Pharma M&A Due Diligence: A Guide to IT System Assessment

By InuitionLabs.ai • 10/17/2025 • 50 min read

pharmaceutical m&a | it due diligence | technology assessment | biotech m&a | ma integration | regulatory compliance | cybersecurity due diligence

Executive Summary

Mergers and acquisitions in the pharmaceutical sector have surged in recent years, driven by factors such as looming patent expirations, the need to replenish pipelines, and the search for novel technologies. In 2023 alone, global pharmaceutical and biotech M&A deal values jumped markedly – Axios reports a 38% increase in pharma and 45% in biotech deal value compared to the prior year (www.axios.com). Major transactions in 2023 included Pfizer's $43.0 billion acquisition of Seagen (the year's largest pharma deal) (www.axios.com) and Bristol-Myers Squibb's $18.1 billion of acquisitions (www.axios.com). By 2025, industry observers forecast an M&A boom (over $4 trillion globally anticipated) as strategic urgency increases (www.reuters.com) (www.reuters.com). Against this backdrop, **comprehensive due diligence** has never been more critical to capture the expected synergies and avoid costly surprises. In particular, IT system and technology due diligence must be integral to the process: failure to thoroughly review IT assets and infrastructure can imperil the combined entity's operations and value. Industry experts warn that neglecting technological compatibility and underestimating integration complexity are common causes of deal failure (www.fiercehealthcare.com) (www.researchgate.net).

In practice, due diligence provides a deep examination of the target's assets, including technology platforms, data, cybersecurity, and compliance status, so that buyers understand exactly what they are purchasing (windsordrake.com) (www.researchgate.net). This ensures that hidden risks (such as outdated systems, compliance gaps, or integration difficulties) are identified and quantified before closing. For example, one ISACA Journal study found that acquirers with strong IT integration capabilities achieved *significantly higher* post-merger performance (www.researchgate.net), underscoring the value of diligent technical assessment. By contrast, poorly executed M&A can lose value: a 2003 KPMG survey found ~70% of deals failed to deliver expected objectives (businesslawtoday.org), often due to oversight of operational and IT factors. Even financial regulators now stress rigorous IT/compliance scrutiny, with the U.S. Department of Justice advising that thorough "pre-M&A due diligence" is a marker of a sound compliance program (businesslawtoday.org).

This report provides an in-depth exploration of pharmaceutical M&A due diligence with a focus on IT system assessment. It begins with background on the pharmaceutical M&A landscape and the role of due diligence, then delves into the unique challenges of examining IT in this sector. Key areas for review (from infrastructure and applications to data governance, cybersecurity, and regulatory compliance) are discussed in detail, drawing on case studies and expert analyses. We also present evidence from studies and industry sources to quantify the importance of technology diligence, and outline best-practice frameworks and checklists. Finally, the report considers future trends – such as digital transformation and AI – that will shape how IT is evaluated in deals. All claims are supported by citations to authoritative sources throughout.

Introduction

Pharmaceutical mergers and acquisitions (M&A) are major strategic moves aimed at combining capabilities, boosting R&D pipelines, and achieving economies of scale. The industry's complex regulatory environment and heavy investment in R&D and manufacturing systems, however, make such transactions especially challenging. Effective **due diligence** is crucial to ensure a deal creates rather than destroys value. Due diligence is the comprehensive appraisal of a target company – financial, legal, regulatory, and operational – that a buyer must perform before closing an acquisition. In highly regulated sectors like pharma, due diligence often extends beyond the surface financials to detailed technical and compliance reviews. In particular, *IT system due diligence* has emerged as a vital component: the acquiring company must inventory and evaluate all of the target's information technology assets, from infrastructure and software to data and cybersecurity, to avoid crippling integration issues post-merger (windsordrake.com) (www.researchgate.net).

This report examines the role of IT system assessment within pharmaceutical M&A due diligence. We first place current activity in context by reviewing recent M&A trends in the industry and the goals of due diligence. We then analyze why technology review is often neglected and why it is so important to success, drawing on studies and high-profile examples. Next, we detail the main domains of IT needling – notably infrastructure, applications, data, security, and compliance – and how to evaluate them in a pharma context. Throughout, we incorporate case examples and data (e.g. actual deal values, survey findings) to ground our discussion. Finally, we explore implications for integration planning and look ahead at how emerging technologies will influence due diligence. The aim is to provide a thorough, practitioner-oriented resource on assessing IT in pharma M&A, backed by evidence from industry research and expert sources.

