Bioscience Solutions

Lonza

White Paper:

Ensuring Data Integrity in the Bacterial Endotoxins Test

« It is essential under data integrity standards to review your data periodically to prove your data is in compliance »

Introduction

Data integrity is a fundamental component in the pharmaceutical industry. Although not a new concept, data integrity is important throughout the entire endotoxin testing process. This White Paper provides an FMEA (Failure Mode and Effect Analysis) that helps QC professionals identify risks that may be inherent in their current processes. Using this risk-based approach, QC professionals will be able to get closer to their overall workflow and help ensure data integrity compliance in the bacterial endotoxins test.

Goal: Determine where Data Integrity Issues Exist in the Process

Integrity of data is not a 'new' regulatory requirement. Data Integrity "refers to the completeness, consistency, and accuracy of data." FDA Draft Guidance to Industry "Data Integrity and Compliance With CGMP Guidance for Industry" (4/2016). The extent to which all data are complete, consistent and accurate throughout the data lifecycle (MHRA).

Data integrity is the degree to which a collection of data is complete, consistent and accurate throughout the data lifecycle. The collected data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate. Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practices. (WHO) FMEA is Failure Mode and Effects Analysis. It is a standard Risk Assessment methodology that is used to assess and rank potential risks or "Failure Modes" for a system or process.

Failure Mode and Effect Analysis Applied to WinKQCL™ Software

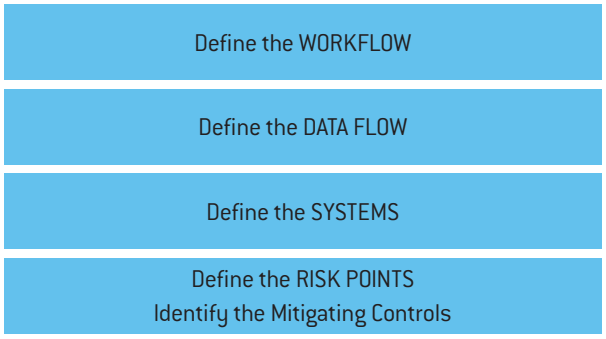
Based on this understanding we developed a questionnaire (FMEA) to serve as a qualitative risk assessment to assess all our systems in a standardized way. This is a binary exercise: either there is a gap requiring action or there is no need for action. This process was then applied to WinKQCL™ Endotoxin Software. Before you start the FMEA, a high level overview of the process is needed. The following diagram provides details about the general workflow before a risk assessment can begin.

