PRAXIS
life sciences

Risk-Based Approach to Software Quality and Validation

By Praxis Life Sciences

1925 West Field Court, Suite 125, Lake Forest, IL 60045
praxislifesciences.com | +1(847) 295-7160

Validation Center™
validationcenter.com

PRAXIS life sciences

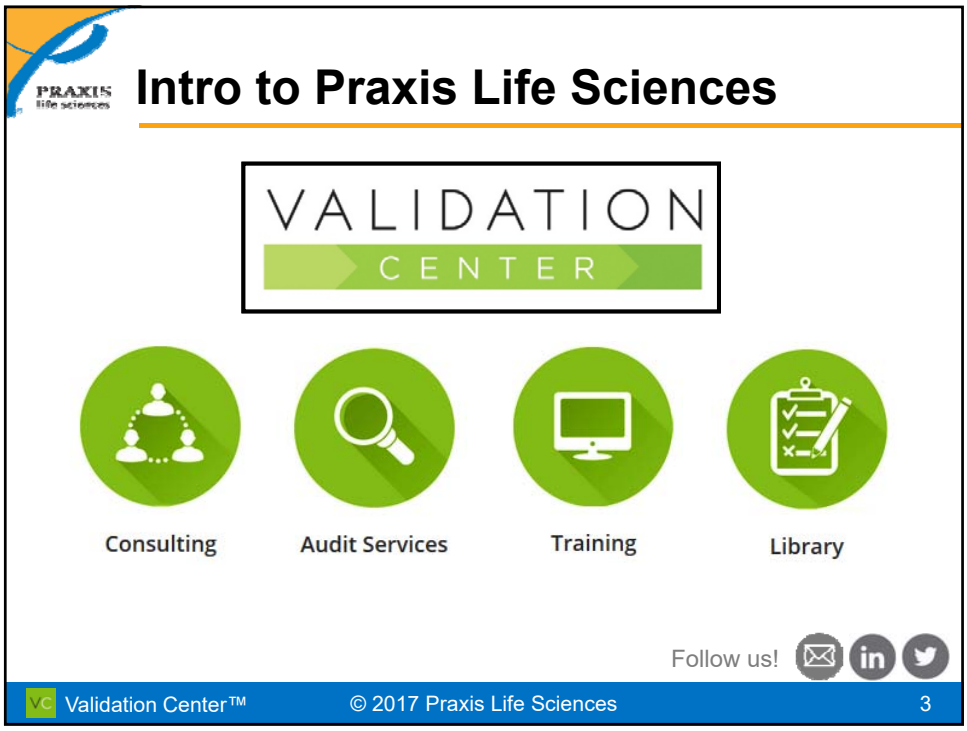
VALIDATION CENTER

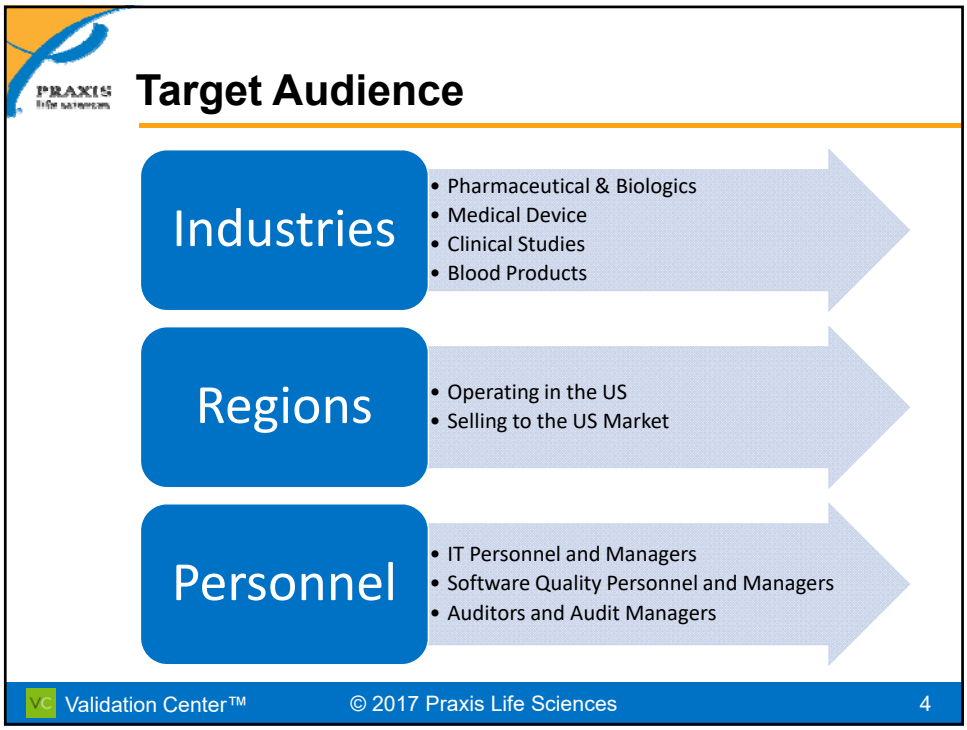
Risk Based Approach to Software Quality and Validation

V 17.05

Your Praxis Facilitator

- Debra Bartel, MBA, CQA, PMP
- Principal, Praxis Life Sciences
- 25+ years experience specializing in software quality assurance, validation and regulatory compliance, Information Systems project management, and process design.
- Prior to joining Praxis, held management positions in the pharmaceutical industry in both Quality Assurance and Information Systems organizations
- Active member of American Society for Quality (ASQ), Northeastern Illinois Section, Software Division





Have you ever heard…

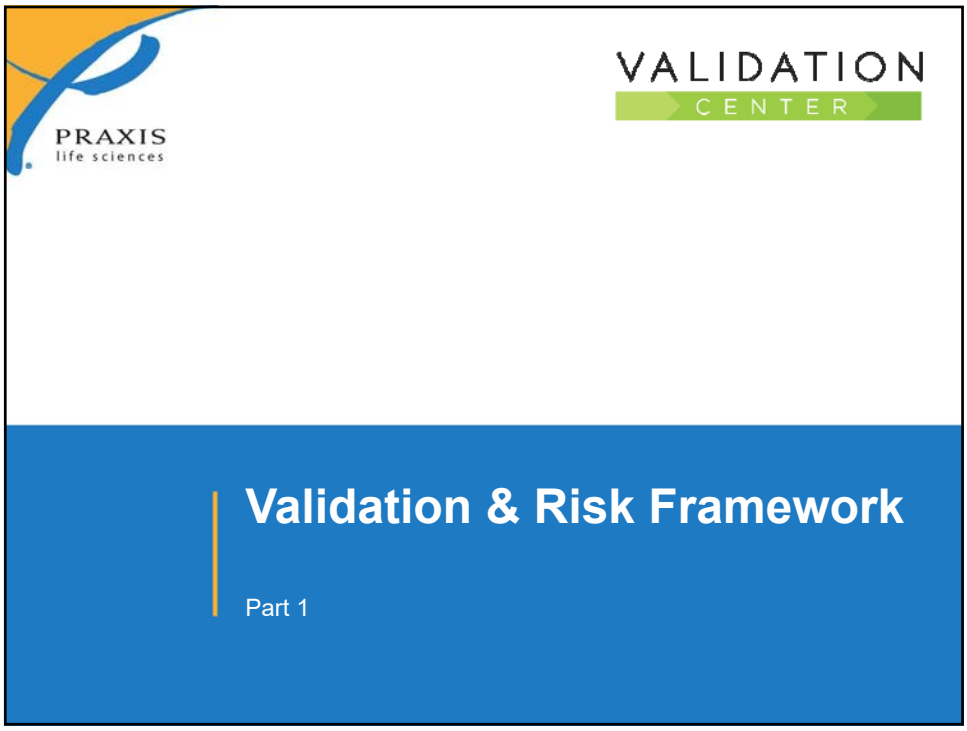
- Computer System Validation is a waste of time
- It's just a bunch of paperwork
- It doesn't find the bugs
- We just repeated everything the vendor already did

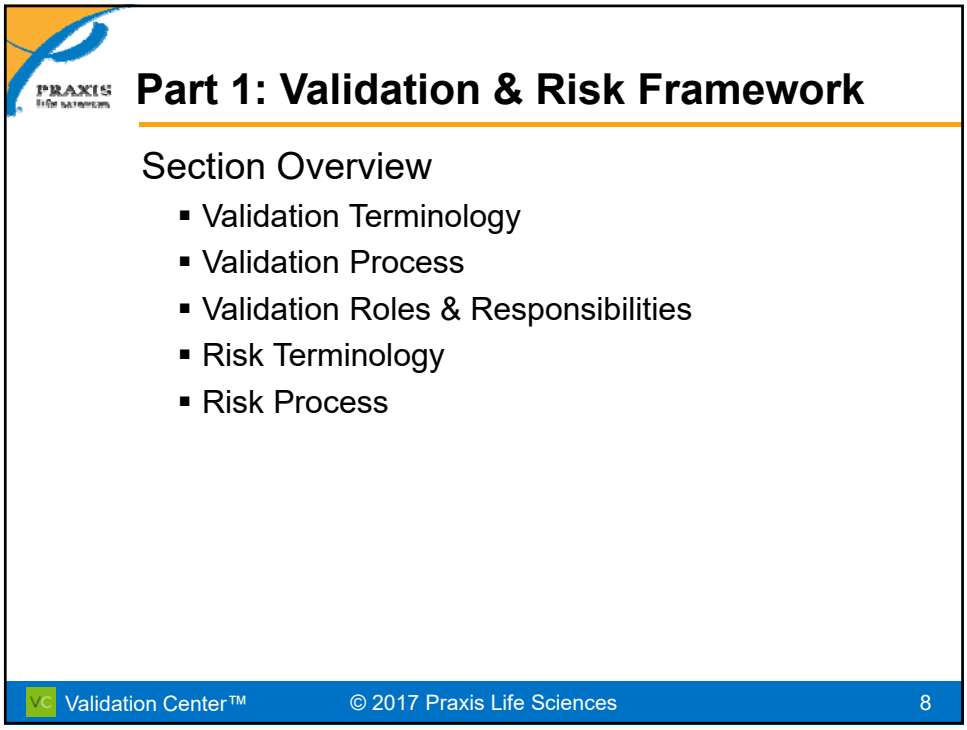
Validation Center™ © 2017 Praxis Life Sciences 5

