



montrium

SharePoint for Pharma - SharePoint and 21 CFR Part 11 **A Risk-Based Validation Approach for Life Sciences**

**Presented by
Paul Fenton
VP Pharmaceutical Processes
and Technology**

April 23rd 2010



SharePoint for Pharma Series

- **Webinar series** that aims to highlight the different aspects of validating and using **SharePoint in GxP environments**
- Should provide attendees with a **good grounding** for their SharePoint projects
- Slides can be distributed upon request. Details on how to request slides will be distributed to attendees following each webinar
- Feel free to ask questions in the **questions panel**
- Thank you for your interest!



Overview

- Objectives of validation
- Regulatory requirements
- How to identify electronic records
- Deploying controlled and non-controlled MOSS environments
- Risk evaluation methods and scoping the validation strategy
- Step by Step overview of the risk-based validation process following the GAMP5 model
- Implementing effective configuration and change control procedures for MOSS
- Maximizing quality and ROI
- Lessons learned and best practices
- Upcoming webinars

- A formal process to ensure that:
 - systems consistently **operate** as they were **intended**
 - user, business and **regulatory** system **requirements** are met
 - information is **secure** and properly **managed** by the system
 - **procedures** and processes are in place for the use and **management** of the system



What the regulations say...

- FDA: 21 CFR Part 11
 - § 11.10(a) **Validation** of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
- ICH E6 – GCP
 - § 5.5.3(a) Ensure and document that the electronic data processing system(s) **conforms** to the sponsor's **established requirements** for completeness, accuracy, reliability and consistent intended performance (i.e. validation)



What the regulations say....

- FDA: CSUCI

§ F5 Change Control - The **integrity** of the data and the integrity of the protocols should be **maintained when making changes** to the computerized system, such as software upgrades, including security and performance patches, equipment, or component replacement, or new instrumentation. The **effects of any changes** to the system should be **evaluated** and some should be **validated depending on risk**. Changes that exceed previously established operational limits or design specifications should be validated. Finally, all changes to the system should be documented.

- PIC/S Annex 11 – PI 011-3 Good Practices for Computerised Systems in Regulated GxP Envrionments (2007)
- US FDA: General Principles of Software Validation; Final Guidance for Industry and FDA Staff (2002)



MONTRIUM

What is expected?

- That **procedures** should be in place to ensure that systems used in regulated activities are adequately validated
- That **systems** should be **maintained** in a validated state through effective **change control** mechanisms
- That sponsors take a **risk based approach** to computer systems validation (CSV)
- That **individuals** involved in CSV activities and the maintenance of validated systems have adequate **experience and training**



How to identify electronic records

- **21 CFR Part 11** defines electronic records as:
 - Records that are required to be **maintained under predicate rule** requirements and that are maintained in electronic format ***in place of paper format***
 - **Records** that are required to be maintained under predicate rules, that are maintained in electronic format ***in addition to paper format, and that are relied on to perform regulated activities***



How to identify electronic records

- **21 CFR Part 11** defines electronic records as:
 - **Records submitted to FDA**, under predicate rules (even if such records are not specifically identified in Agency regulations) in **electronic format**
 - **Electronic signatures** that are intended to be the equivalent of handwritten signatures, initials, and other general signings **required by predicate rules**

- Records within the context of MOSS could be:
 - **Documents** (excluding descriptive metadata) required to be maintained by predicate rule
 - **Metadata** (Columns) used to perform regulated activities (or make regulated decisions)
 - **InfoPath** forms used to document regulated activities



Electronic Records within MOSS

- **Electronic / Digital Signatures** used to sign records required by predicatorules
- **Audit Trails** generated for electronic records being generated and/or managed in MOSS



How to identify electronic records

- Points to consider:
 - Does the record exist in **electronic format** only with no paper source?
 - Is the record required by **predicate rule**?
 - Does the record drive a **regulated process or decision**?
- If the answer to any of the above is '**Yes**' then **21 CFR Part 11 applies** and your system must be **validated**
- You should **document** this in a validation assessment document or **validation plan**. You should also clearly identify the scope of validation in this document
- This document can help **structure** your **MOSS deployment** into controlled and non-controlled environments