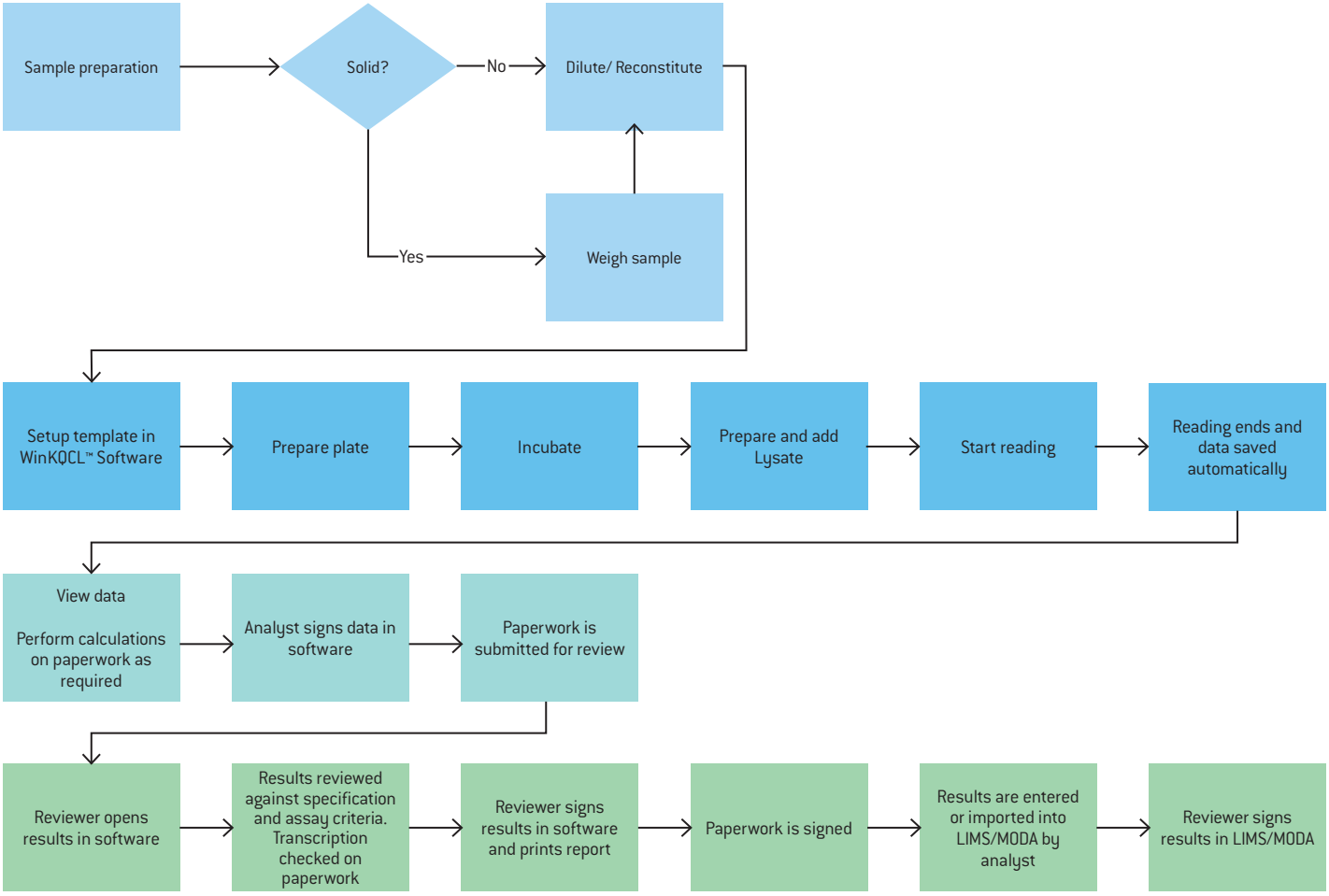
« Data Integrity is not just about what tools are provided by the software or how it is configured but more importantly how it is used in the overall process. »

Consolidated Data Flow in the Endotoxin Testing Lab

In the diagram below, you will find a consolidated data flow for preparing and running your samples to detect endotoxins.

Approach: Document the assay process flow from sample preparation to review and release of results. Review the documented process flow to determine where risks to the data integrity exists. The key is to look for things that could go wrong either intentionally or unintentionally. The defined mitigation should address the risk and lower the risk value to an acceptable level. Before starting the risk assessment the scoring system, thresholds, and acceptable risk levels must be defined.





It Starts as a Company-Wide Philosophy and a Top Level View

We started by looking at our existing systems and developed a more precise set of policies and standards around the new guidance. We ensured that management was visibly involved at the highest level. We also rolled out basic training to establish a common understanding of the subject matter. These actions were to set the stage for what was to come next. Through this process we realized that we have to segregate critical permissions to ensure data is not corrupted; in order to truly ensure that data cannot be altered or deleted, specific sets of controls need to be put in place.

And at every step of the way we kept asking the same question:
"What can people do here to compromise integrity?"

Who is Responsible for Data Integrity?

Ultimately, senior management is responsible for building a culture of data integrity. There should be encouragement of open reporting of errors and training and awareness for the entire organization. A data governance system should be cultivated. You don't need to be an IT expert, but you should be aware of the GMP requirements. It's time to see data integrity as an opportunity to improve quality, and a paperless system, including practical traceability of sample lifecycle data, provides a great benefit from a quality perspective.

Where It Begins: The Design Phase of Your Software

By consistently applying data integrity practices during the design phase, you will help form a company-wide philosophy. The system configuration is defined to meet end-user requirements. You should validate for the intended purpose/use vs. functional validation/PQ testing. If you validate the computer system, but you do not validate it for its intended use, you cannot know if your workflow runs correctly. Controls that are appropriately designed to validate a system for its intended use address software, hardware, personnel, and documentation. SOP's drafted during OQ define the intended use requirements and during validation, establish an approach to review the various types of meaningful metadata, such as audit trails. Validation should include assessing risk and developing quality risk mitigation strategies for the data life cycle.