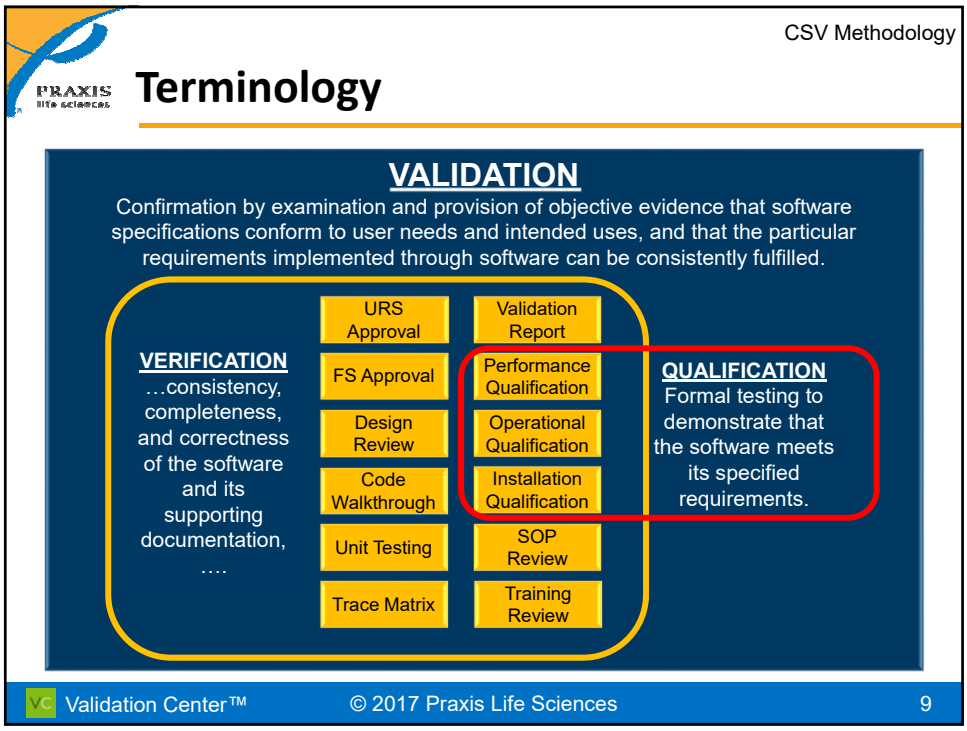
Webinar Outline

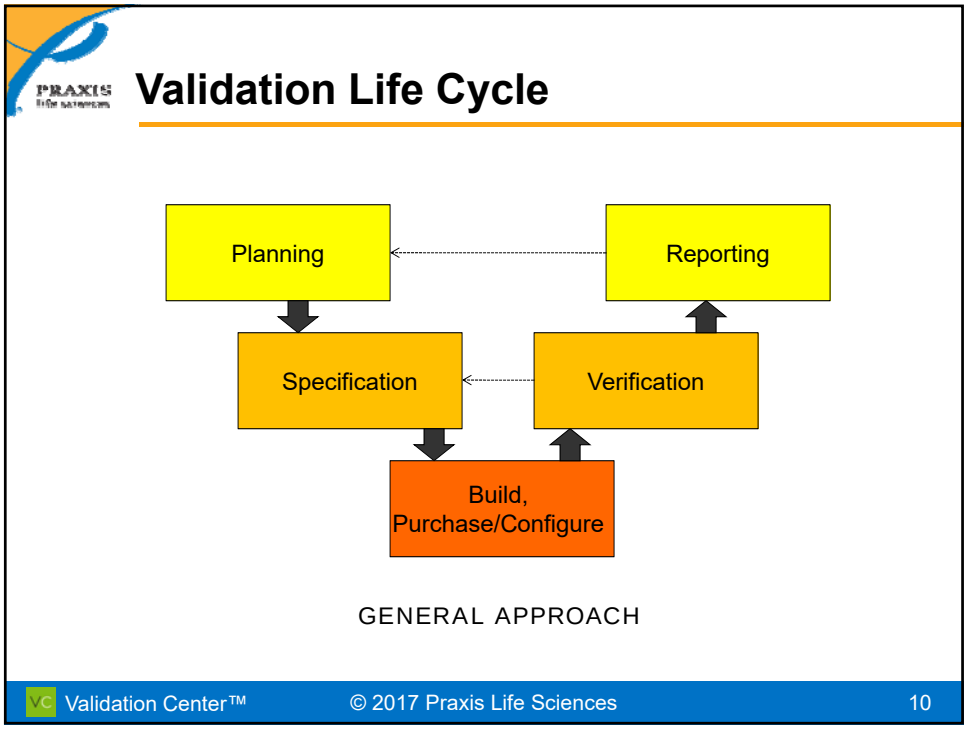
1. Validation & Risk Framework
2. External Guidance
3. Risk Assessment
4. Risk Mitigation
5. FDA Leadership by Example

Validation Center™ © 2017 Praxis Life Sciences 6

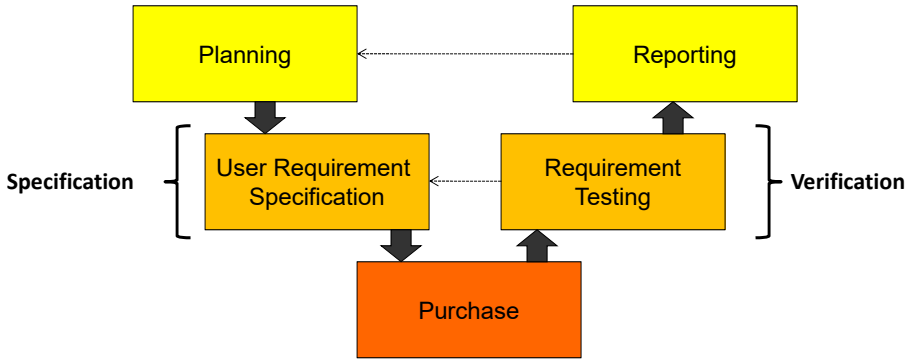








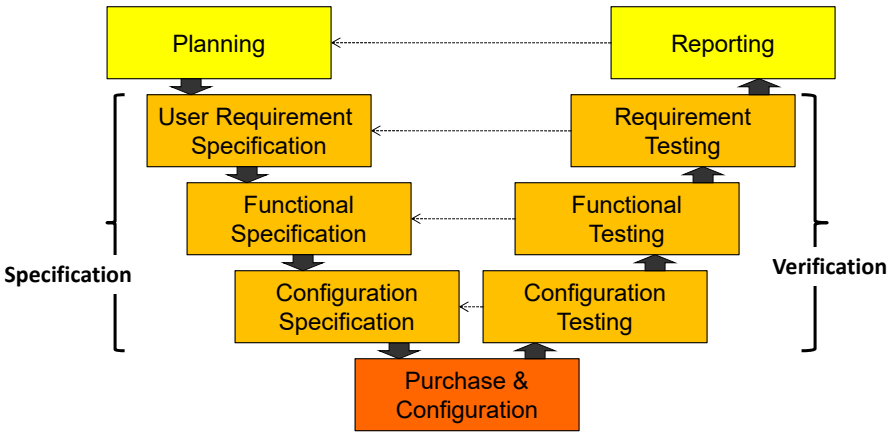
Validation Life Cycle



NON-CONFIGURED PRODUCT APPROACH

Validation Center™ © 2017 Praxis Life Sciences 11

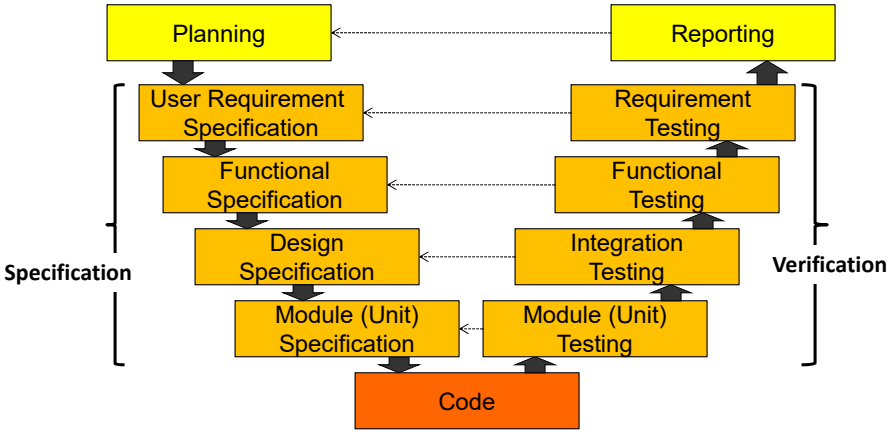
Validation Life Cycle



CONFIGURED PRODUCT APPROACH

Validation Center™ © 2017 Praxis Life Sciences 12

Validation Life Cycle



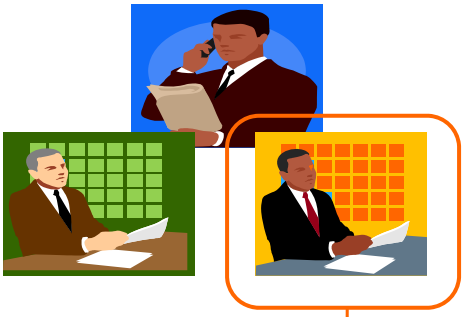
CUSTOM CODED PRODUCT APPROACH

Validation Roles

Business Process Owner

- **Manages the business process that uses the computer system**
- **Ensures that the system is appropriate for the business process**
- **Assigns Subject Matter Experts (SMEs) to participate in requirements definition and verification**

Validation Roles



- **Manages the implementation and support of the computer system**
- **Ensures that the system is available to support the business process**
- **Assigns technical experts to participate in all phases of the validation life cycle**

Validation Roles

- **Ensures that the computer system meets all internal standards**
- **Ensures that the computer system meets all applicable regulations**
- **Ensures that the computer system is ready for inspection**

Basic Risk Terminology

Hazard

A potential source of harm

Basic Risk Terminology

Hazard A potential source of harm

Risk

The combination of the probability of occurrence of a harm and the severity of the harm

Basic Risk Terminology

Hazard — A potential source of harm

Risk — Harm probability and severity

Risk Assessment

A comprehensive evaluation of risks and associated impacts

Basic Risk Terminology

Hazard — A potential source of harm

Risk — Harm probability and severity

Risk Assessment — Evaluation of risk and impact

Risk Mitigation

Actions taken to reduce the impacts of risks

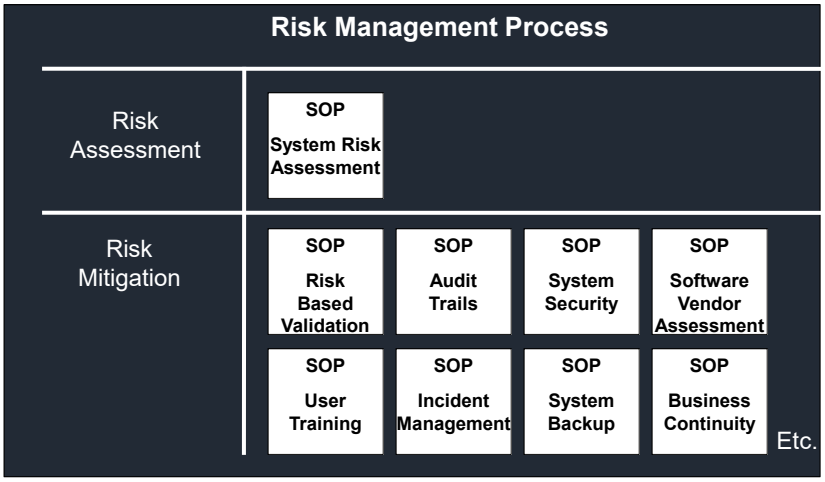
Basic Risk Terminology

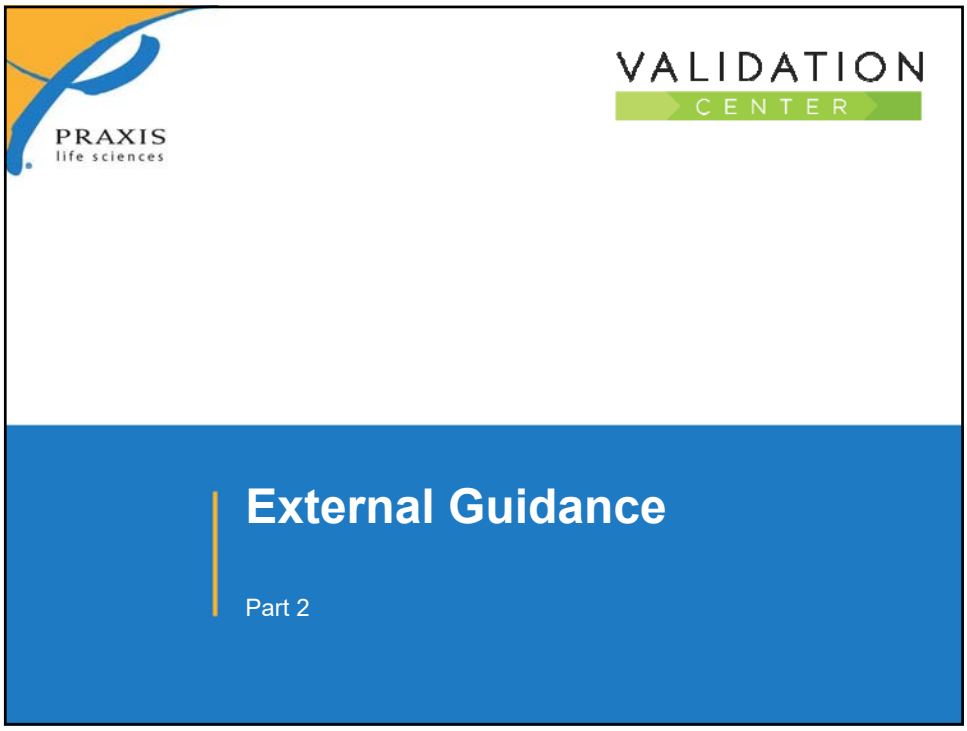
Hazard	A potential source of harm
Risk	Harm probability and severity
Risk Assessment	Evaluation of risk and impact
Risk Mitigation	Action to reduce impact

