

Risk based approach to electronic document management system (EDMS) validation

Presented by:

Michael Zwetkow, VP Operations

Montrium, Inc

The views and opinions expressed in the following PowerPoint slides are those of the individual presenter and should not be attributed to Drug Information Association, Inc. (“DIA”), its directors, officers, employees, volunteers, members, chapters, councils, Special Interest Area Communities or affiliates, or any organization with which the presenter is employed or affiliated.

These PowerPoint slides are the intellectual property of the individual presenter and are protected under the copyright laws of the United States of America and other countries. Used by permission. All rights reserved. Drug Information Association, DIA and DIA logo are registered trademarks or trademarks of Drug Information Association Inc. All other trademarks are the property of their respective owners.

- Overview of a risk based approach for validating an EDMS
- Identify regulatory requirements which apply to an EDMS
- Discuss high risk system functionality which must be validated
- Practical Example
- Good practices for maintaining a validated state via configuration and change control

Why use a Risk Based Approach?

1. Focus validation effort



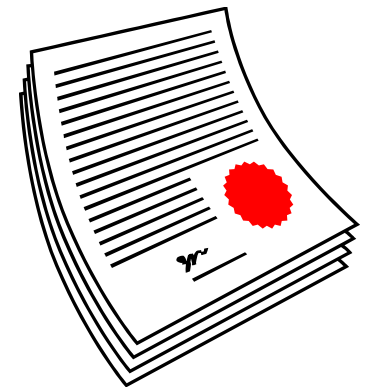
2. Reduce time to implementation



3. Reduce cost



- Documented evidence which demonstrates:
 - systems consistently operate as intended
 - business and regulatory system requirements are met
 - information is secure and properly managed
 - procedures and processes are in place for the use and management of the system



- **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)

- **PIC/S Annex 11**

Validation should be considered as part of the complete life cycle of a computer system. This cycle includes the stages of planning, specification, programming, testing, commissioning, documentation, operation, monitoring and changing.



- Controls/procedures in place to validate system
- Individuals involved in CSV have adequate experience and training
- Level of testing based on system risk, complexity, and novelty
- Change/Configuration Control to maintain system validated state

- Initial system level
- Component level
 - Hazard and Operability Analysis (HAZOP)
 - Failure Mode and Effects Analysis (FMEA)
 - Fault Tree Analysis (FTA)
 - Etc.
- Supplier Audit/Assessment



System Type - **Configured OTS or Custom?**

Identify intended use of the system

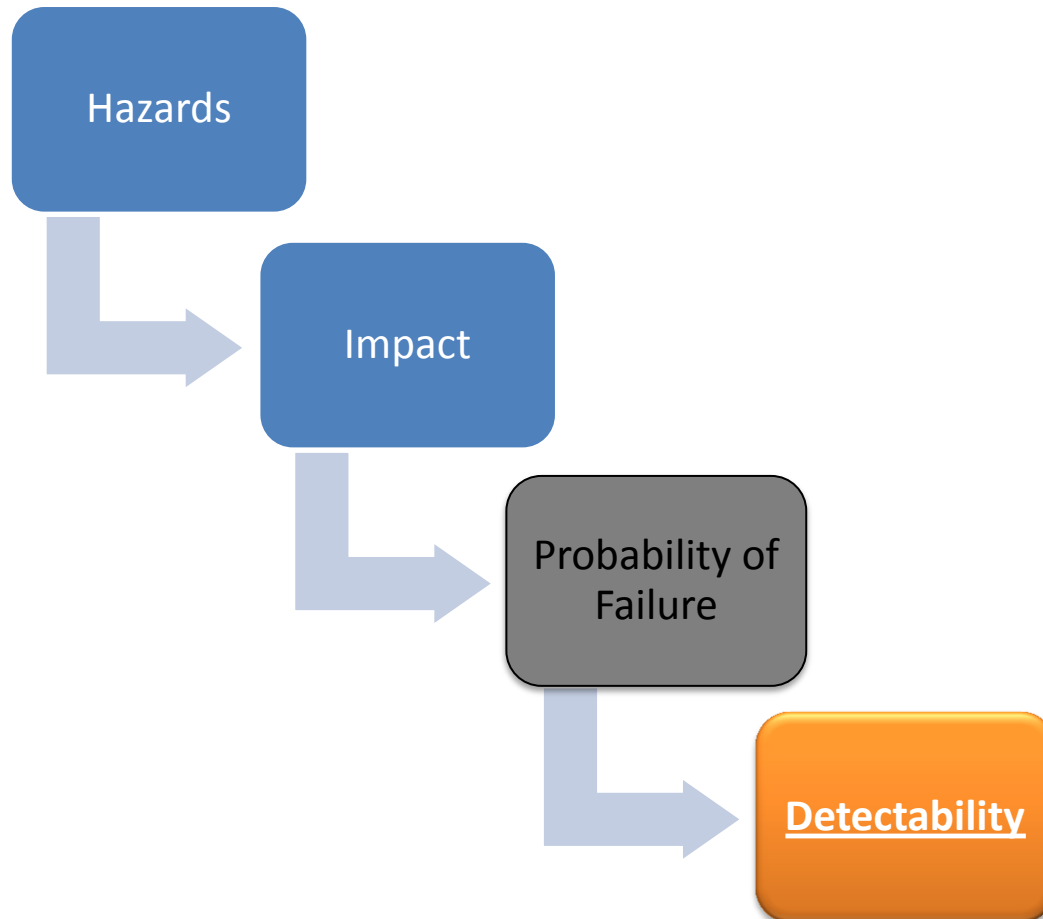
Determine which regulations apply based on the intended use