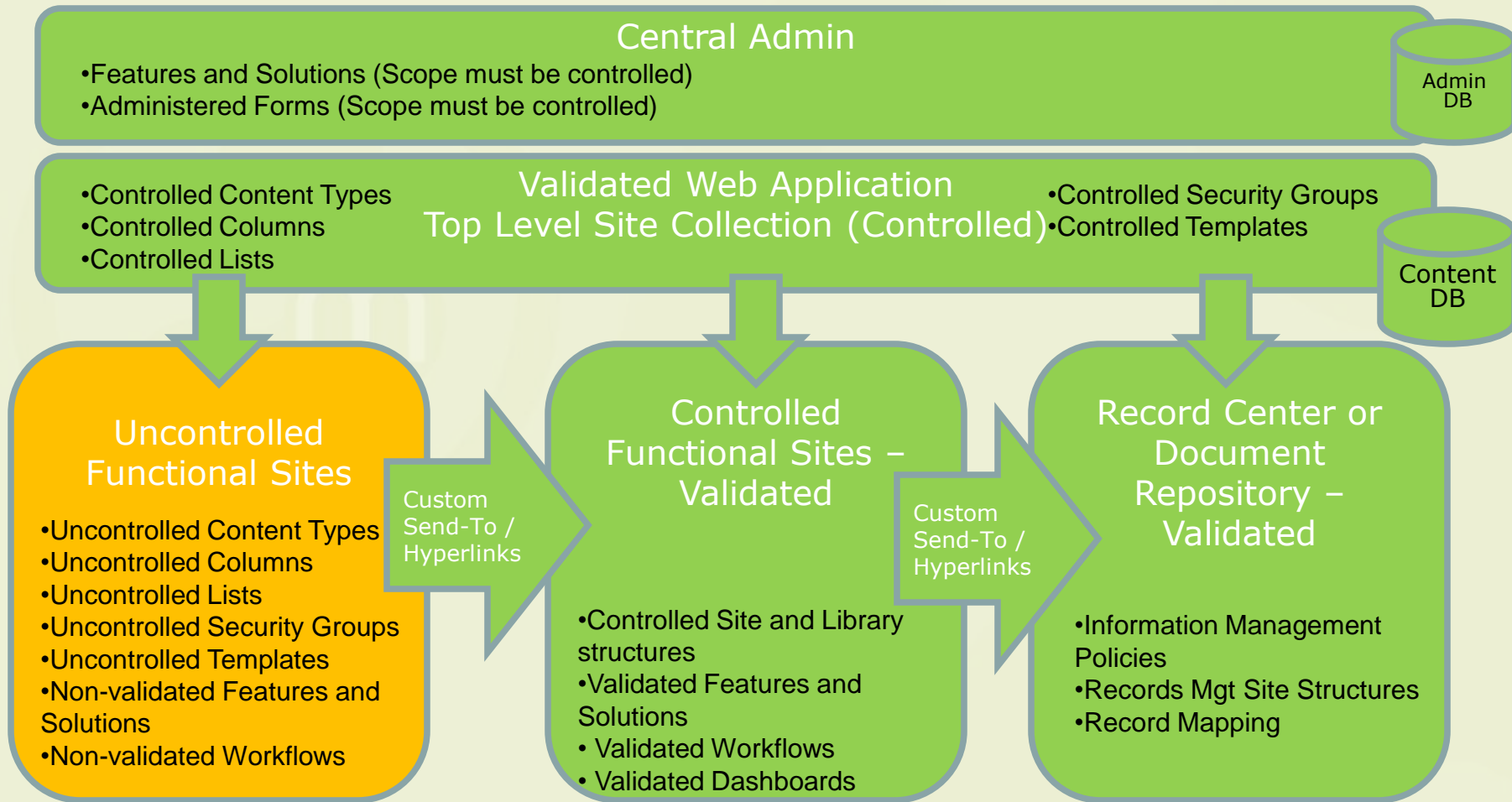


Controlled vs. Non- Controlled MOSS Architecture

- **MOSS** can be used across the enterprise for **many** different **applications** and **groups**
- It is imperative to make a **clear separation** between **controlled** (validated) and **non-controlled** environments
- This can be achieved by deploying an **independent web application/site** collection or **controlled sites** for regulated documents and processes
- There are **advantages** and **disadvantages** to both models due to limitations of MOSS
- These **architecture models** aim to offer both **flexibility** and control and **reduce validation** / change control scope