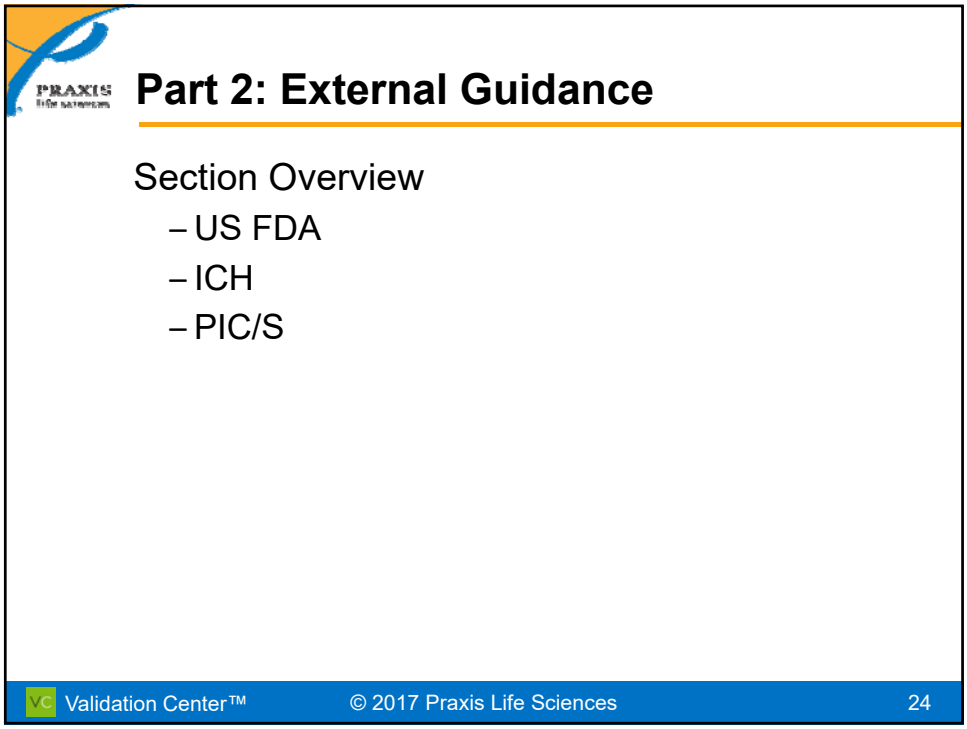
Risk Management

A systematic approach to assessment and mitigation of risks throughout the system life cycle

Risk Management Framework







USA

FDA *Glossary of Computerized System and Software Development Terminology*

Risk = A measure of the **probability** and **severity** of undesired effects. Often taken as the simple product of probability and consequence. (Source: IEEE)

Risk Assessment = A comprehensive evaluation of the **risk** and its associated impact. (Source: DOD).

FDA 21 CFR 820 *Quality System Regulation* (Medical Device GMP)

- Design validation shall include software validation and **risk analysis**, where appropriate.

FDA Guidance*: Off-The-Shelf Software Use in Medical Devices*

- Existing international standards indicate that the estimation of **risk** should be considered as the product of the **severity of harm** and the **probability of occurrence of harm**.
- It is more appropriate to manage **software safety risk** based on the **severity of harm** rather than the **software failure rates**

USA

FDA Guidance *General Principles of Software Validation*

Validation Planning: The quality plan should identify the role that risk (hazard) management will play.

Software Design: Software **design specification should include software risk analysis.**

Tracing: A software requirements traceability analysis should be conducted to trace software requirements to (and from) system requirements and the risk analysis results.

FDA Guidance *General Principles of Software Validation*

Validation Scope & Scale: Validation coverage should be based on the software's **complexity** and **safety risk**. The selection of validation activities should be commensurate with the **complexity** of the software design and the **risk** associated with use of the software for its specific intended use. As the **risk** increases, additional validation activities should be added to cover the additional **risk**

For **very low risk** applications, certain tasks might not be needed at all

USA

FDA Guidance *General Principles of Software Validation*

Testing
The amount of structural testing should be commensurate with the level of **risk** posed by the software. The amount of path coverage is normally established based on the **risk** or **criticality** of the software under test.

Validation Evidence
Document requirements and **risk analysis** of the automated process help to define the scope of the evidence needed to show that the software is validated for its intended use.

Off-the-shelf (OTS) Software
Depending upon the device **risk** involved, the device manufacturer should consider auditing the vendor's design and development methodologies used in the construction of the OTS software and should assess the development and validation documentation generated for the OTS software.

Validation Center™ © 2017 Praxis Life Sciences 27

USA

FDA Guidance *Part 11, Electronic Records; Electronic Signatures – Scope and Application*

General Approach to Part 11: We [FDA] recommend that you base your approach [to part 11] on a justified and **documented risk assessment** and a determination of the potential of the system to impact product quality and safety, and record integrity.

For instance, validation would not be important for a word processor used only to generate SOPs

FDA Guidance *Part 11, Electronic Records; Electronic Signatures – Scope and Application*

Audit Trails: We recommend that you base your decision on whether or not to apply audit trails, or other appropriate measures, on the need to apply with predicate rule requirements, a justified and **documented risk assessment**, and a determination of the potential effect on product quality and safety, and record integrity.

Record Maintenance: We suggest that your decision on how to maintain records be based on predicate rule requirements and that you base your decision on a justified and **documented risk assessment** and a determination of the value of the records over time.

Validation Center™ © 2017 Praxis Life Sciences 28

USA

FDA Guidance *Computerized Systems Used in Clinical Investigations*

Security
We [FDA] recommend that passwords or other access keys be changed at established intervals commensurate with a **documented risk assessment**

Audit Trails
The need for audit trails should be determined based on a justified and documented **risk assessment** that takes into consideration circumstances surrounding system use, the likelihood that information might be compromised, and any system vulnerabilities

Validation of Changes
The effects of changes to the system should be evaluated, and some should be validated depending on **risk**

ICH

ICH Q9, *Quality Risk Management*

Risk assessment consists of the identification of hazards and the analysis and evaluation of **risk**s associated with exposure to those hazards.

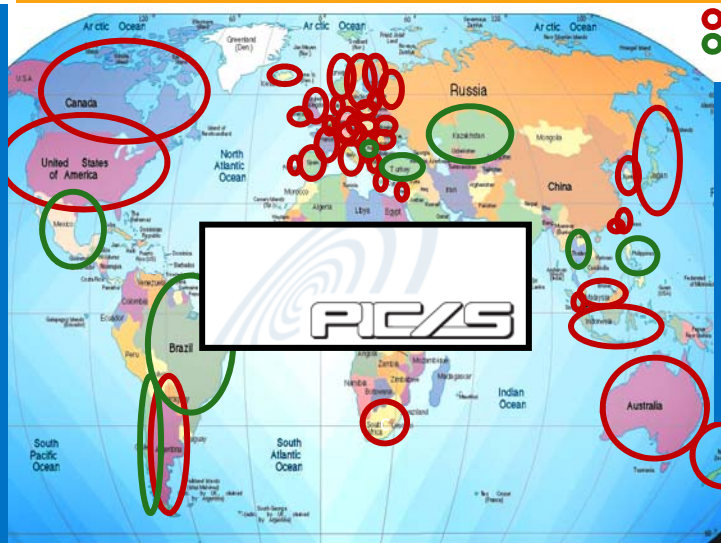
Three fundamental questions:
1. What might go wrong?
2. What is the likelihood (probability) it will go wrong?
3. What are the consequences (severity)?

Potential Areas of Use:
A. To select the design of computer hardware and software

B. To determine the extent of validation, e.g.,
- identification of critical performance parameters
- selection of the requirements and design
- code review
- the extent of testing and test methods
- reliability of electronic records and signatures.

PIC/S

Argentina
Australia
Austria
Belgium
Canada
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland
Indonesia
Ireland
Israel
Italy
Japan
Korea
Latvia
Liechtenstein
Lithuania
Malaysia
Malta
Netherlands



Continued
New Zealand
Norway
Poland
Portugal
Romania
Singapore
Slovak Republic
Slovenia
South Africa
Spain
Sweden
Switzerland
Taiwan
Ukraine
United Kingdom
USA

Validation Center™ © 2017 Praxis Life Sciences 31

PIC/S

Argentina
Australia
Austria
Belgium
Canada
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland
Indonesia
Ireland
Israel
Italy
Japan
Korea
Latvia
Liechtenstein
Lithuania
Malaysia
Malta
Netherlands
New Zealand

PIC/S PI 011 ***Good Practices for Computerised Systems Used in Regulated "GXP" Environments***

Risk Assessment

Regulated users should be able to justify and defend their standards, protocols, acceptance criteria, procedures, and records in the light of their own **documented risk and complexity assessments.**

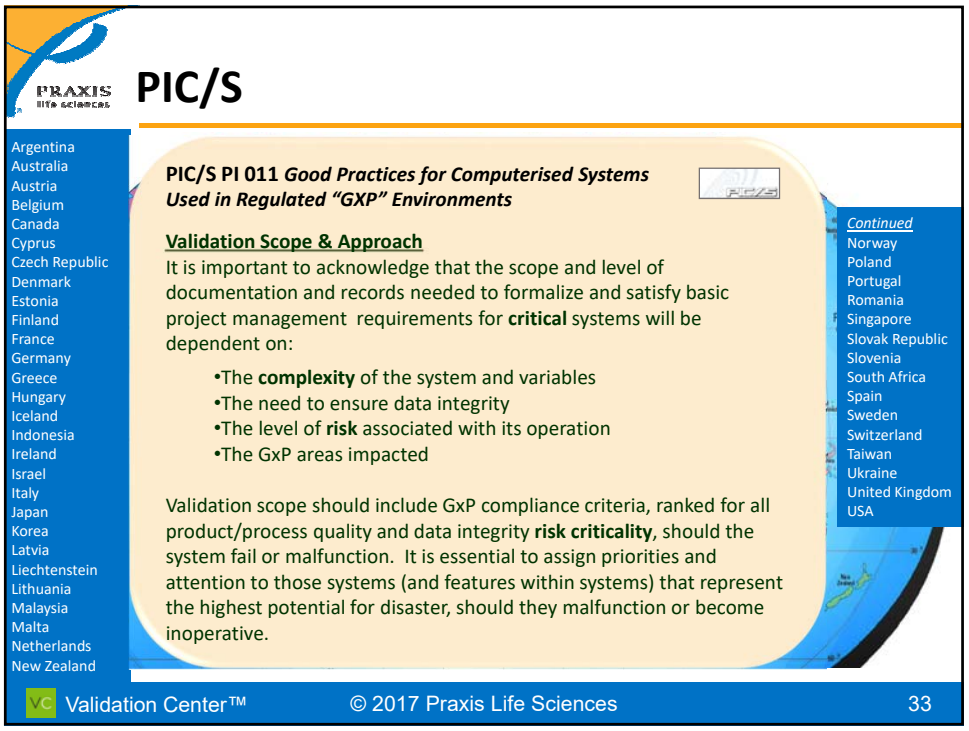
The risk assessment and the results including the reasons for the ranking as either: 'critical' or 'not critical' should be documented.