Data integrity is a key component of the Software Development Life Cycle used to develop, test and verify the WinKQCL™ Software package. You need to validate the compliance in the software. When done correctly, QC automation is validated to demonstrate:

- The required data is collected and enforced by the software
- Only the use of appropriate media/reagents and equipment is allowed
- Specifications/limits are enforced
- Calculations are repeatable and accurately performed

21 CFR Part § 11.10(f) states that procedures and controls for closed systems must include the use of operational checks to enforce permitted sequencing of events, as appropriate. Validation for intended purpose: a lot of companies now take a "risk-based" approach to validation, relying on the vendor to perform the validation that constitutes the bulk of the evidence. But there is a right way to do this, and a wrong way from a data integrity standpoint.

It boils down to a separation of duties:

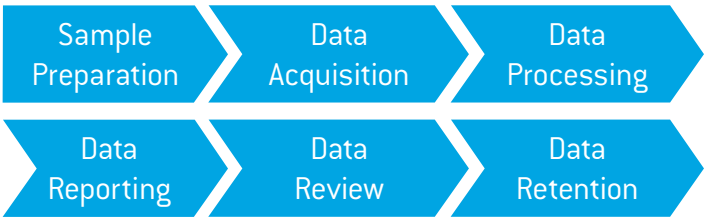
- The vendor should be able to prove the system functions were thoroughly tested and in particular, the integrity of metadata and audit trails is both secure and readable
- But the customer needs to be able to verify not just the vendor's testing, but PROVE that it's usable in their environment and business process. This means:
  - A validation based on the intended use of the system
  - That the metadata is readable and usable in their real-world context, for example, be able to easily search and see the lifecycle of a sample with all of its metadata through each stage of the process: collection, testing, results, review and analysis

WinKQCL™ Endotoxin Detection and Analysis Software

The WinKQCL™ Platform has proved effective over time, with iteration after iteration carefully tuning it to an endotoxin testing system with an installation footprint of thousands of laboratories. We are experts in endotoxin testing. We pay attention to the regulatory needs, new use cases as they arise, pain points, and strive for the best experience for our end-users. This permits users to come in with limited subject matter knowledge and perform the job at a high level.

Know Your Data Flow

The System Data flow should encompass the following phases and boundaries as applicable. Metrics can be added into the system to help with the risk assessment such as data type, responsible parties, input, and actions into each of the phases of your data flow.



Sample Preparation	Begins with obtaining physical sample and ends with samples ready for data acquisition
Data Acquisition	Begins with prepared sample and ends with permanently recorded raw data
Data Processing	Begins with newly acquired raw data and ends with permanently recorded reportable results
Data Reporting	Begins with available reported results and ends with data presented and communicated to stakeholders
Data Review	Begins with permanently recorded reportable results and ends with approval of all data and sample results by a reviewer
Data Retention	Begins when data is created that needs to be retained for business and regulatory aspects and ends when the defined data retention period has been met

Sample Preparation Phase

Phase starts with physical sample from storage location and ends with permanently recorded sample preparation details.

Action	Samples received → Weigh sample if applicable → Dilute
Inputs	
Data Type	
Responsible	
Comments	

