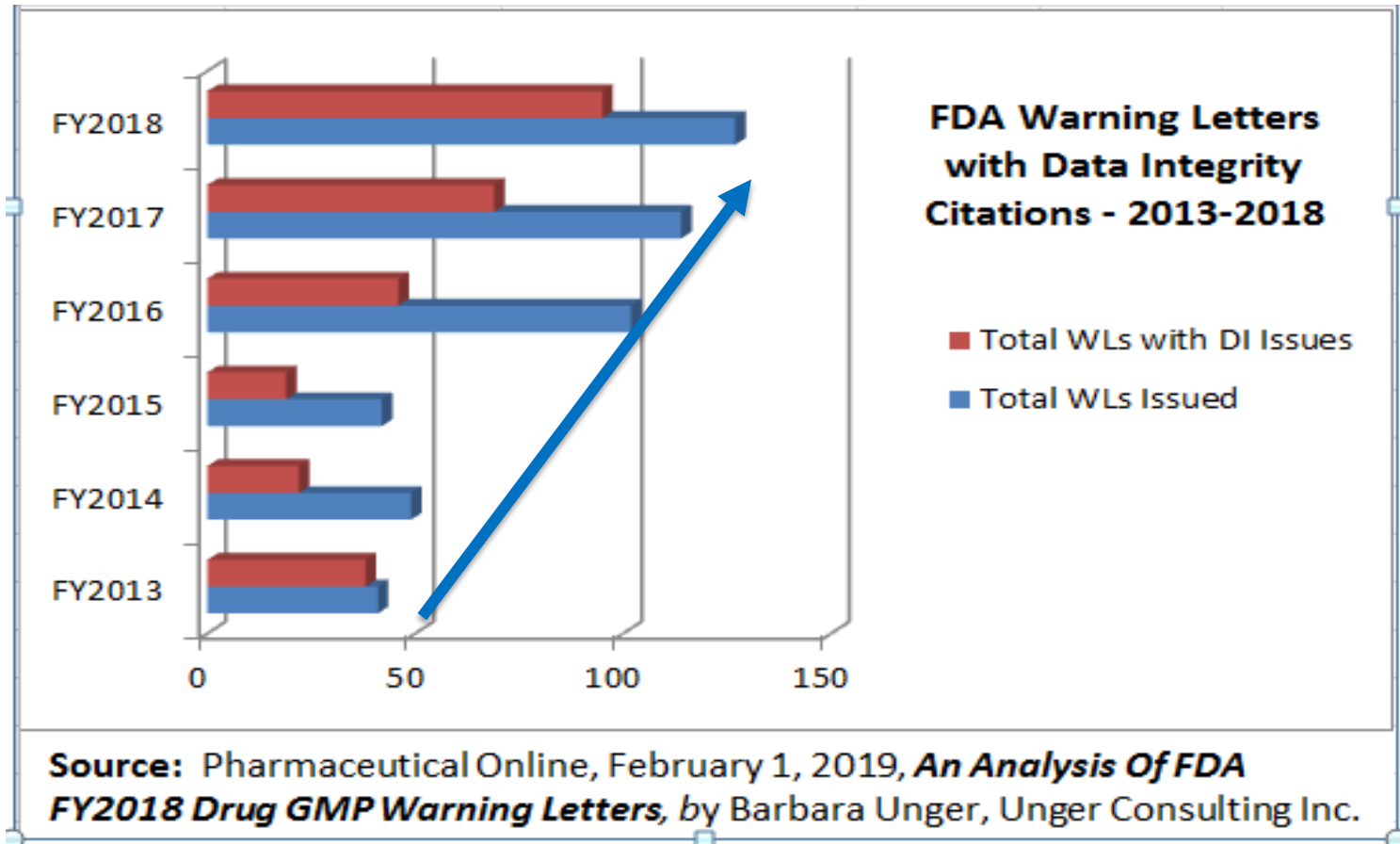
____ Areas



FDA Inspection Trends (continued)



FDA Inspection Trends (continued)



Key Takeaway:

Data/documentation deficiencies continue to increase, despite not changing requirements

FDA Inspection Trends (continued)

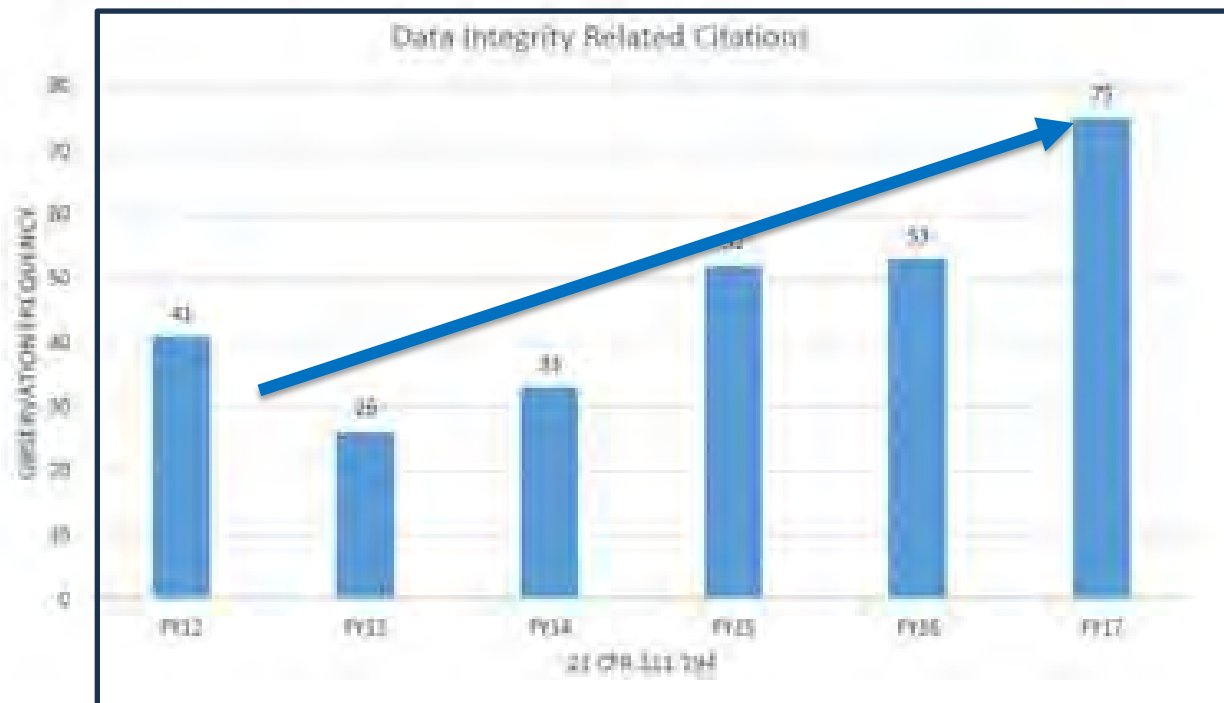
21 CFR 211.68 (b): Appropriate controls are not exercised over computers or related systems to assure that changes in master production and control records or other records are instituted only by authorized personnel.



Source: *FDA Drug Inspection Trends*, Lane Christensen, Ph.D., US FDA China Office, November 20, 2018, Hong Kong GMP Seminar
http://www.icc.com.hk/gmpseminar/pdf/Lane%20Christensen_PPT.pdf

FDA Inspection Trends (continued)

21 CFR 211.194: Laboratory records do not include complete data derived from all tests, examinations and assay necessary to assure compliance with established specifications and standards.