Identify and define GxP electronic records and signatures, based on the predicate rules

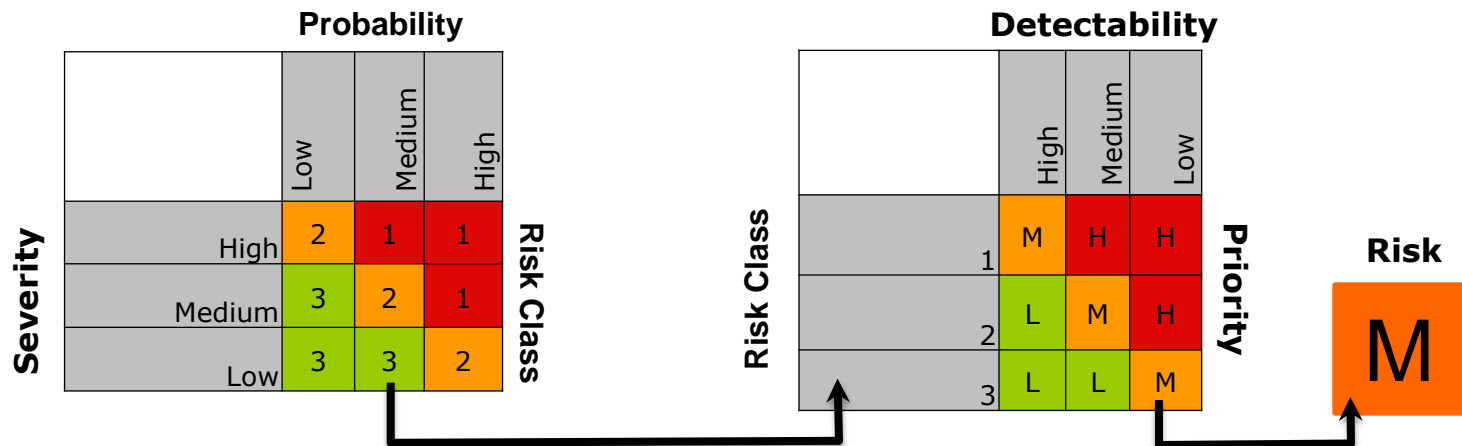
Identify the areas of the system that must be validated

- The definition of an electronic record
- Audit trails
- Electronic copies of records for inspection
- Retention and maintenance of records
- Hybrid and procedural solutions
- Application of electronic signatures

- Within the context of an EDMS electronic records could be in the form of:
 - **Documents & Forms** required to be maintained by predicate rule
 - **Metadata** used to perform regulated activities (or make regulated decisions)
 - **Electronic / Digital Signatures** used to sign records required by predicate rules
 - **Audit Trails** generated for electronic records being generated and/or managed in the EDMS