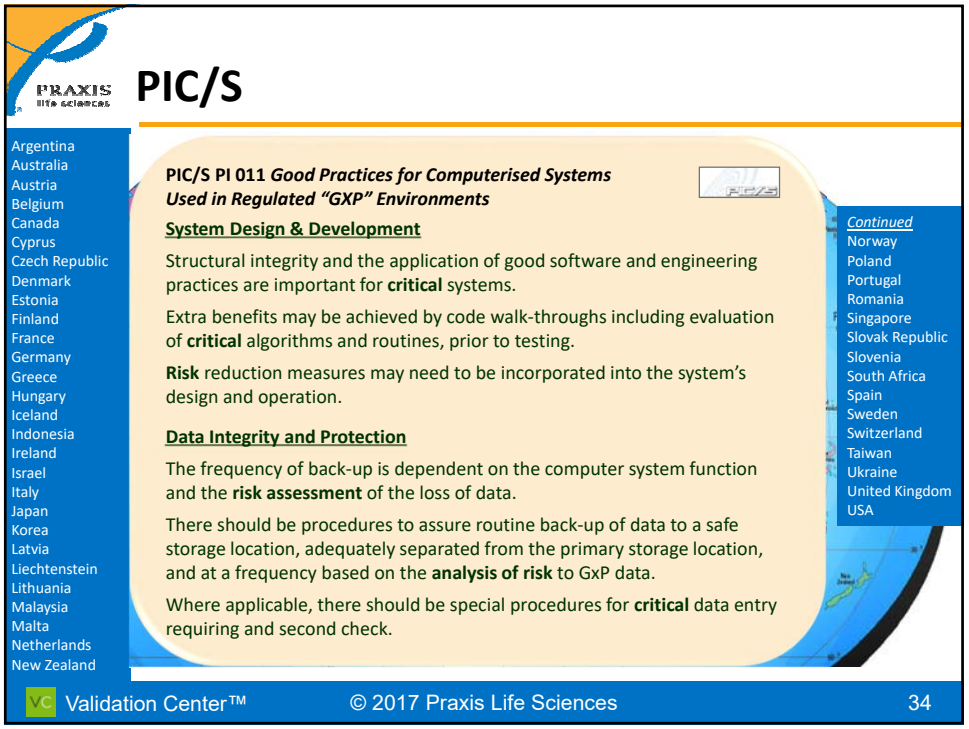
The URS (User Requirements Specs) should form the basis of a risk assessment of the system for GxP compliance requirements, in addition to other risks, such as safety. The risk analysis may be based on the FS (Functional Spec), which is related to the URS.

The **risk assessment** should identify **critical** features

Continued
Norway
Poland
Portugal
Romania
Singapore
Slovak Republic
Slovenia
South Africa
Spain
Sweden
Switzerland
Taiwan
Ukraine
United Kingdom
USA

Validation Center™ © 2017 Praxis Life Sciences 32





PIC/S

Argentina
Australia
Austria
Belgium
Canada
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland
Indonesia
Ireland
Israel
Italy
Japan
Korea
Latvia
Liechtenstein
Lithuania
Malaysia
Malta
Netherlands
New Zealand

PIC/S PI 011 ***Good Practices for Computerised Systems Used in Regulated "GXP" Environments***

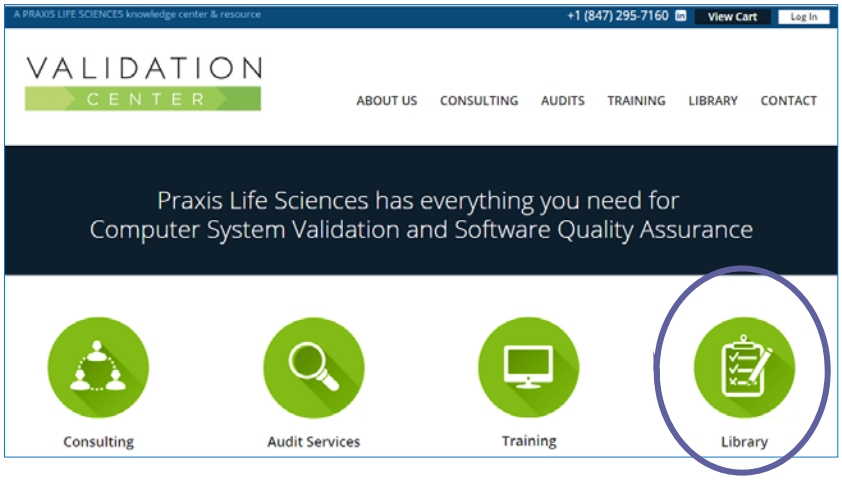
Software Suppliers

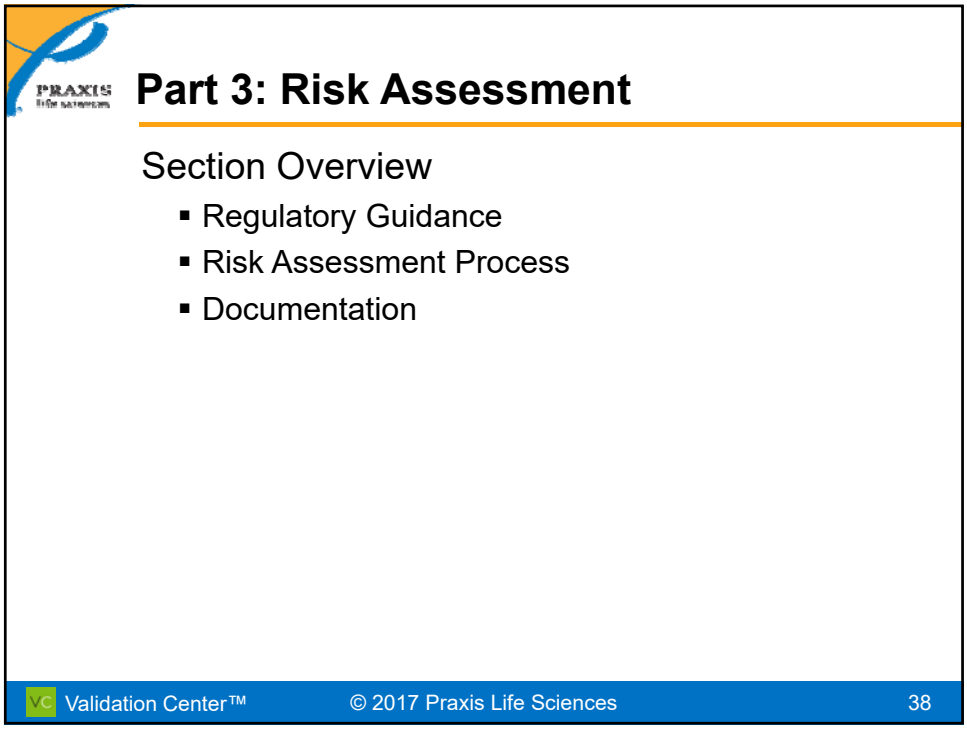
The need to perform a supplier audit should be linked to the regulated user's **risk assessment** and quality assurance standards.

For GxP regulated applications it is essential for the regulated user to define a requirement specification prior to selection and to carry out a properly documented supplier assessment and **risk analysis** for the various system options. Information for such exercises may come from supplier audits and research into the supplier's product versions in the user community and literature.

Continued
Norway
Poland
Portugal
Romania
Singapore
Slovak Republic
Slovenia
South Africa
Spain
Sweden
Switzerland
Taiwan
Ukraine
United Kingdom
USA

www.ValidationCenter.com





Risk Management Framework

Risk Management Process

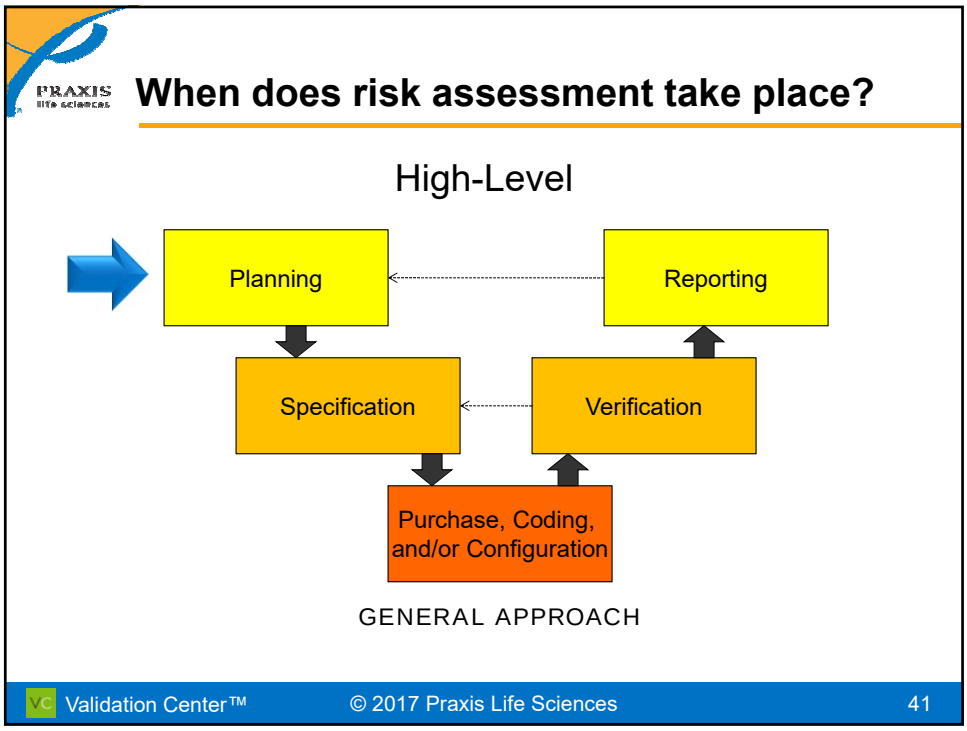
Risk Assessment	SOP System Risk Assessment
Risk Mitigation	SOP Risk Based Validation; SOP Audit Trails; SOP System Security; SOP Software Vendor Assessment; SOP User Training; SOP Incident Management; SOP System Backup; SOP Business Continuity; Etc.

