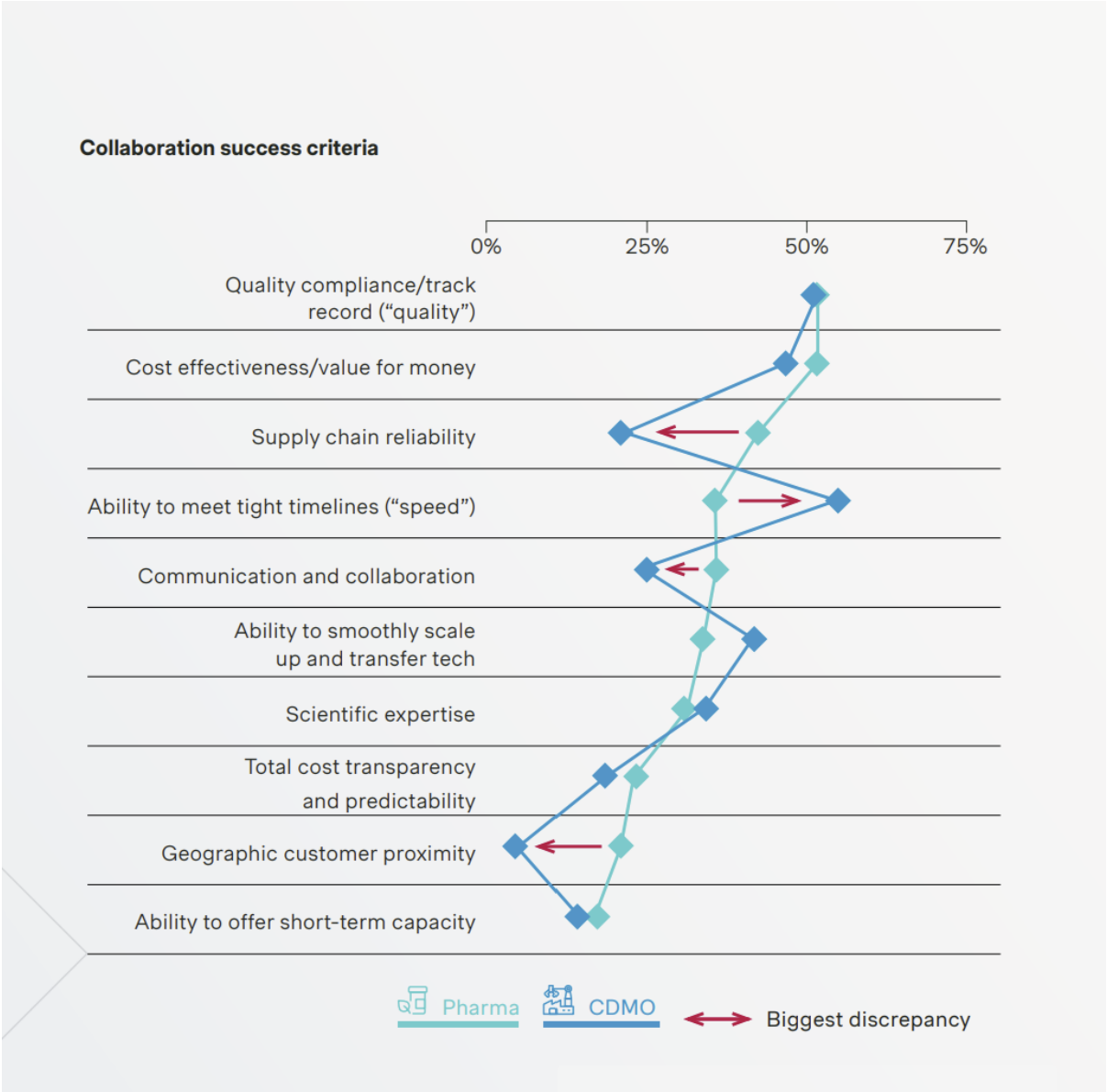
Technical Deep Dive : Tech Transfers, Equipment Choice and Productivity

This is an article written jointly by Pharmagro and Terriva. We focus on the importance of closing the gap between assumed capacity and actual performance. We start at a high level on the need for robust processes and then deep dive into one technical area, powder blending.