1. Pharmaceutical M&A: Background and Trends

M&A has long been a strategic lever in the pharmaceutical and biotech industries. Companies often pursue deals to acquire new drug pipelines, achieve scale, diversify portfolios, or access cutting-edge technologies. In recent years, dealmaking has remained robust despite broader economic headwinds: according to the London Stock Exchange Group, global pharma and biotech M&A deal value in 2025 reached $105.3 billion – a 7% increase year-over-year and the highest since 2023 (www.reuters.com). In 2023, healthcare deal values surged 38% in pharma and 45% in biotech versus the prior year, even as the total number of deals slightly declined (www.axios.com). These figures underscore the high stakes involved: blockbuster acquisitions such as Pfizer's $43 billion purchase of cancer drugmaker Seagen (the largest pharma acquisition of 2023) and Bristol-Myers Squibb's $18.1 billion spending spree highlight the enormous capital at play (www.axios.com) (www.axios.com).

Looking at deal drivers, fiscal pressures (e.g. patent cliffs on top-selling therapies such as Humira) and intense competition have spurred large transactions.For example, AbbVie's 2019 $63 billion bid for Botox-maker Allergan was explicitly aimed at offsetting revenue declines as biosimilars threatened its flagship Humira (apnews.com). Similar motives animate many deals: business leaders in 2025 expect major pharma players (Merck, Johnson & Johnson, Novartis, etc.) to pursue acquisitions to shore up pipelines and revenue (www.reuters.com) (www.reuters.com). Geographic expansion is also a factor – an increasing number of pharma giants are seeking assets in emerging markets, especially China, to capture growth. In mid-2024, for instance, global companies like AstraZeneca and Novartis sought Chinese biotech targets, with deals such as AstraZeneca's $1.2 billion acquisition of Gracell Biotechnologies (www.reuters.com). Despite geopolitical and regulatory hurdles, the strategic interest in those markets remains high.

While recent years have seen huge deals, the overall number of megacaps (>$5B) dipped temporarily in 2024 (www.reuters.com), but analysts forecast a rebound. At the 2025 JPMorgan Healthcare Conference, industry executives observed that 2024 had no pharma deal above $5 billion (a first in a decade) but expected that, with relaxed antitrust oversight and supportive macroeconomics, deals above $10 billion would quickly re-emerge (www.reuters.com). In summary, the pharmaceutical M&A landscape is characterized by high valuations, regulatory complexity, and strategic urgency. Buyers hope to capture synergies and innovation, but as history shows, even marquee deals can go awry if not carefully executed.

2. Due Diligence in M&A

2.1 Purpose and Scope of Due Diligence

Due diligence is the cornerstone of any M&A process. It is the buyer's opportunity to "take a magnifying glass" to the target, verifying facts and uncovering risks before finalizing an agreement. As one legal analysis succinctly notes, the key to M&A success is due diligence: the process "identifies issues that may reduce the price of the target company", validates its assets and contracts, and helps shape the purchase agreement (businesslawtoday.org). In practice, diligence encompasses multiple areas: **financial review** (e.g. auditing books, liabilities, forecasts), **legal/regulatory review** (e.g. compliance with laws, pending litigation), **commercial review** (market position, customers), and **operational/technical review** (assets and processes). In pharmaceutical deals, **quality and regulatory compliance** due diligence is particularly emphasized: any unresolved FDA or GMP violations, for instance, can critically affect deal value (arriello.com). Indeed, a recent American Bar Association guide emphasizes that in pharma M&A, due diligence must often be tailored to focus on FDA and HHS-regulated aspects, such as drug approvals, clinical trial records, and HIPAA compliance (businesslawtoday.org) (businesslawtoday.org).

Statistical studies offer perspective on the stakes. A widely-cited 2003 KPMG survey (across industries) found that nearly 70% of acquisitions failed to meet the acquirers' objectives (businesslawtoday.org). Many observers attribute such failures to gaps in diligence. For example, analysts lament that firms routinely overestimate synergies and enter deals without enough data. McKinsey reported that buyers often have "little data about the target" and limited access to its people and systems when estimating value (www.mckinsey.com). This "information asymmetry" means misplaced confidence: on average acquirers tend to pay a premium (10–35% of the target's value) that often materializes benefits for the seller (www.mckinsey.com). In short, without thorough due diligence, an acquirer can be blindsided by hidden problems – ranging from overstated revenues to incompatible systems.

In response to these risks, regulators have begun to insist on diligent review. The U.S. Department of Justice (DOJ) now explicitly expects companies' compliance programs to include "appropriate scrutiny" of acquisition targets (businesslawtoday.org). Its 2023 guidance on corporate compliance highlights that merging firms must "complete pre-acquisition due diligence and identify misconduct or risk of misconduct", using qualified professionals familiar with FDA-regulated businesses (businesslawtoday.org). In other words, regulators view diligence as a compliance litmus test. For buyers, this means that not only financial and legal aspects, but also quality, safety, and IT-related controls should be in scope.