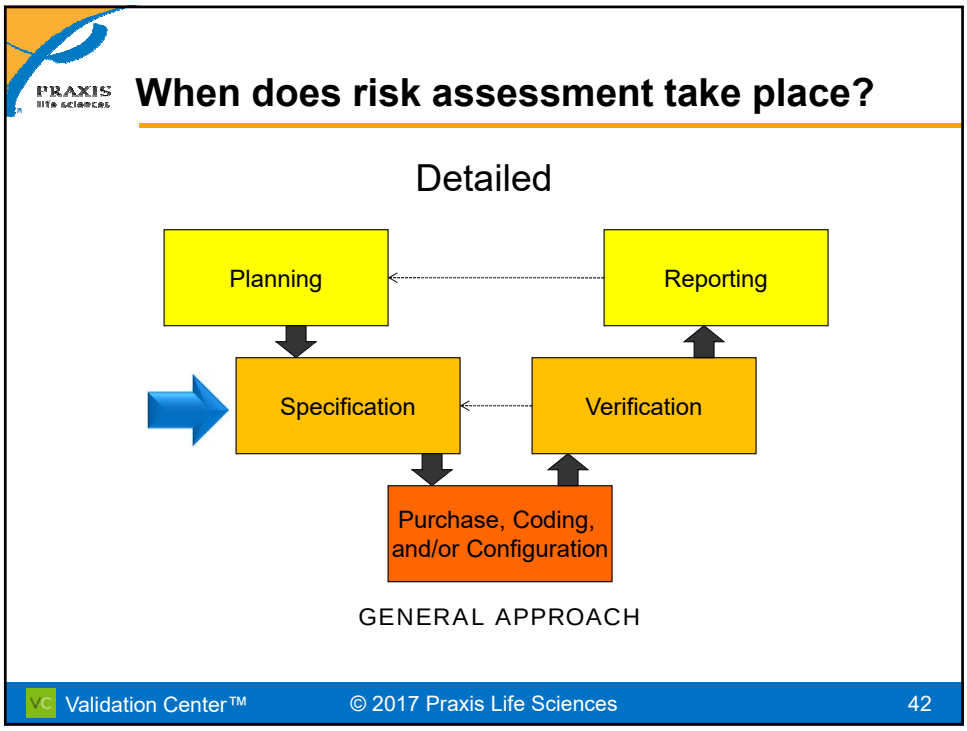
Risk Assessment Roles

Business Process Owner
Identify, Evaluate, and Classify Risks

Quality Assurance
Evaluate any risks associated with regulatory compliance and company policies

Technology Owner
Provide information on how the software works and where it could fail





Risk Assessment Steps

Identification → **Evaluation** → **Classification**

Identification	Evaluation	Classification
Determine and document the hazards associated with use of the system.	Assess the severity and probability of the identified hazards.	Categorize the risks according to severity and probability. Document the classifications.

Hazard Identification

Identification How are hazards identified?

- ❑ Key Question
  - What might go wrong with this system?
- ❑ Areas of focus
  - Feature or functions that would negatively impact
    - Patient safety
    - Product quality
    - The integrity of associated data

Example System

Laboratory Management System

Module "A"
Instrument Control & Test Result Tracking

Module "B"
Lab Analyst Training Management & Tracking

Module "C"
Test Charge Accounting

Example Hazards

Identification What might go wrong?

User Requirement	Identified Hazard
1. Send test instructions to lab instruments and receive test result data from the instrument	An instrument interface problem could result in an incorrect reading from equipment
2. Calculate whether a test passes or fails using input from the lab instruments and analyst entries	An incorrect laboratory calculation could provide a passing test result when it should have failed
3. Assign analysts to perform tests based on training	A data integrity error in the training module could show that a lab analyst was trained when she was not
4. Calculate the charges for testing for each product line	There could be a calculation error in the Test Charge module

Hazard Evaluation

Evaluation How are hazards evaluated?

Risk Definition

The combination of the probability of occurrence of a hazard and the severity of the hazard

Risk Component 1	*Risk Component 2*
Severity of Harm	**Probability of Occurrence**
Measured as Criticality	**Measured as Complexity**

Hazard Evaluation

Evaluation How are hazards evaluated?

- Key Questions
  - What are the consequences (severity) of the hazard?
  - What is the likelihood (probability) the hazard will occur?
- Areas of focus
  - Features or functions that could lead to
    - Patient death or injury
    - Product failure or waste
    - Compromised integrity of the associated data

Hazard Evaluation

Severity Evaluation

How are hazards evaluated?

Risk Definition

The combination of the probability of occurrence of a hazard and the severity of the hazard

Risk Component 1	Risk Component 2
Severity of Harm	Probability of Occurrence
Measured as Criticality	Measured as Complexity

Hazard Evaluation Examples

Severity Evaluation

How are hazards evaluated?

URS	Identified Hazard	Evaluation of Severity
1	An instrument interface problem could result in an incorrect reading from equipment	Could result in an impure batch of product
2	An incorrect laboratory calculation could provide a passing test result when it should have failed	Could result in death of a patient (if too potent) or failure to cure a patient (in not potent enough)
3	A data integrity error in the training module could show that a lab analyst was trained when she was not	Could result in a lab analyst being assigned to run a lab test without proper training
4	There could be a calculation error in the Test Charge module	Could result in a manufacturing department being overcharged

Severity Classification

Severity Classification

How is severity classified?

- Common Classification Method
  - Classification by Criticality
  - 3 Levels

High Criticality	Direct impact on patient safety, product quality, or the integrity of associated data
Medium Criticality	Indirect impact on patient safety, product quality, or the integrity of associated data
Low Criticality	No impact on patient safety, product quality, or the integrity of associated data

Severity Classification

Level	Expanded Definition
High Criticality	Direct control of: • Manufacturing • Labeling • Distribution • Product Testing • Product Release Direct impact on: • Product Quality • Product Efficacy • Patient Safety • Personnel Safety
Medium Criticality	Indirect impact on patient safety, product quality, or the integrity of associated data
Low Criticality	No impact on patient safety, product quality, or the integrity of associated data

Severity Classification

Examples

- Health product software
- Manufacturing controls
- Automated product inspection
- Label management & automation
- Distribution tracking to enable recalls
- Laboratory test results
- Adverse event tracking
- Clinical trial results
- Patient medical records
- Product quality status management

Severity Classification

Level	Expanded Definition
High Criticality	Direct impact on patient safety, product quality, or the integrity of associated data
Medium Criticality	Indirect involvement in: •Manufacturing •Labeling •Distribution •Product Testing & Release Indirect impact on: •Product Quality •Product Efficacy •Patient Safety •Personnel Safety Provides GxP compliance for features not already identified as "High Criticality"
Low Criticality	No impact on patient safety, product quality, or the integrity of associated data

Severity Classification

Examples
- Calibration tracking
- Validation tracking
- Document management
- Training tracking
- Corrective/Preventive action tracking
- System access tracking
- Electronic submissions to regulatory agencies
- Product work order management
- Deviation tracking
- Audit tracking

Validation Center™ © 2017 Praxis Life Sciences 53

Severity Classification

Level	Expanded Definition
High Criticality	Direct impact on patient safety, product quality, or the integrity of associated data
Medium Criticality	Indirect impact on patient safety, product quality, or the integrity of associated data
Low Criticality	Any function not already identified as "High Criticality" or "Medium Criticality

Severity Classification

Examples
- Manufacturing cost reports
- Turnaround time reports

Validation Center™ © 2017 Praxis Life Sciences 54

Severity Classification Examples

Severity Classification

URS	Identified Hazard	Evaluation of Severity	Criticality
1	An instrument interface problem could result in an incorrect reading from equipment	Could result in an impure batch of product	High
2	An incorrect laboratory calculation could provide a passing test result when it should have failed	Could result in death of a patient or failure to cure a patient	High
3	A data integrity error in the training module could show that a lab analyst was trained when she was not	Could result in a lab analyst being assigned to run a lab test without proper training	Medium
4	There could be a calculation error in the Test Charge module	Could result in a manufacturing department being overcharged	Low

Probability Evaluation

Probability Evaluation

How are hazards evaluated?

Risk Definition

The combination of the probability of occurrence of a hazard and the severity of the hazard

Risk Component 1	Risk Component 2
Severity of Harm	Probability of Occurrence
Measured as Criticality	Measured as Complexity

Why is "Complexity" Important

The selection of **validation activities** should be commensurate with the **complexity** of the software and the **risk** associated with use of the software for its specific intended use

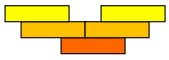
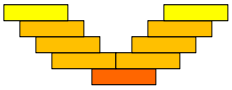
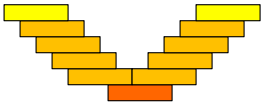
Validation **coverage** should be based on the software' **complexity** and safety **risk.**

The scope and level of **documentation** and **records** needed to formalize and satisfy basic project management requirements for **critical** systems will be dependent on the **complexity** of the system.

Probability Classification

Probability Classification

How can probability be classified?

Validation Approach	Complexity Level	Definition
	**Low**	Standard, non-configured functions within off-the-shelf purchased systems
	**Medium**	Configured functions within off-the-shelf purchased systems
	**High**	Custom developed functions within either purchased or custom systems

Probability Classification

Complexity Level	Definition	Examples
Low	Standard, non-configured functions within off-the-shelf purchased systems	• Standard test result report within an off-the-shelf laboratory system • Standard data entry screen in a medical records system
Medium	Configured functions within off-the-shelf purchased systems	• Report configured with an off-the-shelf query tool • Calculation configured in a laboratory system • Calculation configured in an off-the-shelf spreadsheet tool • Product release algorithm configured in an off-the-shelf inventory control system
High	Custom developed functions within either purchased or custom systems	• Custom accounting report developed in COBOL • Custom code developed to send e-mail notification from an off-the-shelf training management system

Probability Classification Example

Laboratory Management System

Module "A" Instrument Control & Test Result Tracking

Module "B" Lab Analyst Training Management & Tracking

Module "C" Test Charge Accounting

Probability Classification Example

Probability Classification

URS	Requirement	Criticality	Technology	Complexity
1	Send test instructions to lab instruments and receive test result data from the instrument	High	Configured using the out-of-the-box instrument interface tool	Medium
2	Calculate whether a test passes or fails using input from the lab instruments and analyst entries	High	Custom code	High
3	Assign analysts to perform tests based on training	Medium	Out-of the box functionality	Low
4	Calculate the charges for testing for each product line	Low	Custom report developed in house	High

Validation Center™ © 2017 Praxis Life Sciences 61

Classification Levels

Classification

	Requirement Level Criticality	Requirement Level Complexity
1	High	Medium
2	High	High
3	Medium	Low
4	Low	

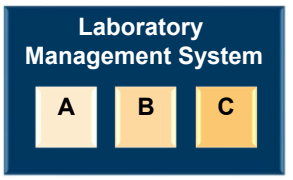
System level criticality is the same as the highest requirement level criticality

System Level Criticality
High

Validation Center™ © 2017 Praxis Life Sciences 62

Risk Assessment Documentation

Where should the risk assessment be documented?



