ISO 17025 BLIND SPOT DIAGNOSTIC

Understanding the Operational Risks Evaluated in the Diagnostic

confience™

1. Introduction

In ISO/IEC 17025 laboratories, there is often a gap between what procedures describe and how operations actually function in practice. This gap is not always visible during routine work, but it becomes highly apparent under external scrutiny, particularly during accreditation audits.

This material was developed to **provide context for the ISO/IEC 17025 Blind Spot Diagnostic.** Its purpose is not to interpret the standard or explain compliance requirements. Instead, it outlines the **operational risk areas evaluated by the diagnostic** and explains why these areas are frequently challenged during audits.

Even experienced teams with a strong compliance history remain exposed to vulnerabilities that internal reviews may miss. The most common issues include:

- Data that cannot be fully reconstructed
- Evidence that exists, but is difficult to retrieve quickly
- Partial traceability across analytical stages
- Operational inconsistencies across departments
- Metrology weaknesses
- Difficulty defending technical decisions under auditor questioning

The sections that follow describe the most common operational blind spots observed during real internal and external ISO/IEC 17025 audits. These are the same areas assessed in the diagnostic and the same points where laboratories are most often required to defend how work was performed.

Reviewing this material before completing the diagnostic will help you interpret the questions accurately and assess your operation based on how it actually performs, rather than how it is intended to perform.

About the Author

Raphael Pimenta has supported industrial and service laboratories in strengthening traceability, improving data integrity, and preparing for ISO/IEC 17025 accreditation audits. He has participated in digital transformation projects that helped labs reduce nonconformities, consolidate audit evidence, and improve operational consistency.

This Diagnostic consolidates recurring findings observed in real internal and external audits, focusing on issues that frequently challenge accredited laboratories.

Raphael Pimenta

Chemical Engineer · ISO/IEC 17025 & Laboratory Digitalization Specialist.

2. ISO/IEC 17025
Risk Pillars

Most ISO/IEC 17025 nonconformities do not result from misunderstanding the standard. They emerge from operational gaps that develop gradually over time, such as fragmented records, weak evidence management, and informal deviations from documented procedures.

The pillars below represent **the core operational risk areas evaluated in the ISO/IEC 17025 Blind Spot Diagnostic.** These areas are consistently identified during accreditation audits conducted by bodies such as **ANAB, A2LA, NVLAP, and SCC,** including in laboratories with mature quality systems.

As laboratory operations grow and evolve, procedures and systems do not always adapt at the same pace. Workarounds become normalized; evidence becomes more difficult to reconstruct, and audits reveal issues that daily operations often conceal.

PILLAR 1 – Data Integrity & Reliability

Data integrity is one of the most sensitive areas of ISO/IEC 17025. Many findings relate to how information is recorded, corrected, accessed, and retained across the analytical lifecycle.

Risk 1 — Manual records without document control

Uncontrolled notebooks or worksheets without versioning, authorship, or defined storage make it difficult to demonstrate when data was generated and who was responsible for it.

Key question: Do all manual records have controlled identification, versioning, and access management?

Risk 2 — Corrections without traceable change history

Unjustified corrections, erasures, or “cleanup” behavior can be interpreted as data manipulation.

Key question: Is every correction dated, signed, justified, and fully traceable?

Risk 3 — Evidence scattered across systems

When raw data, validations, and results are split across paper, spreadsheets, emails, and shared drives, reconstructing a complete test becomes difficult—or impossible.

Key question: Is technical evidence centralized, current, and properly linked?

Risk 4 — Uncontrolled access and weak segregation of duties

If users can edit, delete, or overwrite records freely, data integrity and impartiality are compromised.

Key question: Are user roles, permissions, and access logs clearly defined and enforced?

PILLAR 2 – End-to-End Process Traceability

Traceability requires coherence between sampling, testing, calculations, approvals, and reporting. Any break in the chain can compromise result validity.

Risk 5 — Loss of traceability during re-testing

Repeat tests without documented justification—or without preserving original data—prevent full reconstruction.

Key question: Can you show why, by whom, and under what conditions a test was repeated?

Risk 6 — Poor sample identification

Duplicate, illegible, or non-unique labels jeopardize chain of custody and reliability.

Key question: Does every sample have a unique identifier traceable through to the final report?

Risk 7 — Missing environmental condition records

Critical conditions such as temperature and humidity are often assumed rather than documented, impacting technical validity.