2.2 Consequences of Inadequate Due Diligence

Failing to conduct comprehensive due diligence can be disastrous. In healthcare M&A, poorly vetted deals often implode over operational mismatches or cultural conflicts. For example, Fierce Healthcare describes two "major mistakes" commonly made: first, an "inaccurate, deliberate and judicious assessment of operating risk" (which encompasses technology) (www.fiercehealthcare.com); second, flawed post-merger integration that fails to realize projected synergies (www.fiercehealthcare.com). The advice is clear: understanding the combined organization's people, roles, and technology compatibility up front is imperative; otherwise, planned cost savings and efficiencies may evaporate.

High-profile failures underline this lesson. The infamous 2000 AOL–Time Warner merger, often cited as the archetype of M&A folly, was later blamed partly on failed due diligence. Analysts noted that the deal's valuation ignored dramatic shifts in technology (AOL's dial-up model was already obsolete) and uncovered accounting fraud after closing (www.ansarada.com). Ansarada's post-mortem of that deal explicitly cites "failure of due diligence processes to surface business risks" as a key reason for the ultimate $98 billion write-down (www.ansarada.com). While not a pharmaceutical example, the AOL–Time Warner case illustrates how incomplete diligence (financial or technological) can decimate even a much-lauded merger.

In pharmaceuticals and healthcare, regulatory stumbles can also kill deals. The 2014 attempted brick-and-mortar merger of two Idaho health systems collapsed when antitrust litigation

emerged – a cautionary tale of overlooking legal and compliance risks (www.fiercehealthcare.com). Other missteps have occurred post-merger: observers note that executives often promise synergy numbers (e.g. 2% cost savings) that turn out over-optimistic, quietly falling short after integration (www.fiercehealthcare.com). Perhaps the single most alarming risk is inheriting non-compliance: a buyer may plan a deal worth billions, only to discover the target's manufacturing or trial data systems do not meet regulatory standards, forcing delays or even product withdrawals.

One illustrative story from IT risk literature involves a bank merger where technology was an afterthought. In this example, the acquiring bank's executives focused solely on cost synergies and business restructuring, "but neither IT nor a CIO was actively involved in the pre-merger due-diligence process or consulted in advance on comprehensive post-merger integration planning" (www.researchgate.net). The result? Two years after closing, the combined banks still had not integrated their systems (www.researchgate.net). Such integration gridlock delayed realizing any synergy from the deal. This underscores that neglecting IT during due diligence creates serious operational drag.

In short, research and industry accounts strongly suggest that transactions in which **IT and operational due diligence are thorough** fare much better than those where it is cursory or absent. An analysis of 141 Fortune-1000 acquisitions confirmed this point: firms with "high levels of IT integration capabilities" (implying good tech diligence and planning) achieved "significantly higher" combined firm performance in both short and long term (www.researchgate.net). Conversely, leaving technology to "post-merger" planning (or ignoring it entirely) invites the pitfalls seen in these cautionary examples.

3. The Unique IT Landscape of Pharmaceuticals

Before detailing how to assess IT systems in pharma M&A, it is important to understand what "IT" means in this context. Pharmaceutical companies employ a broad set of specialized information systems to support their operations – far beyond the generic business applications that might be found in other industries. Key categories include:

- **Enterprise Resource Planning (ERP).** Large pharma firms typically have enterprise-wide ERP platforms (e.g. SAP ERP or Oracle) that coordinate supply chain, procurement, finance, and often human resources. These systems are central to operational efficiency. During due diligence, ERP landscapes (number of instances, customization level, module suite) must be inventoried.

- **Manufacturing Systems (MES, SCADA).** Manufacturing Execution Systems (especially those conforming to ISA standards) monitor and control the production floor. MES and related SCADA (Supervisory Control and Data Acquisition) systems are crucial for pharmaceutical manufacturing. They govern batch processing, equipment parameters, quality tracking and produce electronic batch records. Proper integration of MES with ERP and LIMS (laboratory information management) systems ensures real-time compliance data. For example, a merged PharmaTech analysis noted that with integrated MES–ERP–LIMS, "electronic batch records" allow swift FDA audit responses – one site cut its review cycle-time from 36 hours to 4 hours (www.pharmtech.com). By contrast, disjointed MES/ERP environments can make compliance audits a "considerable effort" as data must be manually gathered (www.pharmtech.com). Because manufacturing compliance is non-negotiable in pharma, due diligence must carefully assess the state of MES and associated systems.