System Level
- Validation Master Plan (VMP)
- Stand-alone, Risk Assessment

Requirement Level
- Requirements Specification
- Stand-alone, Risk Assessment

options

Risk Assessment Documentation

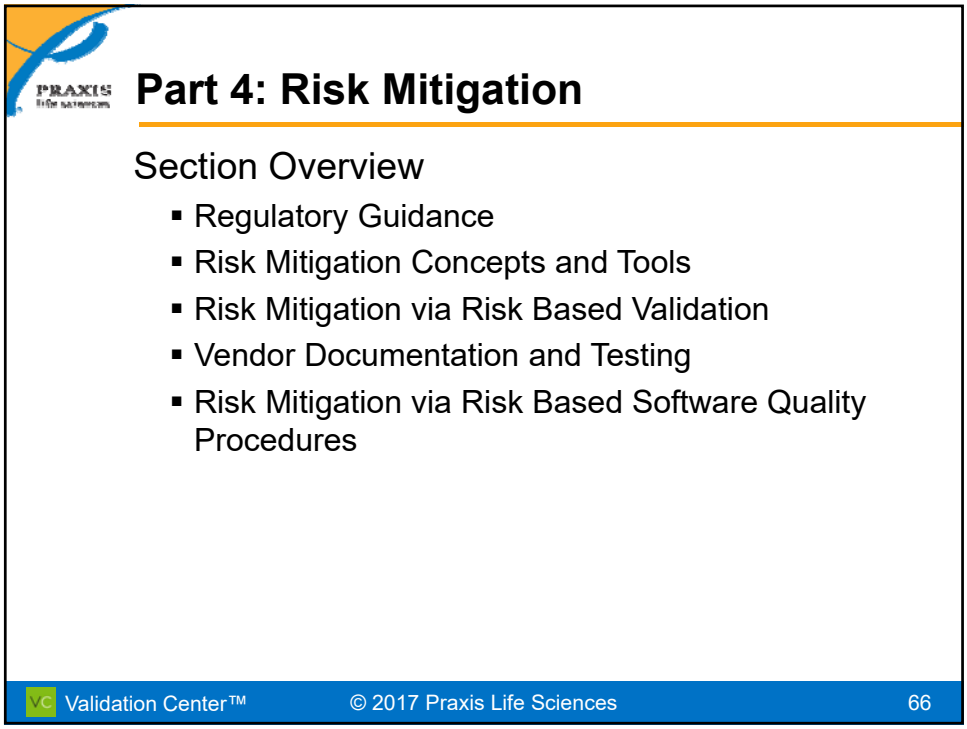
System and Requirement Risk Assessment

System Name: ABC Laboratory Management System
System Version: 1.0

System Criticality Level: ☒ High ☐ Medium ☐ Low
System Criticality Rationale: System performs functions that are critical to patient safety. See details in the analysis, below.

Requirement Criticality and Complexity Analysis

Requirement	Criticality Level	Rationale for Criticality Level	Complexity Level	Rationale for Complexity Level
Instrument control [URS 1]	High	An incorrect lab instrument reading could result in a ruined batch of product, patient death or injury, failure to cure a patient.	Medium	Configured with system's instrument interface tool
Test pass/fail determination [URS 2]	High	A calculation error could result in patient death or injury, failure to cure a patient.	High	Custom Code
Analyst assignment based on training [URS 3]	Medium	A data integrity issue in this function could result in a lab analyst being assigned to run a lab test without proper training.	Low	Standard system functionality without modification
Testing charges for each product [URS 4]	Low	This function has no impact on patient safety or public health.	High	Custom code

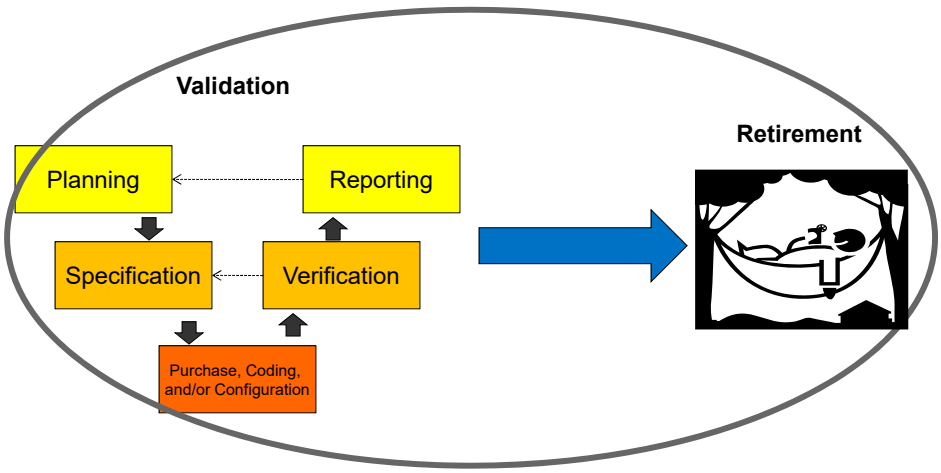


Risk Mitigation Definition

Risk Mitigation

Actions taken to reduce the impacts of risks

When does Risk Mitigation Take Place?



What are Risk Mitigation Activities?

Risk Mitigation

Actions taken to reduce the impacts of risks

Procedures that reduce the likelihood of system failure:

2nd person verification of data entry, calculations, increased user training, etc.

Procedures that increase the likelihood of detection of system failure:

frequent audits of data integrity, back-up tapes, etc.

Activities that reduce the likelihood of system failure:

design changes, design reviews, code walkthroughs, testing, etc.

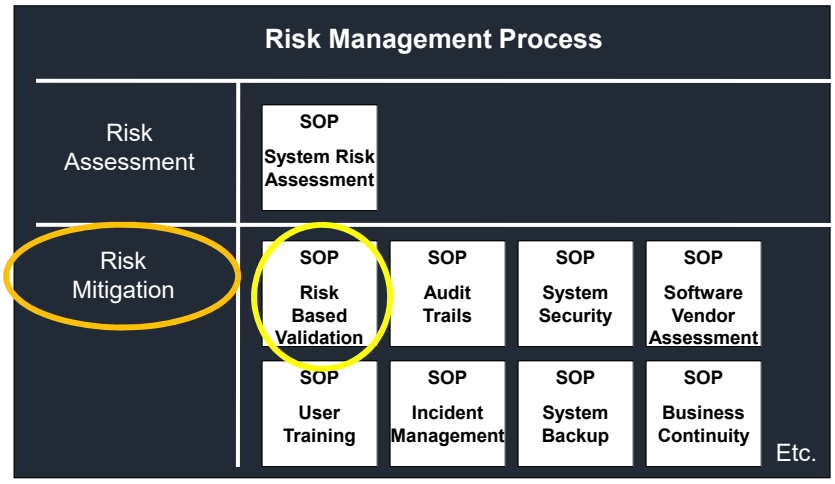
Risk Mitigation Roles

Quality Assurance
Ensure mitigation approach meets expectations for regulatory compliance and company policies

Business Process Owner
Develop procedural mitigation approaches

Technology Owner
Develop technical mitigation approaches

Risk Mitigation Framework



Risk Based Approach to Validation Testing

Criticality	High	Med	Low	High	Med	Low	High	Med	Low
Complexity	High	High	High	Med	Med	Med	Low	Low	Low
Requirements Coverage	All require-ments, multiple data sets	All require-ments, single data set	Sampling	All require-ments, multiple data sets	All require-ments, single data set	Sampling	All require-ments, single data set	All require-ments, single data set	Sampling
Path testing	All paths, multiple scenarios	All paths, single scenario	Sampling	All paths, single scenario	All paths, single scenario	Sampling	All paths, single scenario	Sampling	Sampling
Boundary testing	✓	✓	*Optional*	✓	*Optional*	*Optional*	✓	*Optional*	*Optional*
Test case degree of detail and specificity	Specific, detailed	Medium detail	General	Specific, detailed	Medium detail	General	Specific, detailed	Medium detail	General
Test data similar to production data	✓	✓	*Optional*	✓	*Optional*	*Optional*	✓	*Optional*	*Optional*
Testing evidence	Completed protocol, Screen prints of test inputs and outputs	Completed protocol, Screen prints of test outputs	Completed protocol	Completed protocol, Screen prints of test inputs and outputs	Completed protocol, Screen prints of test outputs	Completed protocol	Completed protocol, Screen prints of test inputs and outputs	Completed protocol, Screen prints of test outputs	Completed protocol
User execution of validation tests	*OQ & PQ*	*PQ*	*Optional*	*PQ*	*Optional*	*Optional*	*PQ*	*Optional*	*Optional*

✓ Required

Risk Based Approach to Validation Documentation

Criticality	High	Med	Low	High	Med	Low	High	Med	Low
Complexity	**High**	**High**	**High**	**Med**	**Med**	**Med**	**Low**	**Low**	**Low**
Change Request	✓	✓	✓	✓	✓	✓	✓	✓	✓
Risk Assessment	✓	✓	✓	✓	✓	✓	✓	✓	✓
Validation Plan	✓	✓	*Optional*	✓	✓	*Optional*	✓	✓	*Optional*
User Requirements (URS)	✓	✓	*Optional*	✓	✓	*Optional*	✓	✓	*Optional*
Functional Specifications (FS)	✓ Highly Detailed	✓ Less Detail	*Optional*	✓ Highly Detailed	✓ Less Detail	*Optional*	✓ Medium Detail	✓ Less Detail	*Optional*
Design: Architecture	✓	✓	*Optional*	✓	✓	*Optional*	✓	✓	*Optional*
Design: Software	✓ Highly Detailed	✓ Less Detail	*Optional*	n/a	n/a	n/a	n/a	n/a	n/a
Design: Configuration	n/a	n/a	n/a	✓	✓	*Optional*	n/a	n/a	n/a
Test Plan/Design	✓	✓	*Optional*	✓	*Optional*	*Optional*	*Optional*	*Optional*	*Optional*
Validation Protocols (IQ. OQ, PQ)	✓	✓	*Optional*	✓	✓	*Optional*	✓	✓	*Optional*

✓ Required

Validation Center™ © 2017 Praxis Life Sciences 73

Risk Based Approach to Validation Documentation

Criticality	High	Med	Low	High	Med	Low	High	Med	Low
Complexity	**High**	**High**	**High**	**Med**	**Med**	**Med**	**Low**	**Low**	**Low**
Validation Incident Reports	✓	✓	*Optional*	✓	✓	*Optional*	✓	✓	*Optional*
Trace Matrix – URS to FS	✓	✓	*Optional*	✓	✓	*Optional*	✓	✓	*Optional*
Trace Matrix – FS to Design	✓	✓	*Optional*	✓	*Optional*	*Optional*	*Optional*	*Optional*	*Optional*
Trace Matrix – URS to PQ	✓	✓	*Optional*	✓	✓	*Optional*	✓	✓	*Optional*
Trace Matrix – FS to OQ	✓	✓	*Optional*	✓	✓	*Optional*	✓	✓	*Optional*
OQ, PQ Trace To:	Test Step	Test Step	*Optional*	Test Step	Test Case	*Optional*	Test Step	Test Case	*Optional*
Validation Summary	✓	✓	*Optional*	✓	✓	*Optional*	✓	✓	*Optional*
Deployment Plan	✓	✓	*Optional*	✓	✓	*Optional*	✓	✓	*Optional*
Data Conversion Plan	✓	✓	*Optional*	✓	✓	*Optional*	✓	✓	*Optional*

✓ Required

Validation Center™ © 2017 Praxis Life Sciences 74

Risk Based Approach to Verification Activities

Criticality	High	Med	Low	High	Med	Low	High	Med	Low
Complexity	High	High	High	Med	Med	Med	Low	Low	Low
Vendor Assessment	n/a	n/a	n/a	✓	✓	*Optional*	✓	✓	*Optional*
Unit Testing	✓	✓	*Optional*	n/a	n/a	n/a	n/a	n/a	n/a
Code Review	✓	✓	*Optional*	n/a	n/a	n/a	n/a	n/a	n/a
Design Review	✓	✓	*Optional*	✓	*Optional*	*Optional*	*Optional*	*Optional*	*Optional*
Part 11 Compliance Assessment	✓	✓	n/a	✓	✓	n/a	✓	✓	n/a
Verification of System Use and Support SOPs **	✓	✓	*Optional*	✓	✓	*Optional*	✓	✓	*Optional*