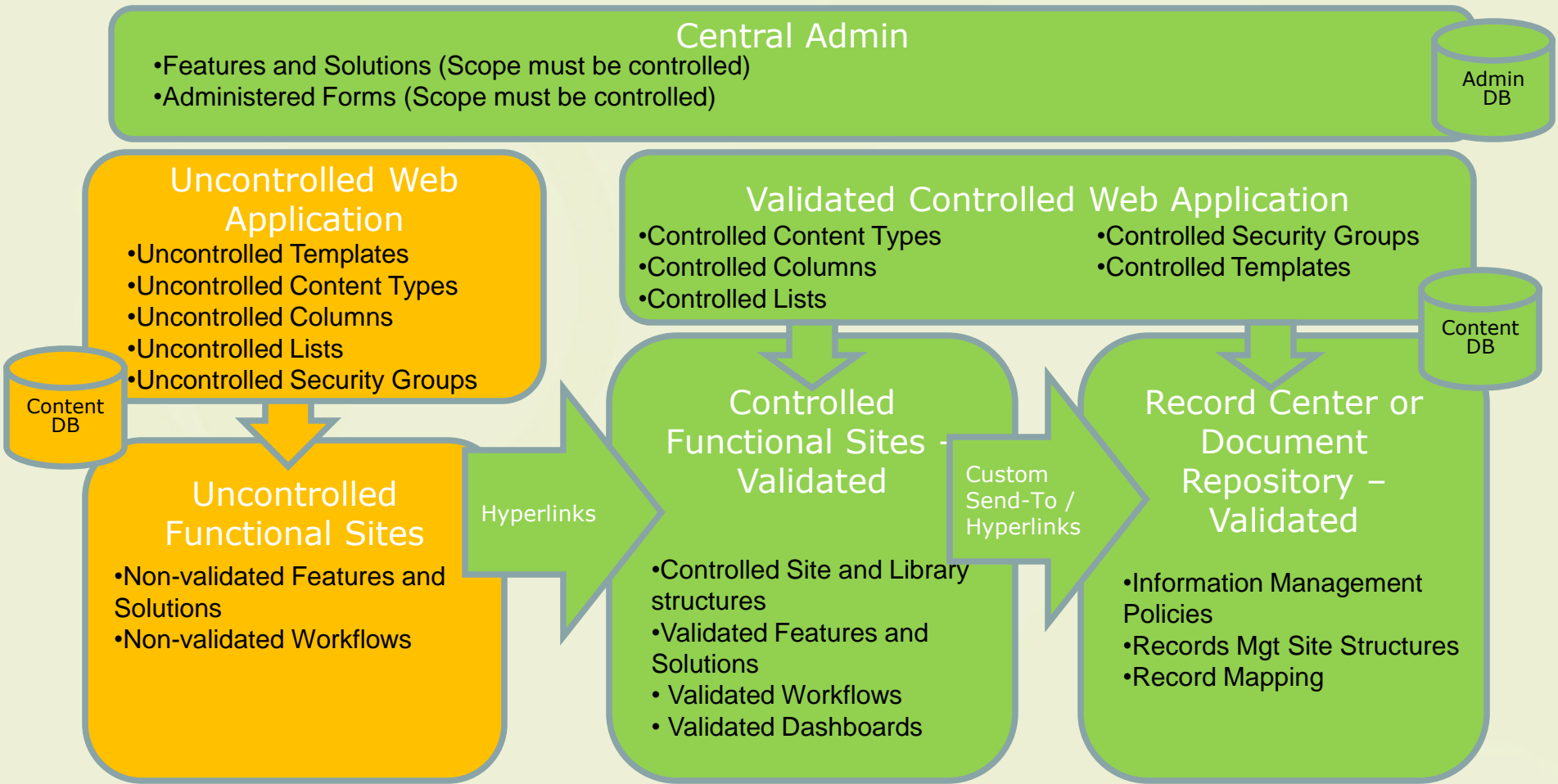


Controlled vs. Non-Controlled – Integrated Option

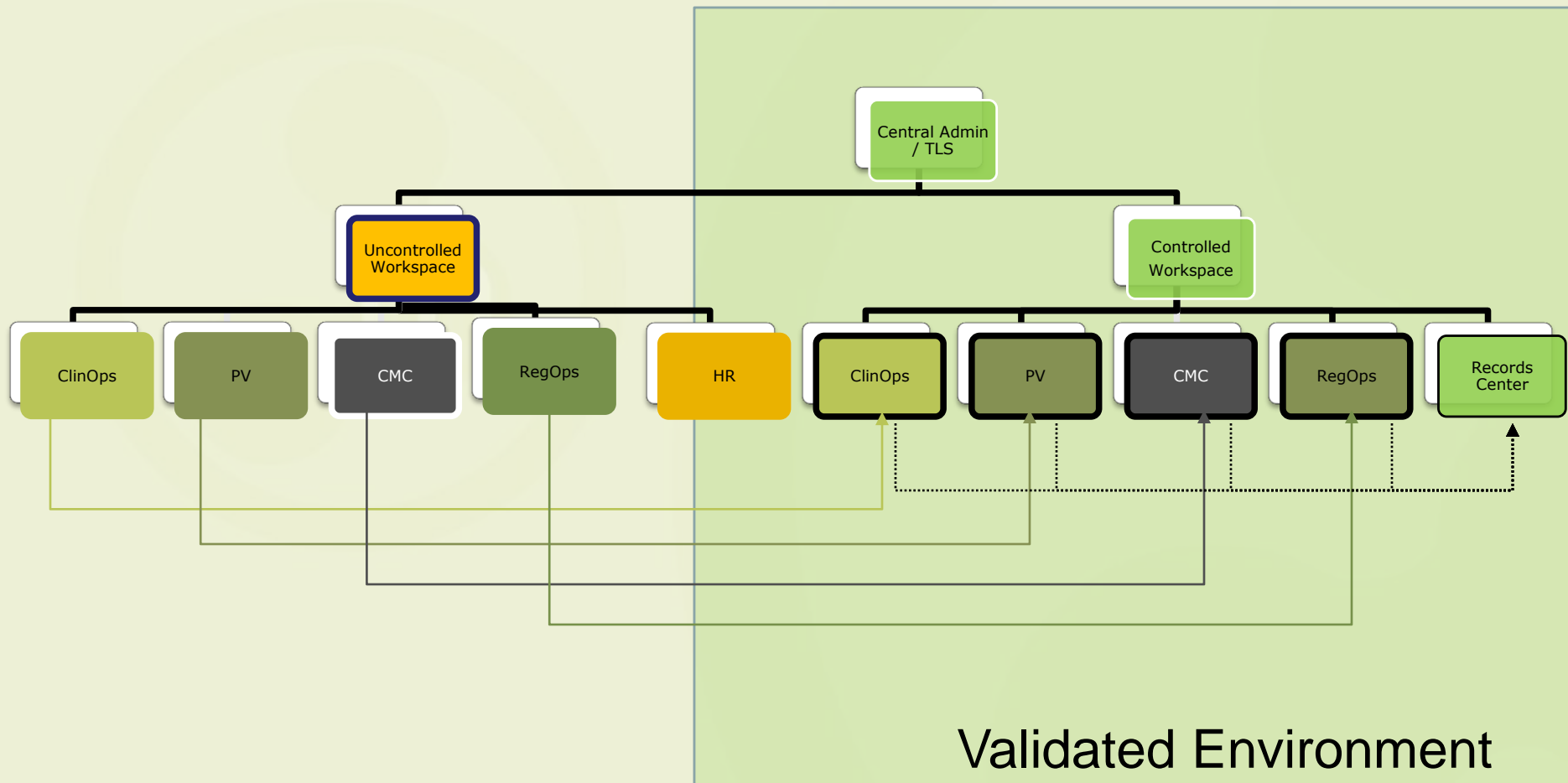




Controlled vs. Non-Controlled – Isolated Option



Example of Controlled and Non-Controlled Environment





Risk Evaluation and Scoping the Validation Strategy

- **Agencies** are actively **encouraging** the use of **risk based approaches** for the validation of computerized systems used in GxP environments
- The use of a risk based approach allows us to **focus** on **high risk** areas whilst **reducing** the **validation effort** and **improving quality**
- When **starting** the deployment of **MOSS in regulated environments**, it is important to evaluate risk so as to **focus validation efforts on high risk areas**
- Risk should be measured at two levels:
 - General **procedural** risk
 - Detailed **functional** risk

- **Risk** can be identified as either **regulatory** risk or **business** risk
- You should **clearly specify** that you intend to **adopt a risk based approach** in your validation plan and also **explain the rationale** behind the approach
- Ensure that **risk assessment** is carried out by a **knowledgeable team**
- **Be strict** as everything can end up being high-risk with enough debate....



Risk based approach 101 – Identify Scope

- **Step 1** - When defining the scope of your MOSS deployment clearly identify regulated procedures and records that will be generated or managed by the system

MOSS Examples:

1. MOSS will be used to generate submission ready electronic PDF records that will be submitted to FDA as part of our INDs
2. MOSS will be used to control the drug shipment authorization process for clinical sites
3. MOSS will be used to generate CAPA records for our GMP facility
4. MOSS will be used to manage audit report observations

IMPORTANT: If MOSS will not be used for processes or records that are governed by predicate rules...there is no regulatory requirement to validate!