Key question: Is there documented evidence of environmental conditions for each analysis?

Risk 8 — Unclear responsibility attribution

Generic or collective sign-offs blur technical accountability.

Key question: Can you clearly identify the analyst, reviewer, and approver for each result?

PILLAR 3 – Impartiality & Operational Consistency

Impartiality extends beyond conflict-of-interest declarations. It reflects the laboratory's ability to demonstrate consistent, objective decision-making backed by evidence.

Risk 9 — No formal impartiality risk assessment

Without documented risk analysis, conflicts may remain unmanaged.

Key question: Do you maintain a formal, documented impartiality risk assessment?

Risk 10 — Internal audits not risk-based

Calendar-driven audits often miss high-risk processes.

Key question: Are internal audits planned based on risk, performance, and past findings?

Risk 11 — Procedures disconnected from real practice

Misalignment between documented procedures and actual operations is a leading cause of nonconformities.

Key question: Do your procedures reflect current laboratory practice?

PILLAR 4 – Metrology & Critical Equipment

Metrology control is central to ISO/IEC 17025. Gaps in this area frequently escalate into major findings.

Risk 12 — Use of out-of-tolerance / nonconforming equipment

Relying on equipment solely because a calibration certificate is "still valid" can invalidate entire datasets.

Key question: Does your system actively prevent the use of nonconforming equipment?

Risk 13 — Missing intermediate checks

Without documented evidence, equipment suitability at the time of testing cannot be demonstrated.

Key question: Is there signed, timestamped evidence of each intermediate check?

Risk 14 — Calibration not representative of real use

If calibration conditions do not reflect actual operating conditions, measurement validity may be compromised.

Key question: Do calibration conditions accurately reflect real laboratory use?

PILLAR 5 – External Audit Readiness

Technical quality is not enough. During audits, the ability to present evidence clearly and efficiently is critical.

Risk 15 — Improvised evidence during the audit

Searching for information in real time signals lack of operational control to auditors.

Key question: Is required evidence readily accessible and well organized?

Risk 16 — Conflicting document versions

Multiple versions across paper, spreadsheets, and systems indicate document control failure.

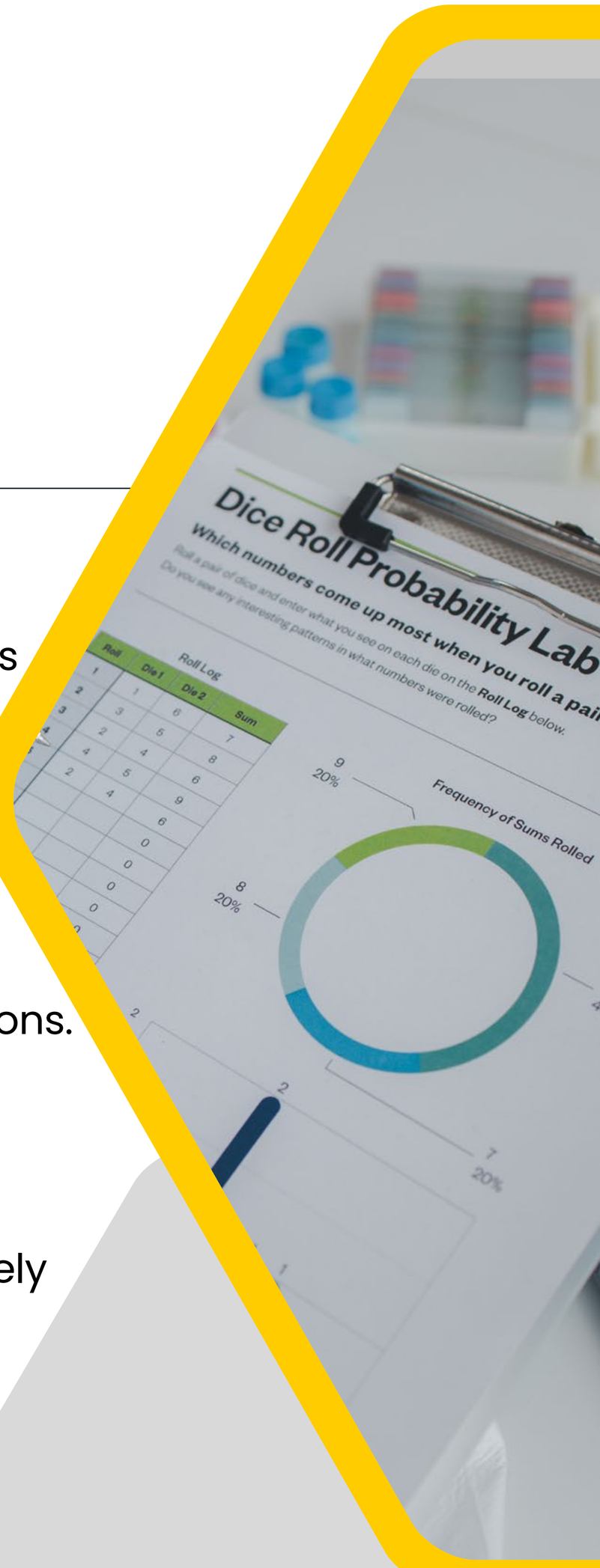
Key question: Do you have full traceability of document versions and approvals?