- **Laboratory and R&D Systems.** Research-intensive companies rely on sophisticated lab informatics: LIMS for chemical and biological testing, ELN (Electronic Lab Notebook) systems, statistical software for analytics, and sometimes specialized simulation or design software. Data generated in R&D – including from high-throughput screening, clinical trials, and preclinical experiments – is a critical asset. These systems often produce large, sensitive datasets that must be migrated or integrated post-transaction.

- **Quality Management Systems (QMS).** Pharma companies maintain QMS software to document SOPs, deviations, CAPA (corrective action/prevention), and audits (e.g. TrackWise, MasterControl). The effectiveness of a QMS impacts regulatory compliance. Due diligence should check whether the QMS is up-to-date, covers all regulated processes, and has no legacy gaps.

- **Clinical Data Systems.** Biotech and pharma companies often have clinical trials underway. EDC (Electronic Data Capture) systems, clinical trial management systems (CTMS), and pharmacovigilance systems (e.g. ArisGlobal or Argus for safety monitoring) are in use. The integrity of patient data in trials and post-market surveillance records must be assured (and are subject to HIPAA and global privacy laws).

- **Other Enterprise Applications.** Like any large corporation, pharma chains use CRM for sales/marketing, document management systems, HRIS, and collaboration tools. However, their use is often intertwined with compliance: e.g. sales data must respect off-label marketing rules, HR data must comply with worker safety regulations, etc.

- **Infrastructure.** Many pharmaceutical companies operate global data centers or co-location facilities, though cloud adoption is increasing. For instance, HPC clusters may support computational chemistry or genomics. Data center location can be strategic (e.g. to comply with EU data rules). The network backbone is critical for linking manufacturing sites and labs. Cloud platforms (AWS, Azure, etc.) may also be used for both general IT and specialized platforms (e.g. cloud-based LIMS or collaboration tools).

- **Data Analytics and AI Tools.** Modern pharma is increasingly integrating advanced analytics, machine learning, and AI (for drug design, patient segmentation, etc.). If the target has proprietary AI models or data lakes, these represent additional assets (or risks) to evaluate in due diligence.

Given this rich IT environment, pharmaceutical M&A due diligence must cast a wide net. In particular, the pharmaceutical context adds constraints: systems must comply with stringent

regulations (good manufacturing/practice, FDA record-keeping rules, patient privacy laws, etc.) while also supporting innovation and large-scale manufacturing. Neglecting any of these dimensions can nullify the benefits of a deal.

For example, an article in *Pharmaceutical Technology* illustrates how integrated MES-ERP systems directly improve compliance: integrated data flows enabled one high-volume manufacturer to submit inspection data to the FDA "in minutes" instead of "considerable effort" (www.pharmtech.com). Likewise, at the research stage, digital traceability of clinical records required by regulations relies on robust IT systems. As Arriello's experts note, even a single FDA Warning Letter (for any violation) can "have a massive impact on company value" (arriello.com). Thus, as we will see, IT due diligence in pharma is as much about verifying compliance and data integrity as it is about pure technical compatibility or cost-savings.

Regulatory Context

Pharmaceutical M&A is governed by a host of regulatory frameworks, and IT systems are often central to compliance. Some key regulations and standards to keep in mind during IT due diligence include:

- **FDA 21 CFR Part 11 (Electronic Records and Signatures).** Applies to pharma systems that manage controlled records (e.g. batch records, clinical trial data). Systems must have audit trails, secure login, and validated functionality for e-signatures. Due diligence must verify that any critical systems are "21 CFR Part 11 compliant" – meaning they can produce reliable electronic documentation meeting FDA requirements.

- **GxP Regulations (GMP, GLP, GCP).** These Good Practice guidelines require that processes in manufacturing (GMP), laboratories (GLP), and clinical trials (GCP) meet standards. IT systems that support these areas (e.g. MES in manufacturing, LIMS in labs, EDC in trials) must be validated and monitored. For example, IT assessments often check that manufacturing software is validated under an FDA-style GAMP framework.

- **HIPAA and HHS Privacy Rules.** If the target handles patient data (e.g. clinical trial participants), then U.S. HIPAA rules apply (businesslawtoday.org). Due diligence must ensure protected health information is securely stored and accessed. This includes encryption, access controls, breach history, and business associate agreements.

- **GDPR (EU Data Protection).** For companies with EU operations or data, GDPR imposes strict rules on personal data. Compliance aspects include data residency, consent records, and privacy-by-design in systems. M&A diligence must thus ask whether personal data in IT systems is handled appropriately (e.g. has the target consented for use of EU patient data?).

- **ISO 27001 (Information Security).** Though not legally mandated, ISO 27001 (and related ISO 27799 for health) is often adopted by pharma firms. Certification means the firm has a formal InfoSec management system. In diligence, the presence of ISO 27001 or SOC2 reports can be strong evidence of security maturity, while the lack of any security standard should raise caution.