✓ Required

** System Use and Support SOPs include: Back-up, Recovery, Security and Access, Training Requirements, Incident Handling, Change Management, Technical Operation and Routine Maintenance, User Operation

Risk Based Validation Example

Examples from Laboratory Management System

	Function	Criticality	Technology	Complexity
A	Interface to a lab instrument to control instrument and read results	**High**	Configured using the out-of-the-box instrument interface screen	**Medium**

Document Requirements
- User Requirements
- Detailed Functional Specs
- Design Documentation (Architecture + Configuration)
- Test Plan/Design
- Protocols (IQ, OQ, PQ)
- Trace Matrices (URS → FS, FS → Design, URS → PQ, FS → OQ)

Testing Requirements
- All requirements, multiple data sets
- All paths, 1 scenario
- Boundaries
- Realistic test data
- Screen prints of inputs and outputs
- Users execute PQ; may delegate OQ execution

Additional Verifications
- Design Review
- Part 11 Compliance Assessment
- SOPs for system use and support

Risk Based Validation Example

Examples from Laboratory Management System

	Function	Criticality	Technology	Complexity
B	Calculation of batch pass/fail based on lab test results	High	Custom code	High

Document Requirements
- User Requirements
- Detailed Functional Specs
- Design Documentation (Architecture + **Software**)
- Test Plan/Design
- Protocols (IQ, OQ, PQ)
- Trace Matrices (URS → FS, FS → Design, URS → PQ, FS → OQ)
- **Unit Test Report**
- **Code Review Report**

Testing Requirements
- All requirements, multiple data sets
- All paths, **multiple** scenarios
- Boundaries
- Realistic test data
- Screen prints of inputs and outputs
- **Users execute both OQ and PQ**

Additional Verifications
- Design Review
- Part 11 Compliance Assessment
- SOPs for feature use
- **Unit Testing**
- **Code Review**

Risk Based Validation Example

Examples from Laboratory Management System

	Function	Criticality	Technology	Complexity
C	Entry of training dates	Medium	Out-of the box functionality	Low

Required Documents
- User Requirements
- Functional Specs **(can be less detailed)**
- Design Documentation **(Architecture only)**
- Protocols (IQ, OQ, PQ)
- Trace Matrices (URS → FS, URS → PQ, FS → OQ)

Optional Documents
- **Test Plan/Design**
- **Trace from FS → Design**

Testing Requirements
- All requirements, **single** data set
- **Sample** of paths
- Screen prints of outputs **(no screen prints of inputs)**

Testing Options
- **Boundary testing**
- **Realistic test data**
- **Users may delegate both OQ & PQ execution**

Additional Verifications
- Part 11 Compliance Assessment
- SOPs for feature use

Optional Verifications
- **Design Review**

Risk Based Validation Example

Examples from Laboratory Management System

	Function	Criticality	Technology	Complexity
D	Reporting of test charges for a department	Low	Custom report developed in house	High

Optional Documents
- User Requirements
- Functional Specs
- Design Documentation
- Test Plan
- Protocols (IQ, OQ, PQ)
- Trace Matrices
- Unit Test Report
- Code Review Report

Testing Requirements
- Sample of requirements
- Sample of paths

Testing Options
- Boundary testing
- Realistic test data
- Screen prints
- Users may delegate both OQ & PQ execution

Optional Verifications
- Part 11 Compliance Assessment
- SOPs for feature use
- Design Review
- Code Review
- Unit Testing

Can we leverage the vendor's work?

Criticality	High	Med	Low	High	Med	Low	High	Med	Low
Complexity	High	High	High	Med	Med	Med	Low	Low	Low
Vendor Assessment	n/a	n/a	n/a	Required	Required	Optional	Required	Required	Optional
Unit Testing	Required	Required	Optional	n/a	n/a	n/a	n/a	n/a	n/a
Code Review	Required	Optional	Optional	n/a	n/a	n/a	n/a	n/a	n/a
Part 11 Compliance Assessment	Required	Required	Optional	Required	Required	Optional	Required	Required	Optional
Verification of System Use and Support SOPs **	Required	Required	Optional	Required	Required	Optional	Required	Required	Optional

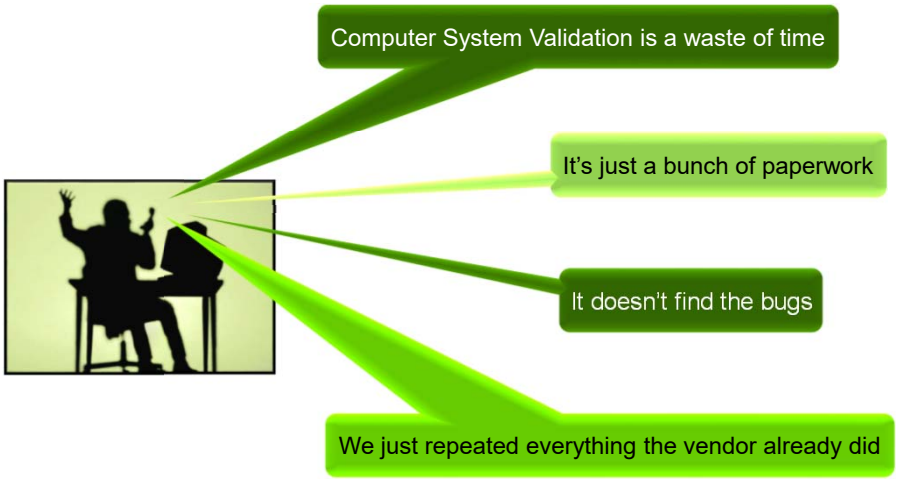
Can we leverage the vendor's work?

Vendor Rating	Impact to Validation Approach
Full Approval	• Follow risk-based validation matrix • Internally review, approve vendor provided documents

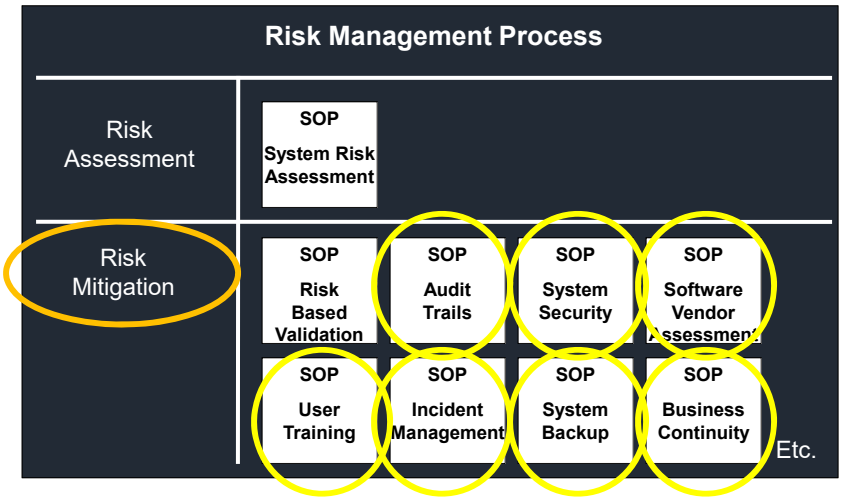
Restricted Approval	• Use vendor documents with caution
	• Rating indicates increased risk, so additional validation required.
	• Approach validation as if 1 complexity level higher
	  • If configured, approach as "custom"
	  • If out-of-the-box, approach as "configured"

Not Approved	• Avoid reliance on vendor documents • Rating indicates increased risk, so additional validation required. • Approach validation as if "Custom"

Have You Ever Heard…



Risk Management Framework



Risk Mitigation in …

Vendor Assessment SOP *example*

SOP Software Vendor Assessment

System Criticality Level	Vendor Assessment Method
High	On-Site assessment is the preferred method for highly critical software applications.
Medium	Mail, e-mail, or telephone assessment is the preferred method for medium criticality software applications. An assessment purchased from a third-party software vendor assessment firm is also acceptable for this criticality level.
Low	Vendors of low criticality software applications do not need to be assessed.

Risk Mitigation in …

Audit Trail SOP *example*

SOP Audit Trails

Requirement Criticality Level	Audit Trail Requirement
High	Audit trail is required for records associated with highly critical system functions
Medium	Audit trail is required for records associated with system functions of medium criticality
Low	Audit trail is not required for records associated with system functions of low criticality

Risk Mitigation in …

System Security SOP *example*

SOP System Security

System Criticality Level	Password Change Frequency
High	Every 90 days
Medium	Every 120 days
Low	Not required

Risk Mitigation in …

User Training SOP *example*

SOP: User Training

Requirement Criticality Level	Training Format: Function is not intuitive to use correctly	Training Format: Function is intuitive to use correctly
High	• Instructor Led Class • Hands-on Exercises • Competency Exam	• Self-study Materials • Hands-on Exercises • Competency Exam
Medium	• Instructor Led Class • Hands-on Exercises	• Self-study Materials
Low	• Self-study Materials • Hands-on Exercises	• Self-study Materials

Risk Mitigation in …

System Back-up SOP *example*

SOP: System Back-Up

System Criticality Level	Back-up Location	Back-up Media Audit Frequency
High	Off-site Secure vault	Annual
Medium	Off-site Locked cabinet	Every 18 months
Low	Separate building	Not required

Risk Mitigation in …

Business Continuity SOP *example*

SOP Business Continuity

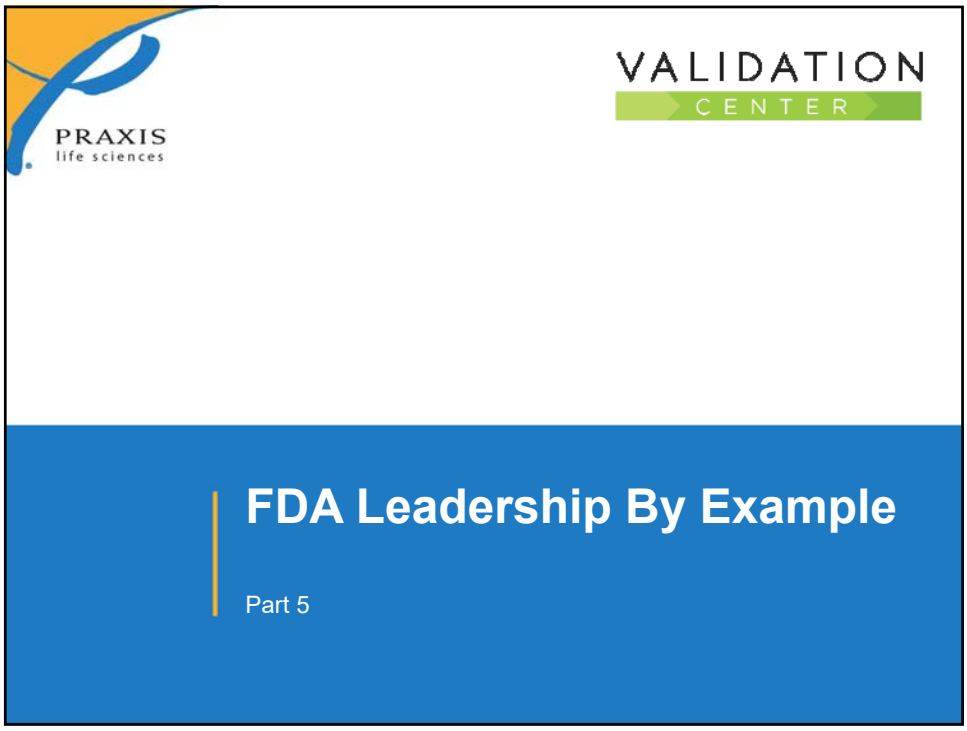
Requirement Criticality Level	Business Continuity Procedure Required	2nd Person Verification of Data Entry Required
High	Yes	Yes
Medium	Yes	No
Low	No	No