Risk based approach 101 – Risk Type / GxP Determination

- **Step 2** - Associate a type of risk (regulatory or business) to each record or process based on the following criteria:
 - A. Is the record or procedure governed or required by predicate rule?
 - B. Does the procedure or record have an impact on subject safety?
 - C. Does the procedure or record have an impact of product quality?
 - D. Does the procedure or record have an impact on data integrity?
 - E. Does the procedure or record have a important impact on our ability to carry out the daily tasks of our business?

MOSS Examples:

1. MOSS will be used to generate submission ready electronic PDF records that will be submitted to FDA as part of our INDs – **Regulatory risk (A)**
2. MOSS will be used to control the drug shipment authorization process for clinical sites – **Regulatory Risk (B)**
3. MOSS will be used to generate CAPA records for our GMP facility – **Regulatory Risk (C)**
4. MOSS will be used to manage audit report observations – **Regulatory and Business Risk (A-E)**

IMPORTANT: If a procedure or record has no regulatory risk associated, it may be excluded from the validation effort provided that adequate rationale is provided

- **Step 3** – Define risk scenarios for each process or record identified. Scenarios should include:
 - Potential risk
 - Likelihood of occurrence/detection
 - Impact
 - Palliative actions

MOSS Example:

1. MOSS will be used to control the drug shipment authorization process for clinical sites –
Regulatory Risk (B)

Risk Scenario A:

- *Risk: IRB approval has not been received and a subject is enrolled in study and treated*
- *Likelihood: Medium – Due to combination of procedural and system controls*
- *Impact: High – Treating subjects without IRB approval considered a serious deviation*
- *Palliative Action: Ensure that drug cannot be shipped to site before IRB approval has been received through system and procedural controls*



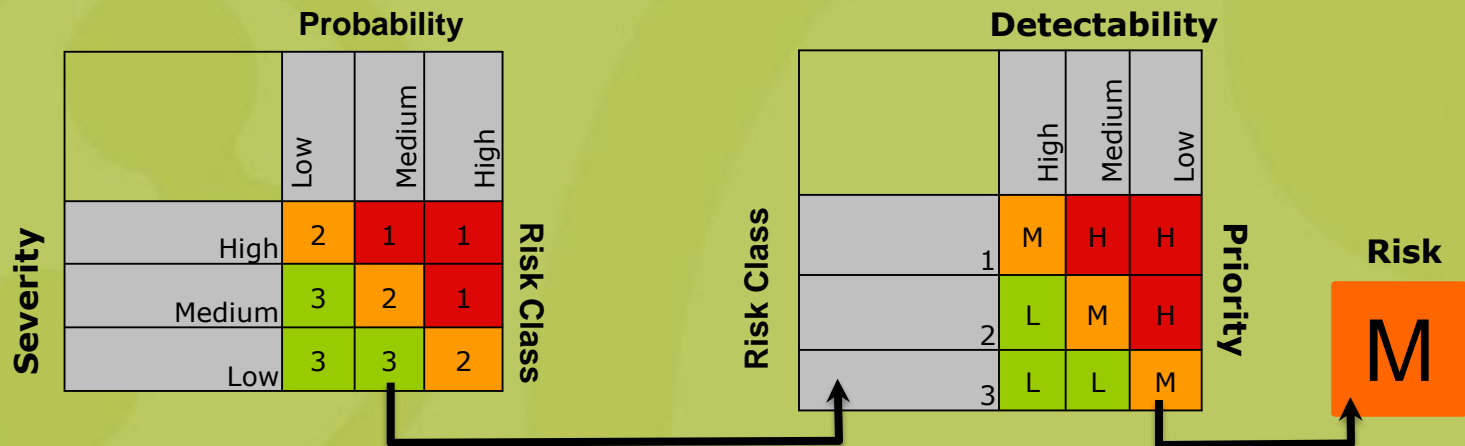
Risk based approach 101 – Link System Functions to Scope

- **Step 4** – Once processes and records have been classified by procedural risk, they must be linked to the system functionality defined in the user requirements specification (URS):

MOSS Example:

Process / Record	URS ID	Requirement
MOSS will be used to generate submission ready electronic PDF records that will be submitted to FDA as part of our INDs	UR3.1.	The system should allow the automatic generation of PDF v1.4. files
	UR3.2.	The system should allow the electronic signature of records
	UR3.3.	The system should be able to invalidate electronic signatures if the signed record is modified
	UR3.4.	The system should manage the version number of records
	UR3.5.	The system should be capable of rendering final records read-only