- **Healthcare-specific standards.** In the U.S., systems integration often uses HL7 standards for clinical data interchange; in labs, CDISC standards may apply. While not compliance per se, adherence to community standards can ease integration.

Table 1 (below) summarizes key IT compliance domains and due diligence focus areas in pharma M&A.

Standard / Regulation	Applicability to Pharma IT	Due Diligence Focus
FDA 21 CFR Part 11	Electronic records/signatures in FDA-regulated processes (e.g. manufacturing, trials)	Verify audit trails, e-signature capabilities, system validation plans
GxP (GMP/GLP/GCP)	Quality standards for manufacturing, labs, and clinical trials	Ensure IT systems (MES, LIMS, EDC) are validated and compliant with GxP; review audit history
HIPAA / HHS Privacy Rules	Protection of patient health information in trial or medical data	Check encryption, access controls, data handling practices; confirm breach management
GDPR (EU Data Protection)	Protection of personal data in EU operations	Assess data residency of systems, consent management, third-party processors
ISO 27001	International information security standard	Look for formal ISMS scope, recent audits/certification reports
Other healthcare standards (HL7, CDISC)	Data exchange/structure in clinical and lab domains	Evaluate data integration standards, compatibility with acquirer's systems

Table 1: Analytical focus areas for IT compliance and regulatory standards in pharmaceutical M&A due diligence.

Citations: We note that due diligence checklists for pharma explicitly include checking HIPAA and data security provisions (businesslawtoday.org), as well as laboratory and manufacturing compliance systems. Integrated IT systems (e.g. MES–ERP) automatically generate audit trails and electronic batch records, which help meet FDA requirements (www.pharmtech.com) (www.pharmamanufacturing.com). Any deficiencies in these regulatory areas can become deal-breakers, so they must be assessed rigorously.

4. IT System Assessment in M&A Due Diligence

4.1 Definition and Objectives

Technology due diligence (often called IT or digital due diligence) is the process by which a potential acquirer examines the target's technology footprint in detail. It is an investigative audit of the target's IT infrastructure, software, data assets, cybersecurity posture, and technology team capabilities. The primary objectives are to:

- **Unearth Technical Liabilities:** Identify outdated, unsupported, or incompatible systems; security vulnerabilities; hidden costs (e.g. license renewals); and non-compliant capabilities that could impose penalties or expensive remediation.

- **Validate Technology Value:** Confirm that proprietary software, data analytics platforms, or IT-driven business processes indeed function as claimed, and assess whether they create competitive advantage worth the premium paid.
- **Assess Integration Feasibility:** Determine how easily the target's systems can be merged with the acquirer's. This includes evaluating data formats, middleware compatibility, network architectures, and the effort to consolidate disparate systems.
- **Estimate Transitional Work:** Calculate the time and cost required for necessary upgrades, system migrations, or new infrastructure to achieve the acquirer's target architecture. These costs can materially affect deal valuation.
- **Support Negotiation and Risk Mitigation:** Provide ammunition for price negotiations (if significant deficiencies are uncovered) and shape post-merger integration planning (by identifying priorities and potential deal-breakers early).

As one guide notes, technology and cybersecurity diligence "preserves deal value" by revealing "hidden costs" and "security problems" that could otherwise surface unpleasantly after closing (windsordrake.com). For pharma deals, this is especially critical: IT systems underpin R&D productivity, regulatory compliance, and manufacturing quality, so surprises can severely dent expected benefits.

In the M&A timeline, IT diligence typically occurs after initial deal interest is established but before signing definitive agreements. It often starts once a Letter of Intent or term sheet is in place, triggering a period (sometimes only a few weeks) of intense examination. As such, buyers often form an interdisciplinary diligence team that includes IT specialists (network architects, system analysts, security experts) alongside legal, financial, and regulatory advisors. This team works in parallel with others but focuses on compiling an "IT due diligence report" outlining findings, risks, and remediation recommendations.