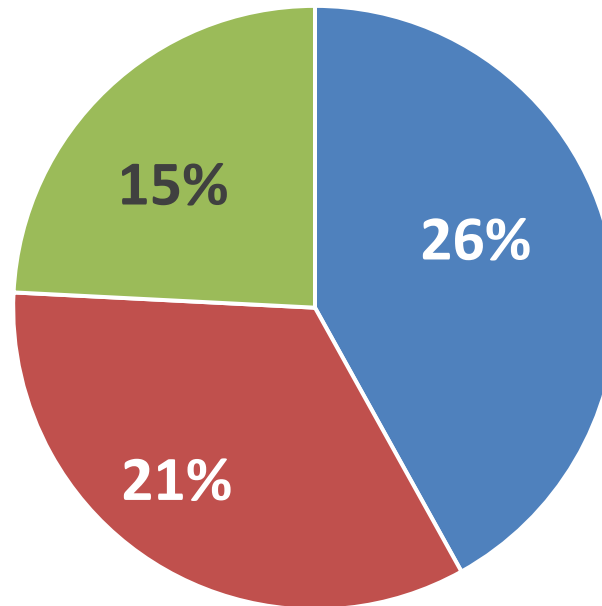


Source: *FDA Drug Inspection Trends*, Lane Christensen, Ph.D., US FDA China Office, November 20, 2018, Hong Kong GMP Seminar

http://www.icc.com.hk/gmpseminar/pdf/Lane%20Christensen_PPT.pdf

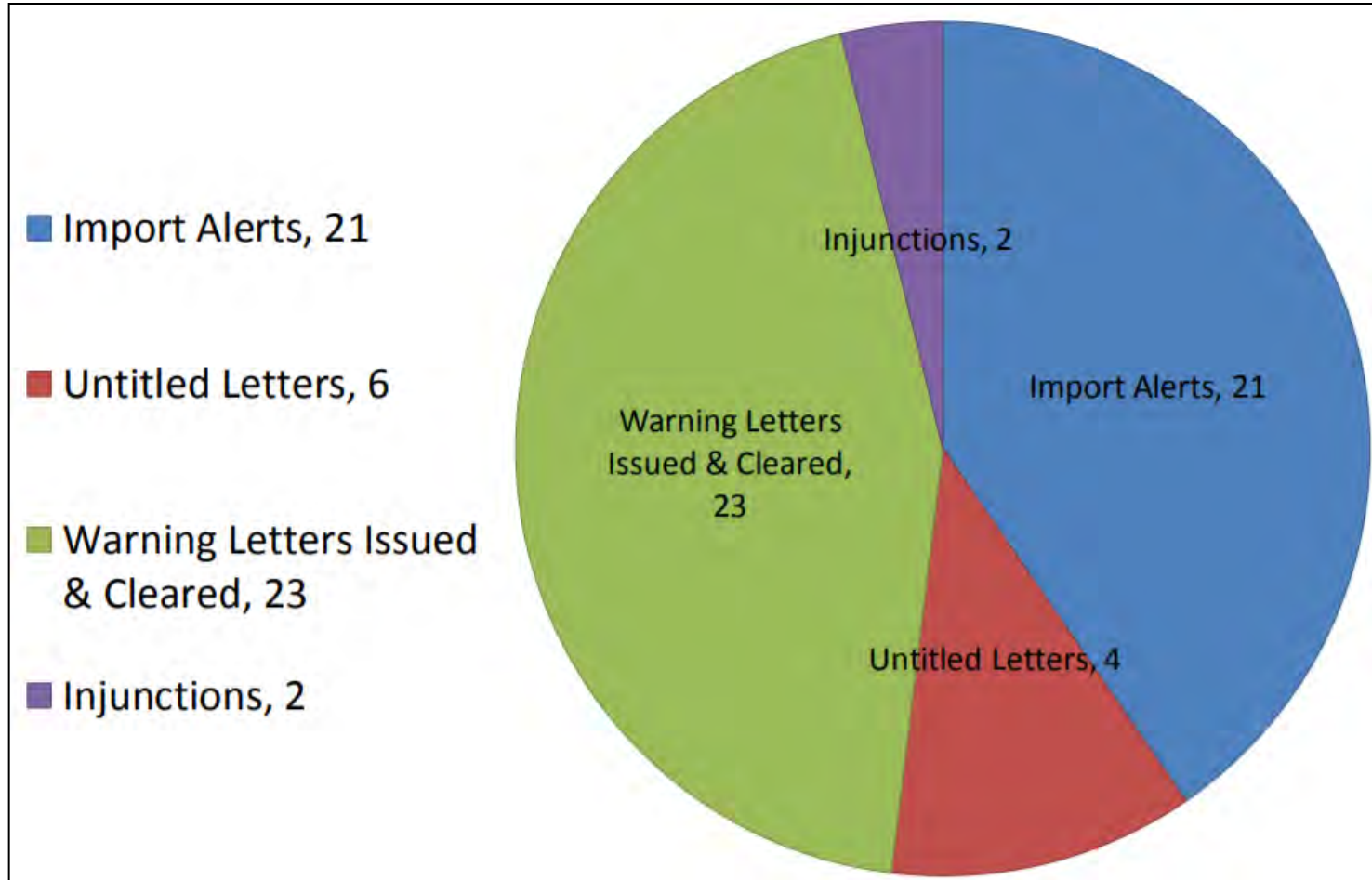
FDA Inspection Trends (continued)