Risk based approach 101 – GAMP Risk Evaluation method



Severity = Impact on Patient Safety, Product Quality or Data Integrity

Probability = Likelihood of fault occurring

Risk Class = Severity x Probability

Detectability = Likelihood that the fault is detected before harm occurs

Priority = Risk Class x Detectability

- **Step 5** – Based on the type of system and the high level risk assessment we must decide on what level of risk must be tested for during validation
 - Custom built systems or components tend to present a higher level of risk than OTS systems
 - It may be appropriate to exclude business risk from testing
 - The validation plan should specify the acceptable risk levels with rationale

MOSS Example:

1. All OTS MOSS functions that have a risk rating of low or medium will not be formally tested during validation. These functions are deemed to be adequately tested by the vendor.
2. All custom applications deployed within the MOSS environment that have GxP impact and a risk rating of medium or high will be formally tested during validation. Low risk functions and functions that do not have GxP impact will be informally verified during the build phase.



Risk based approach 101 – Evaluate System Functions

- **Step 6** – Once processes and records have been linked to system functions, a risk evaluation of each function involved is undertaken:

MOSS Example:

Process / Record	URS ID	Requirement	Risk Scenario	Severity / Probability / Detectability Low (L), Medium (M), High (H)	Test Y/N
MOSS will be used to generate submission ready electronic PDF records that will be submitted to FDA as part of our INDs	UR3.1	The system should allow the automatic generation of PDF v1.4. files	PDF Files are generated in the incorrect format	M L H	No L
	UR3.2	The system should allow the electronic signature of records	Record cannot be signed	L M H	No L
	UR3.3	The system should be able to invalidate electronic signatures if the signed record is modified	Signature remains valid after record modification	H M L	Yes H

- The **result** of the functional risk assessment provides us with the **foundation** for the various **tests** that we should execute against the installed MOSS environment
- The **same methodology** should be applied when performing **change control**
- Risk assessment should be **reviewed** by the **system stake holders** and **QA** for completeness before moving on to the next step of validation