4.2 Core Areas of IT Assessment

Technology due diligence typically covers multiple domains. A broad industry consensus identifies several core components that "can make or break acquisition success" (windsordrake.com). These include:

- **IT Infrastructure and Systems:** Analysis of data centers, servers, networks, cloud platforms, and disaster-recovery systems. Assessments cover server capacity and performance, network bandwidth and uptime, scalability of cloud services, and business continuity plans (windsordrake.com) (windsordrake.com). Many hidden costs lurk here: for example, some buyers run into "unexpected bills" when inherited cloud deployments can't scale without exorbitant costs (windsordrake.com). Due diligence looks at:
- Hardware (age, warranty, maintenance contracts)
- Virtualization and storage systems

- Network design (redundancy, MPLS/VPN links between sites)
- Data backup, failover, and Disaster Recovery (DR) capabilities.
- Cloud usage (services used, cost model, security controls, vendor lock-in).
- Environmental controls (for on-prem centers).
- **Software and Applications:** Examination of the target's application portfolio. In pharma this portfolio can be extensive: ERP/finance systems, lab and manufacturing apps (LIMS, MES, automation control software), R&D tools, CRM, HR, and more. Key questions include:
- Are these applications up-to-date, properly licensed, and supported?
- How proprietary is the software? (Custom-developed code vs. off-the-shelf).
- What are the maintenance fees and renewal schedules?
- Are there any licensing issues (e.g. restrictions on transferring licenses upon an ownership change)?
- What integrations and dependencies exist between applications?
- Does the codebase appear healthy (for custom systems)?

Poorly maintained or fragmented application portfolios are a sign of technical debt. For example, applications with "poor code quality" become black holes for maintenance and slow future development (windsordrake.com). In pharmaceutical diligence, analysts pay special attention to scientific and compliance-critical software; for instance, is the statistical analysis package used in trials validated and documented? Are there legacy Windows 2000 servers running specialized lab equipment? Such legacy issues would need addressing.

- **Data Assets:** This includes the target's databases and data stores – for both operational and analytics data – and the intellectual property (IP) embedded in them. For pharma, valuable data encompasses:
- **Research Data:** Preclinical study results, compound libraries, genomic or proteomic datasets.
- **Clinical Data:** Trial outcomes, patient records, adverse event databases.
- **Manufacturing Data:** Batch records, quality inspection logs, traceability records.
- **Commercial Data:** Sales statistics, market analytics, customer databases.

Key diligence tasks are to inventory major data sources, evaluate how they are structured/managed, and assess data quality and security. Consolidating data across companies is notoriously hard; differing data standards (e.g. legacy formats, missing metadata) can create integration bottlenecks. In regulated contexts, one must verify data integrity and retention (for example, ensuring that an electronic batch record system does not allow unauthorized edits). Also important is checking for any encumbrances on data/IP (e.g. in-licensed technology or collaborative research agreements that may limit data usage).

- **Cybersecurity and Data Protection:** A thorough security audit is essential. Buyers need to know if the target has had breaches or incidents and whether its defenses are robust. Areas of focus include:
- **Policies and Procedures:** Presence of documented security policies, incident response plans, and security training programs.
- **Technical Controls:** Firewall configurations, intrusion detection, endpoint protection, encryption (at rest and in transit), authentication (MFA usage).
- **Vulnerability Posture:** Have recent vulnerability scans or penetration tests been performed, and have critical patches been applied?
- **Incident History:** Records of any past security breaches, data leaks, or regulatory fines (e.g. for HIPAA violations).
- **Compliance Certifications:** Beyond ISO 27001, compliance with NIST, SOC2, PCI-DSS (if payment data), etc.

Given that pharma companies are high-value targets for cyber espionage (stealing drug formulas is lucrative), any security gap could represent existential risk. Indeed, leading dealmakers now insist on cybersecurity due diligence as “nonnegotiable” – not doing so exposes the business to inheriting vulnerabilities (www.researchgate.net) (www.researchgate.net). For example, a survey by Accenture found that only 25% of CEOs reported performing technology due diligence on most deals, despite 74% saying technology is crucial for growth (windsordrake.com) – a gulf that cybersecurity due diligence seeks to bridge.

- **Intellectual Property (IT-related):** This looks at patents and proprietary technology, including software code/IP owned by the target. Are there strong patents covering key products? Are any critical technologies unpatentable or at risk? Particularly if the target was a biotech or tech-rich pharma, one must review patent portfolios and freedom-to-operate. If software products are sold to customers (e.g. a digital health device), the due diligence should verify IP ownership, open-source license compliance, and any litigation history.
- **Organization and Personnel:** The IT organization itself is examined. Are there key personnel whose knowledge is indispensable? A thorough review includes the reporting structure (e.g. is there a CIO/CTO, or are IT functions decentralized?), headcount, skills, and ongoing projects. If the deal involves merging cultures (e.g. corporate pharma acquiring agile biotech), understanding differences in IT culture and processes becomes vital. Since cultural mismatch is frequently cited as an integration risk (www.fiercehealthcare.com) (www.researchgate.net), due diligence should assess how the IT teams operate.
- **Vendor and Contract Review:** All contracts with third-party vendors and service providers should be vetted. This includes cloud subscription agreements, outsourced development contracts, SaaS licenses, data center leases, and any long-term equipment maintenance deals. Some contracts contain change-of-control clauses which could accelerate payments or terminate services upon M&A. For example, a buyer might inherit an ERP license that, if transferred, triggers a sudden renewal at higher rates. These hidden liabilities can be uncovered through due diligence.