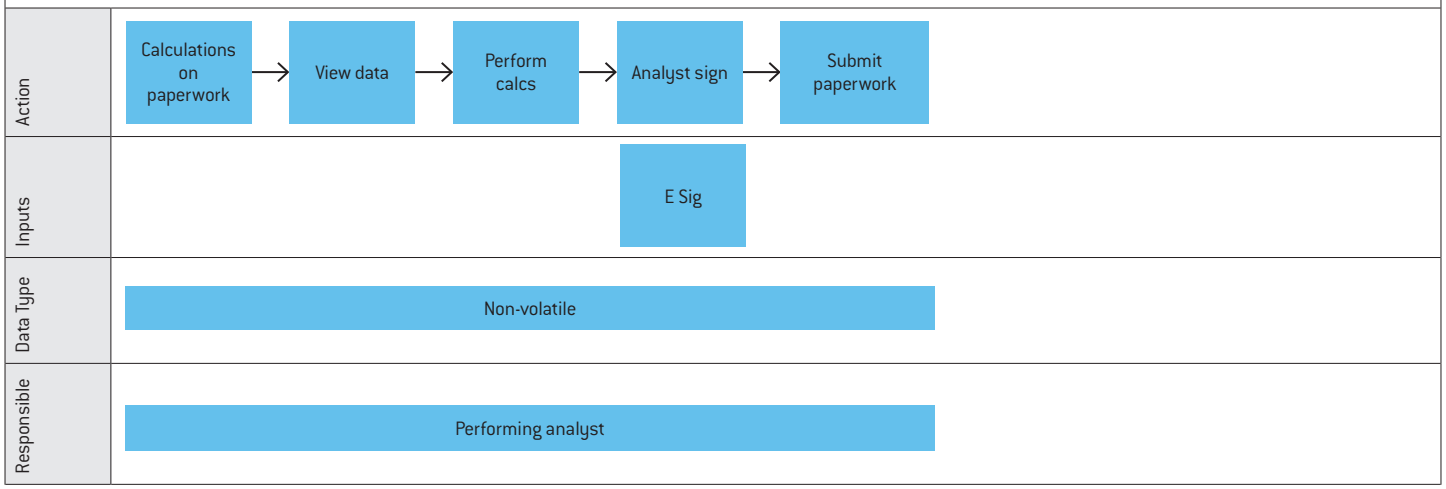
Data Acquisition Phase

Phase starts with prepared sample and ends with permanently data

Action	Setup template → Prepare plate + samples → Incubate → Prepare lysate → Add lysate → Start reading → Reading ends → Data saved automatically
Inputs	
Data Type	Non-volatile
Responsible	Performing analyst

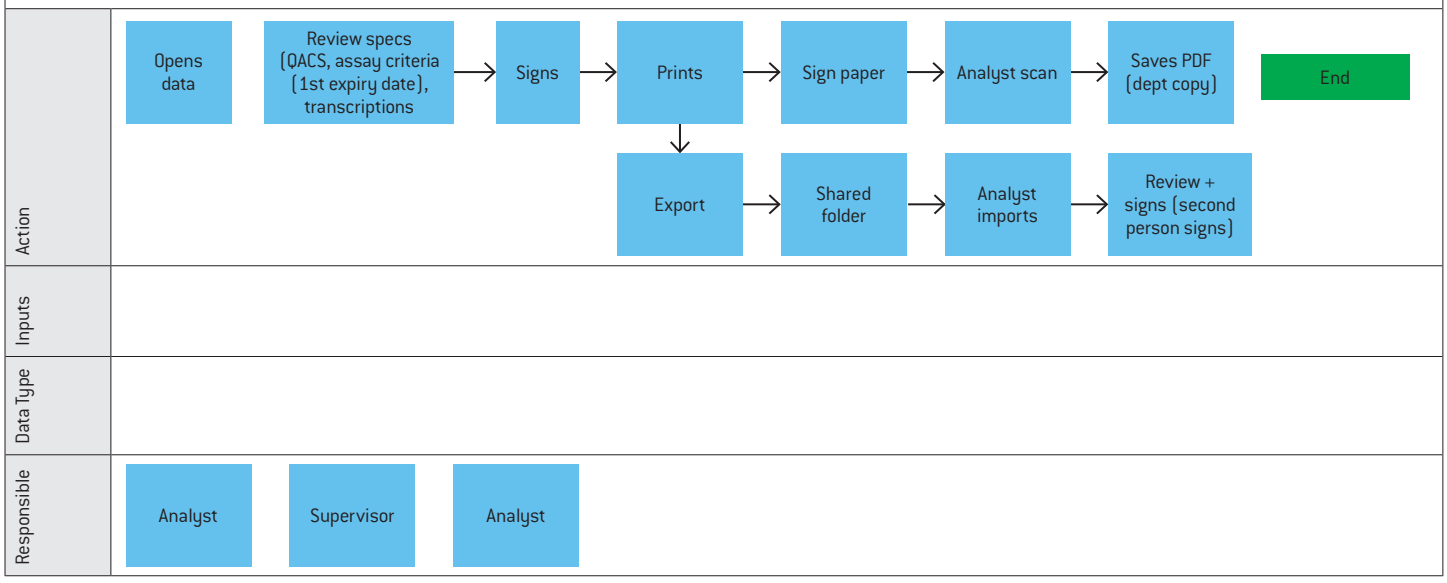
Data Processing Phase

Phase starts with viewing acquired raw data and ends with permanetly recorded reportable results