In their report *CDMO Growth Report 2025*, the consultancy Simon Kucher assessed the elements that make for successful collaboration between pharma companies and CDMOs. The graph shows how each side rated ten criteria. Interestingly the CDMOs overestimated the need for speed (ability to meet tight deadlines) while underestimating supply chain reliability. Both sides were in close agreement on the need for smooth scale up.



Source : *CDMO Growth Report 2025* Simon Kucher

Having sat in board meetings and seen the consequences of failed PPQs or late tech transfers, we will cover broad topics of the trade-off between speed and reliability, and will deep dive into examples of equipment choice.

The five articles will cover

1. Audit Ready By Design – What CDMOs miss about CFR21 in Equipment Selection
2. Tech Transfer and Process Inconsistency – The Example of Blending
3. Speed – Not At Any Cost
4. Containment & Control
5. Scaling from R&D to Commercial

Terriva provides state of the art powder blending equipment and control systems. Pharmagro provides software and services for business development and portfolio management. Both companies share a data driven approach to scaling up, whether it is equipment or processes.

Article 1 – Audit Ready By Design – What CDMOs miss about 21 CFR compliance in equipment selection

There are considerable capacity expansions being announced by CDMOs, particularly in the areas of high spec small molecule manufacturing and sterile fill / finish. Installation of the equipment is one thing, but as important are the software, process controls and training of the operators.

The Illusion of Compliance

Most Contract Development and Manufacturing Organisations (CDMOs) believe they are 21 CFR Part 11 compliant.

Until an audit proves otherwise.

The assumption is simple:
If the software is compliant, the system is compliant.

But auditors don't assess software in isolation.
They assess **system behaviour, data integrity, and how equipment performs in real-world conditions**.

That's where the gap exists.

And it's why compliance failures are often discovered not during validation — but under audit pressure.

The Core Misconception: "Compliance is a Software Layer"

21 CFR Part 11 is frequently treated as a feature set:

- Electronic signatures
- User access controls
- Data storage

But the reality is more demanding:

"Can your system prove, without ambiguity, what happened, when it happened, and who was responsible?

That is not just software.
That is **how the system is designed, integrated, and controlled**.

If the underlying equipment and control architecture don't support this — compliance is fragile at best.

What Auditors Actually Test

Audits are not theoretical exercises.
They are designed to expose weaknesses in real-world operation.

Auditors will typically focus on:

Data Integrity (ALCOA+)

"Data integrity ensures that data remains accurate, complete, and reliable throughout its lifecycle. In pharmaceutical manufacturing, this is supported by the ALCOA+ principles, which require data to be attributable, legible, recorded at the time of activity, original, and accurate—ensuring it can be trusted for audits and decision-making.

- Is data attributable, legible, contemporaneous, original, and accurate?
- Can data be altered without trace?

Audit TRails

- Are all critical process parameters automatically recorded?
- Are changes logged in real time?
- Can records be edited, overwritten, or deleted?

User Permissions & Access Control

- Are roles clearly defined and enforced?
- Is there segregation of duties?

- Are actions traceable to individuals?

System Behaviour Under Operation

- Does the system enforce process parameters?
- Can operators override steps without traceability?
- Are deviations captured and justified?

Data Retention & Retrieval

- Can batch records be retrieved quickly and securely?
- Is data protected, backed up, and exportable?

The key point:
Auditors are not checking if a system *can* be compliant —
they are testing whether it *is compliant in practice*.

Where CDMOs Get Caught Out

Most compliance gaps don't come from intent.
They come from **equipment decisions made without fully understanding downstream risk**.