Note: Must be detected before the consequences of the failure cause harm



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

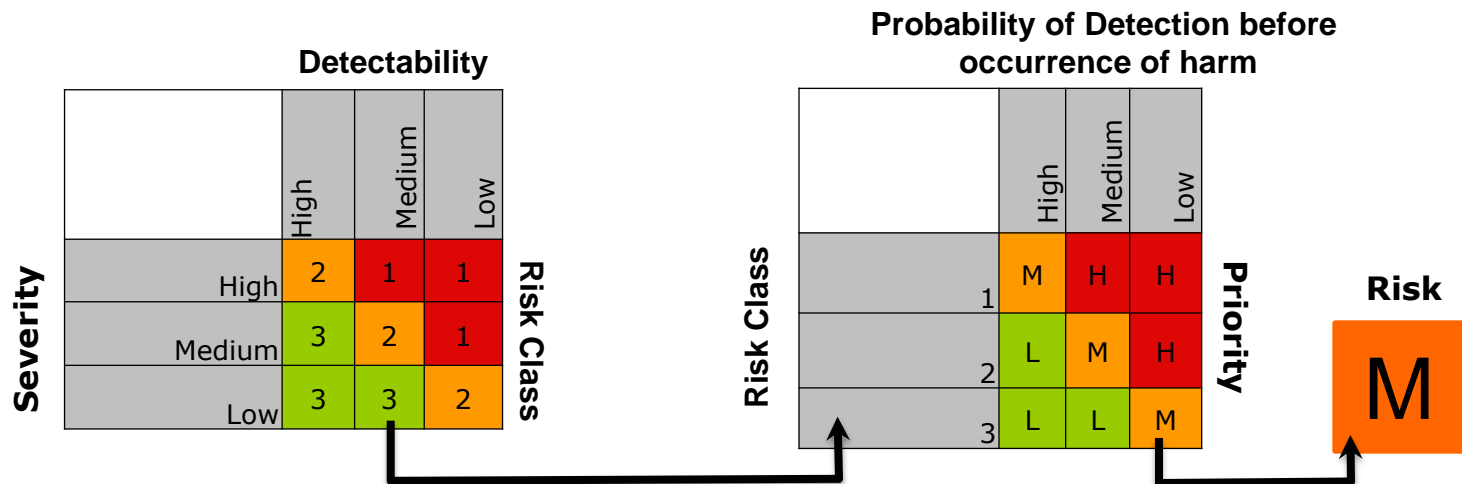
Probability = Likelihood of fault occurring

Risk Class = Severity x Probability

Detectability = Likelihood that the fault is detected

Priority = Risk Class x Detectability

Recommended Risk Evaluation Method for EDMS



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

Detectability = How easily can fault be detected

Risk Class = Severity x Detectability

Probability = Likelihood that the fault is detected before the occurrence of harm

Priority = Risk Class x Probability

Step 1

- Perform Initial Risk Assessment and Determine System Impact

Step 2

- Identify Functions with Impact on Patient Safety, Product Quality and Data Integrity

Step 3

- Perform Functional Assessments and Identify Controls

Step 4

- Implement and Verify Appropriate Controls

Step 5

- Review Risks and Monitor Controls

- The OTS EDMS will be used to:
 - Generate submission ready electronic PDF records that will be submitted to FDA as part of our INDs
 - Manage CAPA process and CAPA records
 - Manage Document Change Request process for controlled documents (i.e. SOPs, Policies, Validation Documents etc.)
- System Impact
 - Regulatory: Functions with regulatory impact will be validated
 - Business: Functions with business impact will not be validated (since it is an OTS and Vendor Assessment has been performed)

- Example (EDMS Functional Requirements with impact on Data Integrity)
 1. The system must be able convert the Final Draft Word document to a PDF format which will be submitted for approval
 2. The system must copy the metadata from the Word document to the PDF copy

Step 3 - Perform Functional Assessments and Identify Controls

Function	Risk scenario	Regulatory Impact	Detectability	Probability of Detection	Risk Priority	Validation Required?
Controlled Document Review workflow calls a web service which sends the Word document to the PDF Rendering Server, which returns the PDF and saves it in the Controlled Documents library.	The web service fails to send the document to the PDF Rendering server and the PDF is not generated	Medium	High	High	Low	No
	The web service incorrectly renders the PDF and generates a inexact copy of the Word document.	High	Medium	High	Medium	Yes

- Risks can be mitigated by implementing procedural or technical controls
 - The following standard operating should be in place to mitigate procedure risks:
 - Documentation Management SOP
 - Computer System Validation SOP
 - Backup SOP
 - Retention/Archiving SOP
 - Logical & Physical Security SOP
 - System Administration & Maintenance SOP
 - Training SOP
- Technical controls must be validated to demonstrate that the risk has been mitigated

- Periodic review of systems in order to:
 - verify that controls are still effective
 - previously unrecognized hazards are present
 - previously identified hazards are no longer applicable
 - the estimated risk level associated with a hazard is no longer acceptable

- Implement SOPs and WIs which clearly define how the environment is administered
- Configuration / Change Control SOP to manage changes
- Same risk based approach should be used during Change Control process
- Should significant changes or additions be made, a new validation project may be required

- Follow a stage risk assessment process
- Make to have SME from each business unit
- Make sure individuals involved in the risk assessment & validation have relevant experience
- Be strict otherwise everything becomes high risk...
- Leverage Vendor Audit & Vendor Testing