Risk 17 — No post-audit review process

When audit outcomes are not analyzed, the same findings tend to repeat.

Key question: Do you have a formal post-audit review and improvement process?

3. Preparing for the Diagnostic



The diagnostic that follows is designed to be completed quickly and without preparation. Each question corresponds directly to the operational risk areas described in this document.

When answering, focus on how your laboratory currently operates in practice, not on how procedures are written or how processes are intended to function under ideal conditions. Consider situations where auditors request evidence, trace decisions, or challenge assumptions during an audit.

The value of the diagnostic result depends on how accurately your responses reflect real operational behavior.

Results Interpretation

Your final score ranges **from 0 to 34.** This scale reflects your laboratory's level of **operational exposure** based on how controls are established and applied in practice.

Score Ranges

27 – 34 | ● Low Risk

Strong level of operational control and traceability.

Most controls are formally established, consistently applied, and supported by reliable evidence.

17 – 26 | ● Moderate Risk

Relevant gaps in consistency or control.

Some processes rely on partial controls, key individuals, or dispersed evidence and may be challenged under external review.

0 – 16 | ● Critical Risk

High operational exposure.

Controls are largely informal or not established, making traceability and defensibility difficult to demonstrate.

What happens next?

- You will receive your score by email
- You can identify which operational pillars present the highest exposure
- If helpful, you may connect with a technical specialist from our team to review your results and discuss how these gaps can be addressed using **myLIMS.**

4. The Moment of Truth

You are now ready to evaluate your operation across the ISO/IEC 17025 risk areas outlined in this material.

The ISO/IEC 17025 Blind Spot Diagnostic generates your results automatically based on how operational controls are established and applied in practice.

Discover your blind spots

Start the ISO/IEC 17025 Blind Spot Diagnostic

Note: *This diagnostic is an operational risk assessment tool intended to support internal improvement efforts. It does not constitute an accreditation decision or legal advice.*

myLIMS — Reducing ISO/IEC 17025 Blind Spots

The blind spots outlined in this diagnostic, including fragmented records, traceability gaps, operational inconsistencies, and metrology weaknesses, do not stem from lack of expertise or intent. They typically emerge as laboratory operations scale beyond the controls originally designed to support them.

Many laboratories already operate with a LIMS. However, audit challenges rarely arise from the absence of a system. They arise when data, processes, and technical decisions cannot be **reconstructed clearly and consistently under audit pressure.**

myLIMS is designed to address this gap by enforcing operational discipline across data, decisions, and evidence. It helps ensure that what happened can be understood and defended without relying on individual explanations or improvised reconstruction.

Rather than replacing existing systems, **myLIMS** strengthens how evidence is governed, connected, and made visible as operational complexity increases.

How myLIMS supports laboratory operations:

- Reduces parallel records by enforcing a single source of controlled evidence
- Protects data integrity with complete, usable audit trails and version control
- Enables end-to-end reconstruction of the sample lifecycle when required
- Standardizes records to reduce rework and interpretation gaps
- Supports metrology control and helps prevent the use of nonconforming equipment

Built as a true SaaS platform, **myLIMS** enables laboratories to strengthen operational defensibility without adding infrastructure overhead, supporting more consistent and sustainable ISO/IEC 17025 operations.

Start the ISO/IEC 17025 Blind Spots Diagnostic

myLIMS™

by confience

sales@confience.io

confience.io