Common issues include:

- **Incomplete audit trails** (manual inputs, non-continuous data capture)
- **Weak access control** (shared logins, untracked overrides)
- **Disconnected systems** (manual data transfer, multiple data sources)
- **Unenforced processes** (operators able to adjust parameters without trace)

These gaps are rarely visible at purchase stage.

But they become highly visible during an audit.

The Real Issue: Compliance Risk is Introduced at Selection

In CDMO environments, equipment decisions are rarely isolated.

They must support:

- Multiple customers
- Multiple product types
- Varying regulatory expectations
- Long lifecycle requirements

Which means:

“Every equipment decision carries portfolio-level risk.

Pharmagro Perspective: Compliance Risk Starts at the Investment Decision

From Pharmagro’s perspective, 21 CFR Part 11 is not just a validation topic.

It is a strategic risk consideration embedded within portfolio and investment decisions.

Before equipment is selected, CDMOs should be asking:

- Is this system aligned with the molecules and processes we intend to support?
- Does it introduce hidden compliance or scale-up risk?
- Can it deliver consistent, repeatable performance across multiple programmes? How will this impact timelines, regulatory exposure, and commercial outcomes?

Because in practice:

“Compliance failures are often a symptom of earlier investment decisions.”

Through technical due diligence and portfolio-level thinking, Pharmagro help CDMOs identify where:

- System design may compromise data integrity
- Control limitations may introduce future audit exposure
- Equipment-process misalignment may lead to inconsistency at scale

In a CDMO model, where flexibility and speed are critical, these risks compound quickly.

Terriva Perspective: Engineering Compliance Into the System

Once the right investment decision is made, compliance must be **engineered into the equipment itself**.

From Terriva’s standpoint, 21 CFR Part 11 readiness is not an add-on — it is built into:

Control System Architecture

- Secure, tamper-evident audit trails
- Role-based user access
- Electronic records and signatures aligned to regulatory expectations

Process Enforcement

- Defined recipes with locked parameters
- Controlled operator interaction
- Full traceability of any deviation

Data Integrity by Design

- Automated, continuous data capture
- Secure storage and structured export
- Integration-ready systems for wider digital environments

This ensures that the system doesn't just perform — it can **prove compliance under scrutiny**.

Key Insight: Compliance Isn't Added Later — It's Engineered In

This is the shift CDMOs need to make.

21 CFR Part 11 is not:

- A software upgrade
- A validation exercise
- A documentation process

It is a **system-level design principle**.

And the earlier it is addressed, the lower the risk. Furthermore, the use of Artificial Intelligence in manufacturing requires a base of reliable data that can be kept up to date. Therefore, 21 CFR compliance is an important contributor to this.

Practical Questions CDMOs Should Be Asking

Before selecting equipment, ask:

- Can this system **demonstrate data integrity under audit conditions?**
- Are audit trails **automatic, secure, and tamper-evident?**
- Is user access **fully controlled and traceable?**
- Does the system **enforce process discipline, not rely on operator behaviour?**
- Will this system **support multiple products and regulatory expectations over time?**

If any of these answers are unclear —
you are introducing risk into your operation.

Conclusion: Designing for Audit, Not Just Operation

In today's CDMO landscape:

- Regulatory scrutiny is increasing
- Customer expectations are rising
- Data integrity is non-negotiable

The difference between passing and failing an audit is rarely effort.

It is design.

"Audit-ready systems are not built during validation.
They are defined at the point of investment — and engineered at the point of delivery.

Joint Positioning

- **Pharmagro** support CDMOs in making the right investment decisions by identifying **portfolio, technical, and compliance risk upfront**
- **Terriva** ensures those decisions are realised through **equipment engineered for audit-ready performance**

Pharmagro define the risk. Terriva engineer it out.

If you are reviewing your equipment strategy or planning future investment:

Speak to Pharmagro and Terriva about building systems that don't just perform — but stand up to audit.

nick@pharmagro.co.uk andy.brookes@terriva.com

May 2026