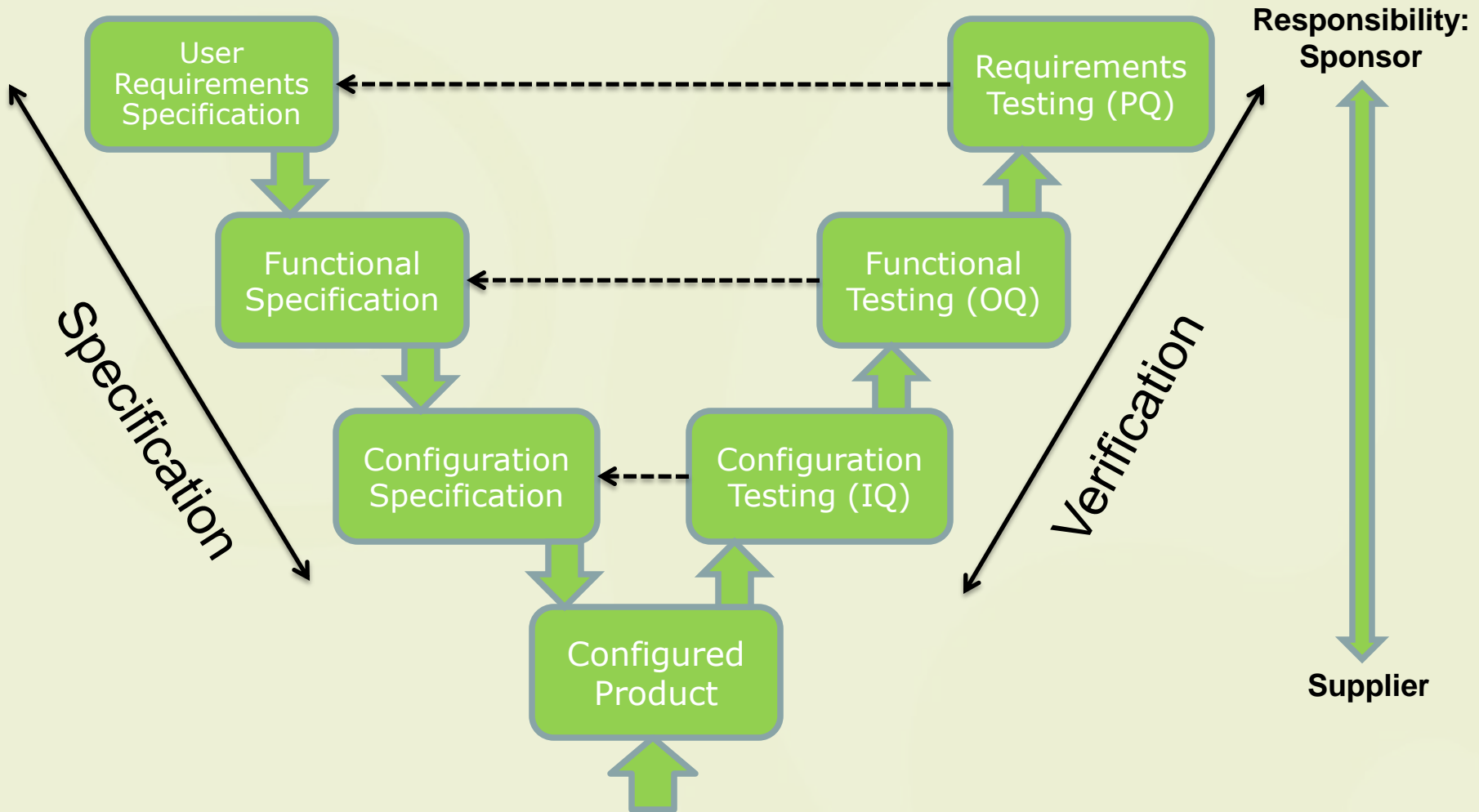


Step by Step CSV Model

- **GAMP5** is a standard that was established by **ISPE**
- The standard provides a framework for achieving **compliant GxP computerized systems**
- This standard is widely **recognized** and **understood** by **industry**
- GAMP provides **guidance** for the **validation** of different **categories** of systems
- **MOSS** would be considered a **Configured Off the Shelf** system within the context of GAMP
- It is **expected** that these systems have already **undergone significant validation** during development by the **vendor**
- Configured **off the shelf systems** require **less validation** effort than customized systems



GAMP5 – CSV Framework for a Configured Product



- **Governs** the validation process for a system
- Outlines:
 - Roles and responsibilities
 - Validation approach and risk rationale
 - System scope and pre-requisite requirements
 - Documentation deliverables for the system
- The plan should be **high level** and **flexible** whilst clearly specifying what is **required** to **achieve compliance**
- If MOSS is to be deployed in a controlled and non-controlled configuration, the **plan** should clearly state that **only the controlled environment will be validated**



CSV Documents – User Requirements Specification

- Document that defines:
 - business (end user) requirements
 - functional requirements
 - performance requirements
 - regulatory requirements (including 21 CFR Part 11 requirements)
 - system architecture and security requirements
- Requirements should be **precise** and **measurable**
- Used as the **basis** for developing **test scripts**
- Try to **prioritize** requirements (Must, Should, Want)
- Try and minimize requirements and **avoid stating the obvious** for known OTS systems such as MOSS

- It is **strongly recommended** that a traceability matrix is maintained throughout the **lifetime of the system**
- The trace matrix:
 - **Links** test scripts to user and functional requirements
 - Ensures that all requirements are **adequately tested**
 - **Indicates** the **risk** classification for each testable requirement
 - Should be considered a **living document** and therefore versioned and updated during change control



CSV Documents – Functional Specification

- Functional specifications allow us to describe **how system functions** will meet user requirements
- The functional specification clearly describes:
 - The purpose of each function
 - The inputs
 - The process
 - The outputs
- Functional specifications are **not required** for the installation and configuration of **baseline MOSS**
- Functional specifications **should** be developed for:
 - Validated InfoPath forms
 - Validated workflows
 - Custom web parts, features and solutions
 - Integration with any third party applications or services

- The configuration specification clearly documents:
 - The **baseline MOSS parameters** and **architecture** required for installation of the product and any 3rd party add-ons
 - The structure of the controlled environment, notably:
 - Site and library settings
 - Libraries
 - Content types
 - Columns
 - Security groups and user rights
 - Template and workflow deployment
- The specification can be versioned and used to **document** the **execution** of the configuration in MOSS
- The specification should be **updated** each time changes are required through **change control**