Data Review and Reporting Phase

Phase starts with submittal of the final version of the data and ends with data made available to stakeholders



Data Retention Phase

Phase starts with data is created and ends when retention period is reached

How to Build an Audit Trail and Data Review Process?

The whole purpose of an audit trail is to capture and preserve the integrity of changes during the process. With paper, the changes are obvious, you see the cross-outs, the person, the date/time, etc., and people understand this. Moving toward electronic systems, this understanding was missing because the "cross-outs" in many cases, are in the audit trail, and very often not in the printed final reports.

Before data integrity and CFR 21 Part 11 compliance, there had been no risk reduction, no risk acceptance, and no means of prioritization in review of audit trails.

So now in inspections, if you provide printed reports, the auditor can, and often will, ask for the audit trail behind it, because they are looking to see how well YOU understand how changes are managed in your process. A lot of times, this has a lot more to do with being able to demonstrate how you review your sample and testing information, rather than the technical audit trail. So the key is to have **SOPs in place detailing the data life cycle, the data review process, including the audit trail, and have a demonstrable training and understanding of the process.**

Ultimately, a well-designed electronic system allows you to validate against this SOP and review your data on a day-to-day basis by exception. In other words, if your system enforces the basic capture of the metadata and raw data in accordance with your SOPS, and you can prove it, then your reviews can focus on what goes wrong in your process, such as an over limit event, versus deviations to your data-capture process, which should be a lot more frequent on a paper system. With high sample volumes in the thousands, such as in EM (environmental monitoring) or water monitoring, review by exception is critical.

Criteria to Build an Audit Trail Review by Utilizing a FMEA: Failure Mode and Effects Analysis

The goal is to create a risk assessment that is: quantifiable, objective and actionable. We took into account the possible measures that can be taken to reduce the risk to data integrity. We first should build an FMEA risk assessment for data integrity based on the possible measures.

Based on our experience, we wanted to create a risk assessment process that is quantifiable, objective and most importantly actionable. We took into account the possible measures that can be taken to reduce the risk to data integrity and we then built an FMEA risk assessment around those possible measures. And of course, at the heart of any FMEA there are failure modes.

Setting Up Priority and Building Risk into Audit Trail Review

- **High Risk** = A mechanism exists to detect the event before batch or material release
- **Medium Risk** = A mechanism exists to detect the event, but after batch or material release
- **Low Risk** = There is no mechanism to detect the event (e.g. for objective data)

	Failure Mode and Effects	Control Measures	Residual Risk	Assessment			Risk category	Action	Assessment			Risk Acceptance
				S	O	D			S	O	D	
1.	Sample weight is not recorded properly. Weight is recorded directly from balance and there is no printout of the value included with the paperwork	None	Incorrect sample weight would result in incorrect result	3	1	3	High	Printout sample weight from balance and attach to paperwork	3	1	1	Low
2.	Template or plate setup incorrectly	Process is defined by SOP. Template settings verified by reviewer	None	3	1	1	Low	None	3	1	1	Low
3.	Required incubation time not met	Software prohibits running if incubation time is not correct	None	3	1	1	Low	None	3	1	1	Low
4.	Incorrect calculated result on paperworK	Calculations verified by reviewer	None	3	1	1	Low	None	3	1	1	Low
5.	Template modification performed by analyst that impacts reported result	None	Template modification not visible to reviewer without checking audit trail	3	2	3	High	Implement audit trail review as part of review process. Define critical audit entries that need to be reviewed as part of the routine assay review	3	2	1	Medium

Mock example of using WinkQCL™ Endotoxin Detection and Analysis Software

We Can Set Up a Risk Assessment Framework

- Define acceptable level and unacceptable level
- Calculate score
- Define actions for score above acceptable level
- Recalculate score taking into account actions
- Repeat until score below acceptable level or risk accepted

This gives us the framework to consistently assess the risk to data integrity and perform standardized reassessments as the systems and processes change and evolve.