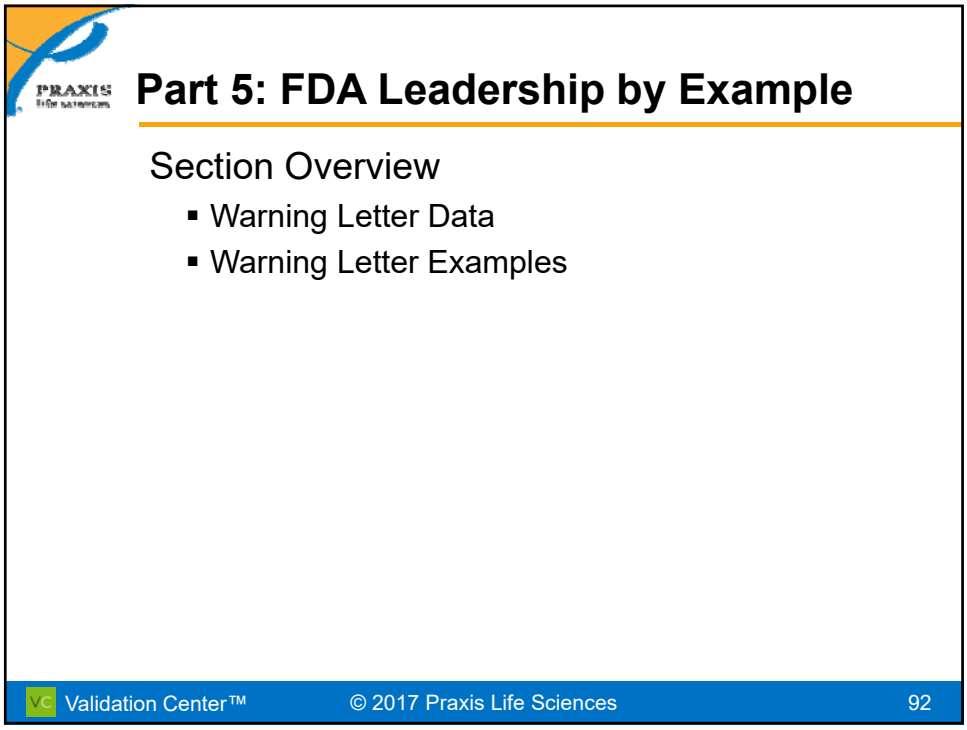
Risk Mitigation in …

Incident Management SOP *example*

SOP Incident Management

Requirment Criticality Level	Resolution Priority		
	Users cannot perform job	Major Inconvenience	Minor Inconvenience
High	High	High	High
Medium	High	Medium	Medium
Low	High	Medium	Low





FDA Warning Letter Data

– Data Source
- FDA Warning Letters related to Software and Computers
- 3 Year Date Range: Q1-2014 through Q4-2016

– Summaries
- By system type
- By observation topic
  - By validation observation topic

FDA Warning Letter Example

Regulatory Reference

Summary Finding

2. Your firm failed to exercise appropriate controls over computer or related systems to assure that only authorized personnel institute changes in master production and control records, or other records (21 C.F.R. §211.68(b)).

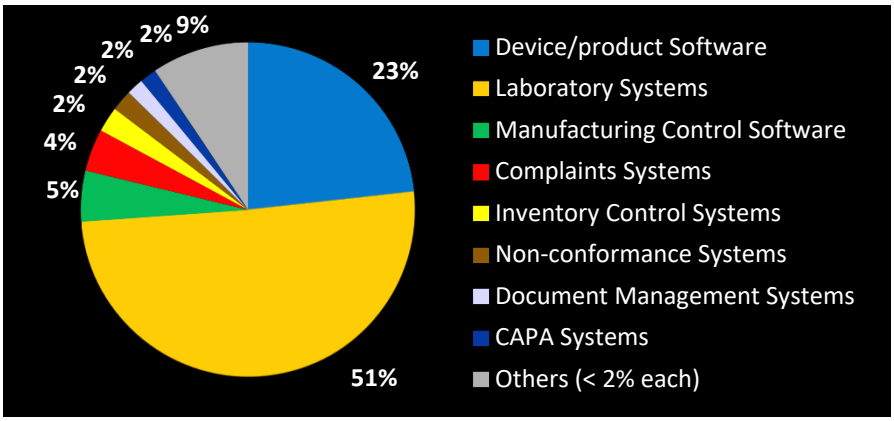
Your firm failed to have adequate procedures for the use of computerized systems in the quality control (QC) laboratory. Our inspection team found that current computer users in the laboratory were able to delete data from analyses. Notably, we also found that the audit trail function for the gas chromatograph (GC) and the X-Ray Diffraction (XRD) systems was disabled at the time of the inspection. Therefore, your firm lacks records for the acquisition, or modification, of laboratory data.

Moreover, greater than **(b)(4)** QC laboratory personnel shared **(b)(4)** login IDs for **(b)(4)** high performance liquid chromatographs (HPLC) units. In addition, your laboratory staff shared one login ID for the XRD unit. Analysts also shared the username and password for the Windows operating system for the **(b)(4)** GC workstations and no computer lock mechanism had been configured to prevent unauthorized access to the operating systems. Additionally, there was no procedure for the backup and protection of data on the GC standalone workstations.

Specific Observations

Software & Computer Warning Letters

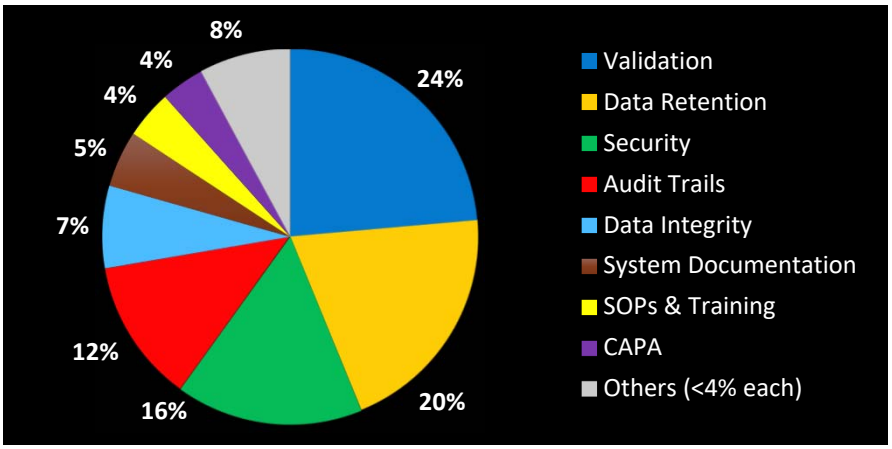
3 Year Summary by System Type



"Other" system types include systems for Labeling, Calibration Management, Building Management, Inspection Systems, Clinical Trial Data Management, Service Records, Distribution, Certificate of Analysis, Audit Management, Change , Control, Product Design Software, Equipment Tracking, Qualification Tracking, and Supplier Approval Tracking,

Software & Computer Warning Letters

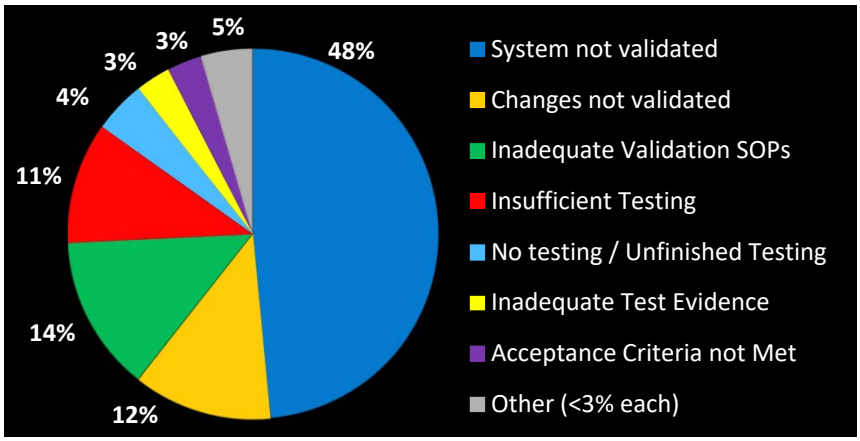
3 Year Summary by Observation Topic



"Other" observation topics include Change Control, Suitability for Use, Quality Oversight, Risk Analysis, Electronic Signatures, Vendor Management, and Data Accuracy

Software & Computer Warning Letters

3 Year Summary by Validation Observation Details



"Other" observation validation topics include Inadequate Validation Plan, No Source Code Evaluation, and No Trace Matrix, Incomplete Design Documentation, and Went Live with Known Critical Defects

Warning Letter Examples

Regulatory Reference	21 CFR 820 (Medical Devices)
System Type	Medical Device Software
FDA Branch or District	CDRH

Failure to adequately establish and maintain procedures to control the design to ensure that requirements are met.

- *Development of Key Functionality*, requires the firm to assess risk and re-assess risk as needed. Although XXXXXX was released on November 25, 2010, Software Risk Management Summary Doc. was not completed until July 14, 2011 and did not include an analysis of the risk specific to the intended use of XXXXXX.

Warning Letter Examples

Regulatory Reference	21 CFR 820 (Medical Devices)
System Type	Medical Device Software
FDA Branch or District	Cincinnati District

Failure to demonstrate that the device was developed in accordance with the design control requirements of the Quality System regulation.

- Failure to have complete risk analyses in that 5 versions of risk analysis were not controlled documents.
- Risk analyses were not reviewed and approved.
- Risk analyses were not updated when a software issue was discovered that resulted in a software change.

Warning Letter Examples

Regulatory Reference	21 CFR 820 (Medical Devices)
System Type	Medical Device Software
FDA Branch or District	Florida District

Failure to adequately establish and maintain procedures for validation.

- Firm's Risk Analysis Report for software version 00, does not adequately assess the risk presented by the software controlling the X-Ray Unit XXX as a moderate risk to users and patients.
- For example, the report indicates a "No" to the questions:
  - "Could a malfunction of, or a latent design flaw in the Software Device lead to an erroneous diagnosis or a delay in delivery of appropriate medical care that would likely lead to Moderate Injury?"
  - "Does the Software Device control the delivery of potentially harmful energy that could result in death or serious injury?"

PRAXIS life sciences

VALIDATION CENTER

Conclusion

PRAXIS life sciences

Next Steps

1. Review your regulations and guidelines
2. Identify your criticality levels and definitions
3. Define your complexity measures
4. Determine how you will apply complexity & criticality to validation and software quality practices
5. Write your policies and procedures
6. Train your staff

Need Help?

- ValidationCenter.com Library of SOPs and Template
- Online and Classroom CSV Training
- Software QA and Validation Program Implementation
  Validation Services
- Audit Readiness Assessments

Thank You!

- Thanks for your interest in Risk Based Approach to
  - Software Quality & Validation.
- Any questions about what we have discussed today?
  - Please, feel free to contact me:

Deb Bartel

+1 (847) 295-7160
dbartel@PraxisLifeSciences.com

ValidationCenter.com
PraxisLifesSciences.com

Follow us!