Warning Letter Citations (2010-2020)



■ Process Validation ■ Data Integrity ■ Quality Control

FDA Inspection Trends (continued)



Recent Warning Letter Trends for Data Integrity

- Lack of control over access to computerized systems
- Non-contemporaneous record-keeping
- Deletion, falsification, alteration, or other manipulation
- Contract Manufacturers

Specific areas at most risk during inspection:

- Security and Access
- Testing and Validation
- Training and Expertise
- Documentation

FDA Inspection Trends (continued)



Security and Access

Recent FDA findings have pointed to more ***lax practices*** in companies when it comes to ***security and access***:

- ***Sharing*** of user names, passwords and accounts
- Lack of rigor in electronic record/signature ***security***
- Users provided with ***greater access*** than needed and/or appropriate
- ***Change control*** and ***audit trails*** compromised
- ***Segregation of duties*** not always ensured or clear

Testing and Validation

- **Lack** of validation of GxP systems, including those in GAMP® Category 3
- **Insufficient** validation of GxP systems
- Documentation **lacking**
- Testing **insufficient** (lack negative scenarios, boundary testing, stress testing)
- **Unable** to trace requirements to test scripts
- SOPs **not updated**

Training & Expertise

- Training ***not mandatory***, or ***not enforced***
- System steward ***not trained*** to ***maintain*** a system as ***validated***
- Resources doing ***validation*** not ***appropriately trained***
- Users lack training/use ***“legacy”*** systems ***confusing*** decision source
- ***Internal auditors*** are not fluent in the validation process or the systems and cannot serve the organization effectively
- ***Training logs, resumes, CVs*** not current, don't reflect needed skills

Documentation

- No documented ***risk assessment***
- ***No list of GxP systems*** and applications (prioritized by risk)
- ***Insufficient*** testing documentation
- Not following GxP requirements for ***documentation*** of CSV activities
- Incomplete or inadequate ***training records***

NOTE: *If Delay/Deny/Limit/Refuse Inspection, products can be deemed adulterated by inspector*

Some Contributing Factors:

- ***Regulatory maturity*** (regulators & inspected firms)
- ***Investigator*** background and expertise
- Company ***culture*** and ***management oversight***
- ***Prior history***/relationship with FDA office & inspectors
- ***Geographical location*** of inspected firms
- Availability of ***required expertise***
- ***Public information*** related to safety and efficacy

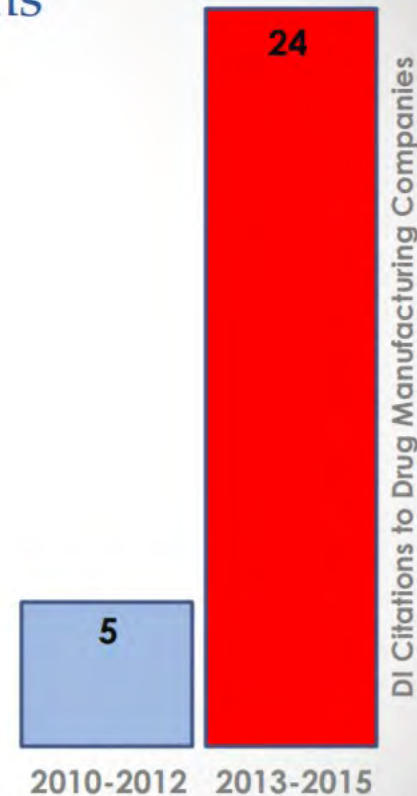
REMEMBER:

- *Requirements for record retention and review do NOT differ by data format*
- *Paper-based and electronic data record-keeping systems are subject to the SAME requirements*

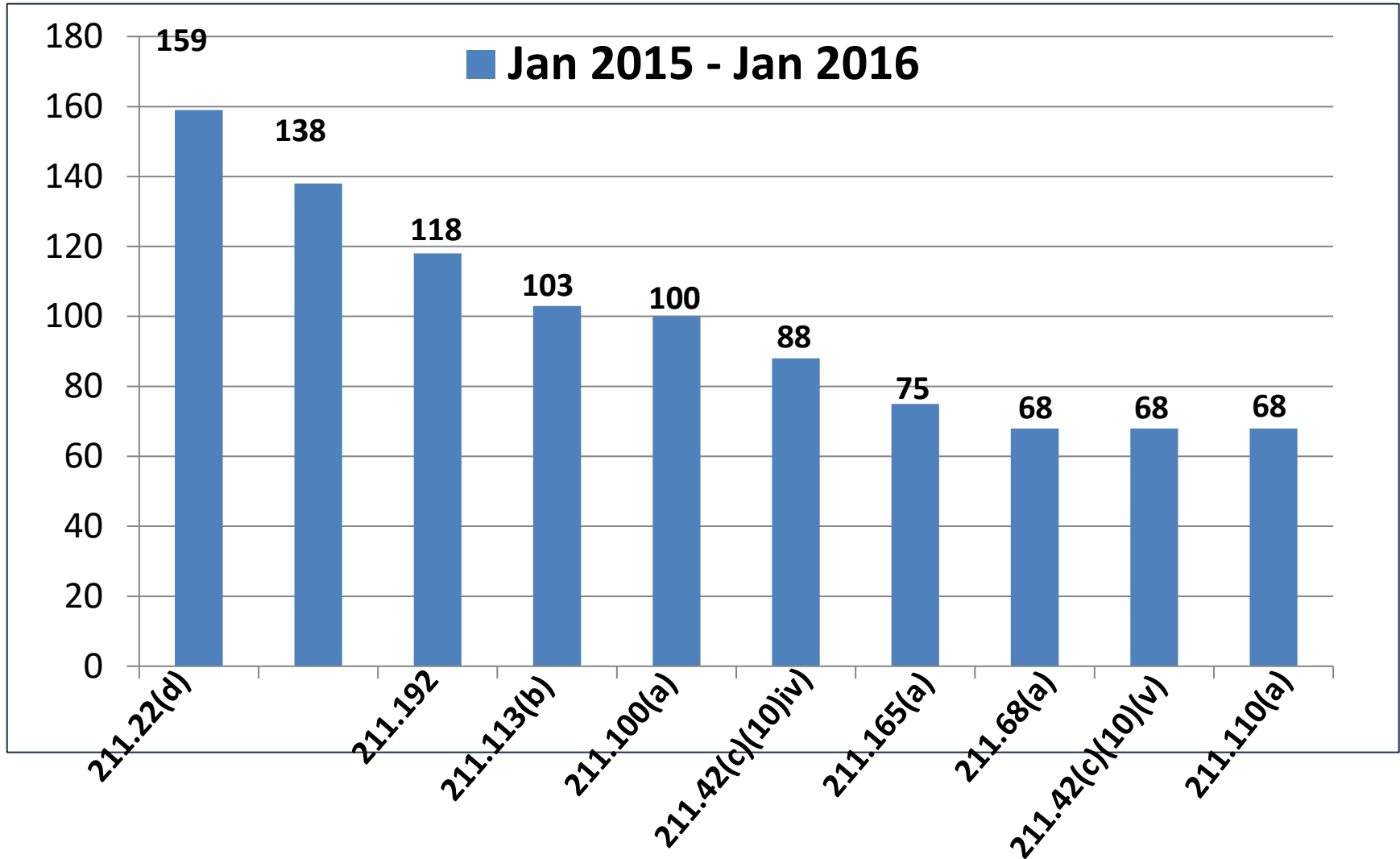
- ***Computer systems*** and the associated ***data***, whether paper or electronic, are ***essential*** to industry
- They are relied on heavily for making ***decisions and assumptions*** on ***product quality & compliance***
- ***Violations*** may have a ***negative safety, efficacy, and/or quality*** impact on ***product***, & on a ***patient***
- ***The incidence of computer system/ data integrity violations is at an ALL-TIME HIGH***