As with other risk assessment tools, we can now define the acceptable level of risk. We can perform calculations by taking into account the score by multiplying the factors and define remediation actions. By doing this, we take into account the actions and we can then recalculate the score and repeat the process until the risk is either reduced below the acceptable level or formally accepted. This gives us the framework to consistently assess the risk to data integrity and perform standardized reassessments as the systems and processes change and evolve.

Creating Periodic Reviews Based on your Levels of Risk

Timelines for periodic reviews can be based on the point system from the FMEA. High risk items should be reviewed at a much higher level vs. low risk items, due to criticality. With so much metadata to review, the low risk items could potentially be removed entirely.

Example of Suggested Review Frequencies for Software by Risk Class

Risk Class	Software categories of a system: Good Automated Manufacturing Process			
High	3 months	6 months	12 months	24 months
Medium	6 months	12 months	24 months	For cause
Low	24 months	36 months	For cause	For cause

To Summarize

All of our endotoxin systems produce vast amounts of information during use – how can we keep track? The system should be validated first. Define which data is critical to patient safety and regulatory compliance. Analyze the path of data in the system and the business process, specifically looking at the defined data flow. Identify areas of high risk to patient safety and compliance by looking for failure modes within each process in the data flow. Review the documented process flow to determine where risks to the data integrity exists. The key is to look for things that could go wrong either intentionally or unintentionally. The defined mitigation should address the risk and lower the risk value to an acceptable level. Before starting the risk assessment the scoring system, thresholds, and acceptable risk levels should be defined.

And again it boils down to the question:
"What can people do to compromise data integrity either intentionally or unintentionally?"

"The number of computerized data acquisition and processing systems in the pharmaceutical industry is growing quickly and with it the number of records generated that are inextricably linked with the regulated products manufactured by the industry. The situation is complicated by the integration of systems, interfaces between the systems, and conversions, calculations, and compression of information that may take place during transmission. The knowledge generated from these data and information is directly used in the manufacture of drugs.

Data integrity and its practical maintenance are therefore crucial to the safety of patients and the quality of healthcare products. By using a risk-based approach and the presented principles, it is possible to generate meaningful reviews and proof of data integrity."

References

http://www.pharmtech.com/risk-based-approach-data-integrity?pageID=2
By Kurt In Albon, Daniel Davis, PhD, James L. Brooks
Pharmaceutical Technology
Volume 39, Issue 7, pg 46–50

Data Integrity and Compliance With CGMP Guidance for Industry DRAFT GUIDANCE (Apr 2016) http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-drugs-gen/documents/document/ucm495891.pdf

Contact Information

North America

Customer Service: + 1 800 638 8174 (toll free)
order.us@lonza.com
Scientific Support: + 1 800 521 0390 (toll free)
scientific.support@lonza.com

Europe

Customer Service: + 32 87 321 611
order.europe@lonza.com
Scientific Support: + 32 87 321 611
scientific.support.eu@lonza.com

International

Contact your local Lonza distributor
Customer Service: + 1 301 898 7025
Fax: + 1 301 845 8291
scientific.support@lonza.com

International Offices

Australia	+ 61 3 9550 0883
Belgium	+ 32 87 321 611
Brazil	+ 55 11 2069 8800
China	+ 86 21 6340 3488
France	0800 91 19 81 (toll free)
Germany	0800 182 52 87 (toll free)
India	+ 91 22 4342 4000
Japan	+ 81 3 6264 0660
Luxemburg	+ 32 87 321 611
Singapore	+ 65 6521 4379
The Netherlands	0800 022 4525 (toll free)
United Kingdom	0808 234 97 88 (toll free)

Lonza Walkersville, Inc. – Walkersville, MD 21793

RT-SP011 08/17

www.lonza.com/pharmabiotech
www.lonza.com/winkqcl