- Ensures that all **software modules** are **installed correctly**
- Lists **step by step process** for the installation and configuration of all software modules
- Defines **expected results** at each **control point** of the installation
- Ensures that all **documentation** is in place and that the system is adequately **protected**
- Ensures proper **verification** of the **structural** elements i.e. sites, content types etc.
- It is recommended to develop an IQ **protocol** which governs the overall **installation** and **configuration** process
- Develop **IQ scripts** for the installation of **baseline MOSS** and **3rd party add-ons** in all validated environments
- Develop **IQ scripts** for the execution of the **configuration specification** for structural MOSS elements

- Consists of **end to end positive and negative testing** that all system components i.e. hardware and software are **operating as intended**
- Tests are executed on **base functionality** by end users and IT
- Tests are governed by a **test protocol** which clearly describes the test and deviation management **procedures** that must be followed
- Tests should be broken down into test scripts by **functional area**, linked to baseline system functions, and be **approved before execution**
- All test results should be clearly documented using good documentation practices (**ALCOA**)
- Tests serve as a **mechanism** to **verify** that the system is operating correctly in its **installed environment**

- Requirements testing consists of **positive testing** of business specific configuration and **user requirements**
- Tests are executed on business specific functionality such as **workflows** or **InfoPath forms** that were identified as being testable during the risk assessment exercise
- Tests are governed by a test protocol which clearly describes the test and deviation management procedures that must be followed
- Tests should be broken down into **test scripts** by **process** and be linked to user and functional requirements, and be approved before execution
- All test results should be clearly documented using good documentation practices (**ALCOA**)
- Tests are typically executed by end users and serve as a **user acceptance mechanism**

- Describes **how** the **validation went**, verifies that all deviations are closed, and provides for the final approval of the CSV document package to allow the system to go into production
- **Individual** summary reports for each step of the verification process **or** a **comprehensive** report covering all steps may be produced
- The summary report should clearly show that the validation plan and protocols were followed and that the **acceptance criteria** for putting the **system** into **production** have been met

- Configuration control should be governed by a **formal MOSS specific procedure** in addition to any general provisions of the IT Configuration control SOP
- This procedure should **govern** the update of the **configuration specification**
- The configuration specification should be used to clearly **document** updates / additions to MOSS
- Any changes to the validated controlled environment must also be documented using **change control**
- Should **significant** changes or additions be made, a **new validation** project may be required
- For **workflows, forms or features/solutions** it is imperative to correctly evaluate **impact** and **risk** and produce **adequate test scripts** properly integrate the additional elements into the current environment



Maximizing quality and ROI

- Validation can be **expensive** and **time consuming** if it is not done correctly
- By defining a **clear validation strategy** and by leveraging risk assessment techniques, we are able to focus the validation effort on what is really important
- Consider **acquiring tried and tested test scripts** and/or validation packages for MOSS / third party add-ons so as to **reduce** the amount of preparation **time** and improve quality
- Make sure that all **individuals** involved in the validation effort are fully **trained** and understand the CSV process
- **Isolated** controlled environments **facilitate** validation and configuration control
- Use **virtual environments** so as to facilitate **replication** between production and test environments



Lessons learned and best practices

- Create a '**Big Picture**' of your MOSS deployment so as to ensure that you are able to adequately accommodate all of your controlled and non-controlled needs
- Use a **risk based approach** to focus and reduce validation efforts – be strict otherwise everything becomes high risk...
- Remember that **MOSS** is an **off-the-shelf product** and that you should limit validation scope to high risk business and regulatory requirements as much as possible
- Establish a MOSS **validation team** to oversee and manage the validation process and changes to the controlled MOSS environment
- Implement **SOPs** and **WIs** which clearly define how the environment is configured and administered and which level of documentation / re-validation is required by type of change
- Use a **step by step** deployment methodology to keep things manageable



montrium

It is easy to drown
in the details....
Try and keep it
SIMPLE!





What's next...

- Montrium will present the second webinar in its SharePoint for Pharma series on Configuration Control of SharePoint in Regulated Environments on Friday May 7th 2010 at 11am EST
- This webinar will cover:
 - Implementation of formal system specific configuration control procedures
 - Importance of defining clear taxonomies and standards across the enterprise
 - Configuration deployment and version control techniques
 - Integration with the validation and change control process
 - Importance of leveraging a risk based approach to QC
 - Using SharePoint to manage configuration control

We look forward to seeing you there!



Contact Details

Paul Fenton
Montrium Inc.

361 St-Joseph West,
Montreal (QC) H2V 2P1
Canada

Tel. 514-223-9153 ext. 206

pfenton@montrium.com

www.montrium.com

You can also find me on LinkedIn...