Trends of Violations

- Since 2010, the FDA has issued warning letters to an increasing number of companies for Data Integrity violations
 - The FDA issued warnings to 10 drug companies in 2015 for data integrity violations – the most in at least 10 years.



FDA Inspection Trends (continued)



FDA Inspection Trends (continued)

FDA Inspection Trends (continued)

FDA Inspection Trends (continued)

FDA Inspection Trends (continued)

FDA Inspection Trends (continued)

Yet more examples...

- Lab with test results **approved** online, but decision based on notebook data/record
- **Product released** due to approval decision based on paper, but system validation did not include validation of print-outs
- **Sharing** of user id's and passwords
- Improper use of **mobile** devices



- Sites located **globally** with time differences/issues
- Policy and/or procedure **deficiencies**
- **Outdated** Policy and/or Procedure used
- Policy and/or procedure **not followed**
- Internal audit **deficiencies**
- Training **deficiencies**
- Training record **deficiencies**



- Obtain **buy-in** for an ER/ES strategy from Senior Management
- Know the **organizational culture** – can it work here?
 - From a **user standpoint**
 - From an **IT or other support** standpoint
- Include the **business users** in all decisions
- Include **detailed scenarios** for users to play out what will happen under different circumstances
- Quality performs **internal audits**, including GxP systems & data, with findings set for remediation

- Define the ***system of record and data of record***, and base all decisions on these
- Ensure that the system of record is ***validated and maintained in a validated state***
- Validate systems ***consistently*** across the enterprise, based on approved Policies and Procedures
- Assess the ***potential risk of failure*** of all GxP systems, including probability, severity, detectability and mitigation
- Base the ***approach to validation testing*** on a risk assessment, system categorization (GAMP 5) and the size and complexity

- Create and maintain an ***inventory of GxP systems*** prioritized according to risk of failure
- Conduct a ***vendor audit*** every 2 years, using a questionnaire or site visit; document findings & follow up on activities
- Ensure ***audit trails*** used for GxP data, with original & new values, date, identity of person, & reason for change
- Use ***role-based assignment*** for user authorization
- Establish ***security procedures***/monitor activity for adherence
- Secure ***mobile devices &*** assets using an approved procedure

- Define ***system and data retention periods*** and adhere to these by preserving them through retention and disposing of them afterward to reduce liability
- Include both ***positive and negative*** test scenarios, and ***boundary and stress*** testing
- Create a ***Requirements Traceability Matrix (RTM)*** ensuring every functional requirement is unique, and has at least one design/configuration element and at least one test script associated with it

- Establish a mandatory ***training program & enforce it***
- Use ***online training***, to enable greater self-sufficiency
- Identify ***“legacy” systems*** & develop a plan to obsolete them
- Perform ***internal audits*** to ensure compliance
- ***Document*** plans, deliverables from execution, results & summary reports in compliance with FDA

- For a ***hosted environment***, ensure that the vendor is qualified, has a mature QMS and consistently adheres to Policies and Procedures
- Establish ***archival, backup and restore*** procedures and adhere to these
- Establish a ***Disaster Recovery Program*** and test the plan
- Establish a ***Business Continuity Program*** and test the plan

- ***DOCUMENT, DOCUMENT, DOCUMENT!!!***

- **Q&A**
- ***Follow-Up Items***