Together, these areas form the typical scope of IT due diligence. In practice, the diligence team will use a combination of questionnaires, document review, interviews, and system inspections. They may run network scans, review architecture diagrams, and test sample cybersecurity incidents. The output is a risk scoring or report highlighting high-priority issues (e.g. "target's LIMS server not backed up" or "bring-your-own-device policy does not enforce encryption"), so that deal terms or integration plans can be adjusted accordingly.

4.3 Process and Best Practices

Successful IT due diligence requires clear planning and cross-functional cooperation. Key steps and best practices include:

- **Planning Phase:** Early on, define the scope of IT review in the diligence charter. Align with legal and financial teams to avoid duplicate requests, but ensure nothing is overlooked. Engage experienced IT M&A specialists if possible – either from your company's IT leadership or external advisers, ideally those with pharma or life-sciences backgrounds. In large pharma deals, consulting firms including Accenture or Bain may supply technical due diligence teams.

- **Information Gathering:** Provide the target with a detailed data request list (often in a data room). Requests typically include network diagrams, inventory of hardware/software, architecture documents, service agreements, recent audit reports, security policies, and evidence of compliance (e.g. validation documents). If time is short, prioritize "red flag" items (e.g. ask for any "known vulnerabilities", critical system obsolescence, or pending regulatory issues). Some due diligence teams use structured checklists to ensure thoroughness (see *Table 2* below for an example checklist of IT focus areas).

- **Interviews and Site Visits:** It is invaluable for diligence engineers to conduct interviews with the target's IT leadership (CIO/CISO, infrastructure managers, etc.) to clarify undocumented details. If possible, site visits to data centers, factories, or labs can reveal unstated realities (e.g. a spartan server room, or legacy printers that rely on unsupported OS). However, due diligence is often remote, and virtual meetings with screen-sharing may suffice.

- **Analysis and Risk Assessment:** After collecting data, assess the findings against the buyer's priorities and thresholds. Score each area on risk/complexity. For instance, a critical vulnerability without mitigation would be "high risk"; a well-documented and updated system would be "low risk/green". Quantify where possible: estimate the cost and timeline to fix issues. One may compute a range of integration costs or potential fines under non-compliance scenarios. This information then feeds into negotiation of purchase price (via indemnities or price adjustments) or deal covenants.

- **Integration Planning Input:** Good IT due diligence doesn't stop at deal signing. It should produce actionable input for integration. For example, if the target's manufacturing database needs to be migrated, due diligence notes will include an outline of that project. In other words, the output is a risk register that will guide the post-merger IT integration roadmap. If a deal proceeds, often the diligence team transitions (or hands off its findings) to the integration team.

- **Documentation:** Maintain clear documentation of all findings and sources. This is not only for the buyer's decision but can be important if regulators or auditors later ask "what did you know about X before acquisition?". Proving rigorous diligence occurred can be a legal safeguard.

Several best-practice guides emphasize integrating IT specialists early. As one study noted, only about 25% of CEOs report conducting tech due diligence routinely (windsordrake.com), yet most acknowledge that technology is a key growth enabler. Bridging this gap means bringing the CIO/CISO into early discussions and ensuring IT risk is represented at the negotiation table.

5. Assessing Key IT Due Diligence Domains

In this section we delve deeper into each major domain of IT diligence, highlighting specific concerns and assessment methods relevant to the pharmaceutical sector.

5.1 Infrastructure and Architecture

Scope: Evaluate the target's hardware, network, cloud, and system topology. Key questions:

- **Data Centers and Servers:** Where are the servers located? Are they on-premises datacenters, co-lo facilities, or in the cloud? What is the utilization and lifecycle status of hardware? (e.g. aging servers requiring replacement). In pharma, multiple manufacturing or R&D sites may each have separate infrastructures. Consolidation post-merger can be complex if architectures differ.
- **Network and Connectivity:** Review the network architecture – is it a robust multi-site VPN/MPLS? Assess bandwidth and performance, especially for global operations. Look at wireless infrastructure and factory floor connectivity (Industrial IoT networks often exist in modern plants).
- **Cloud Platforms:** Identify all SaaS and IaaS usage. Does the company use AWS/Azure/GCP? For example, cloud might host critical systems (like a global ERP instance or an online collaboration platform). Key diligence points are billing structure and scalability. As one M&A guide warns, cloud environments often "bring surprises": if a legacy on-prem app is lifted to cloud but not architected for the cloud, unexpected bills can result when usage spikes (windsordrake.com). Confirm that licensing is appropriate for cloud (e.g., Windows Server Azure licensing issues) and examine any "shadow IT" – departmental cloud apps not tracked by IT.
- **Disaster Recovery / Business Continuity:** Inspect backup strategies and DR plans. For example, if a production site goes offline, how do they restore critical systems? Multi-site pharma companies often replicate key systems (ERPs, QMS) across geography. Check when the last DR test was performed, and whether there are gaps (e.g. "cold" backups requiring days to recover). Regulatory expectations in pharma make DR essential – product batches cannot be rerun at will if IT systems fail.
- **Environmental Controls:** For on-prem datacenters, ensure proper physical security, fire suppression, cooling, and power redundancy. While often overlooked, downtimes at manufacturing data centers could halt production lines – a risk to quantify.

Key risks if overlooked: Inadequate capacity could mean the combined company must invest millions extra post-merger to expand servers or bandwidth. Single points of failure (e.g. no backup data center) may induce prolonged outage in an integration hiccup. Unbudgeted cloud expenses can erode projected synergy savings. Weaker infrastructure in one company may end up being an unplanned drag for the acquirer.

5.2 Software Applications and Technology Stack

Scope: Examine all major enterprise and operational software. For each system or category, determine its health, cost, and strategic importance. Consider:

- **Enterprise Systems (ERP, CRM, Finance):** Verify versions, customizations, and support status. Older versions may be unsupported or cannot upgrade easily. Are different companies using the same ERP vendor or completely different systems? Multiple ERP instances (e.g. one for each region) complicate consolidation. Also check compliance of financial systems (e.g. SOX controls) if dealing with public companies.
- **Manufacturing & QC Software:** Critical systems include MES, SCADA, LIMS, QA/QC software. Validate their regulatory certifications: e.g. is the MES 21 CFR Part 11-compliant? Are electronic batch record systems validated? A production facility with only a paper-based record (like the older Ferring example) requires immediate remediation. Ferring Pharmaceuticals, upon experiencing rapid growth, implemented an integrated MES with electronic batch records to replace paper, acknowledging that "batch records and process transparency are critical elements of regulatory compliance" (www.pharmamanufacturing.com). In diligence, any target still on paper should be flagged as high risk needing major IT investment.
- **Clinical and Research Software:** List any EDC (electronic data capture) systems for trials, bioinformatics platforms (for genomics data), and specialized simulation tools. Check that patient data management systems have adequate privacy safeguards. For R&D, see if there are collaborative platforms (ELNs, chemical inventories) and whether valuable data sets are locked in proprietary formats.
- **IT Operations and Support Tools:** This includes Service & Helpdesk software (e.g. ServiceNow), monitoring tools, backup management software, etc. While not "customer-facing", these can affect integration speed. For example, if the target's helpdesk system cannot track tickets across both companies, employee training and issue resolution could lag post-merger.
- **Licensing and Compliance:** For all software, confirm that licenses are transferable and compliant. Many complex software licenses (e.g. SAP, Oracle DB) contain change-of-control clauses. Due diligence teams must check the EULAs and involve legal counsel to negotiate any needed re-licensing.

A holistic view of the technology stack is important. Are there any "shadow" systems not maintained by IT (old databases, spreadsheets used as makeshift apps)? Often diligence includes asking for a "software inventory" listing all enterprise software, version numbers, and license keys. Outdated custom software can be especially problematic – well-documented code and reasonable modularity reduce risk, but "spaghetti" code could mean lengthy rewrites.

Key risks if overlooked: Unsupported and unpatched software could leave operations vulnerable to failures or attacks. Licensing non-compliance may trigger large retroactive fees. Multiple disparate systems with no clear upgrade path could delay integration by years. Conversely, a clean, modern application portfolio is a bargaining chip – a buyer can justify paying a premium for robust tech platforms.

5.3 Data Assets and Intellectual Property

Scope: Catalog and appraise the target's data and IP. Key elements:

- **Data Repositories:** Identify major databases (SQL, NoSQL, data warehouses, cloud data lakes). What data do they hold (clinical trial records, regulatory submissions, production logs)? Determine data schemas, standards used (are there metadata, is data normalized?). Evaluate data quality controls – are there known data integrity issues? In pharma, inaccurate or incomplete data can have cascading effects (e.g. wrong labeling, wrong dosage tests).
- **Intellectual Property Files:** For pharma, IP includes patents, trade secrets, and proprietary formulas (often stored digitally). The legal team typically reviews patents, but from a systems view, check if IP documentation is stored securely and backed up. Are there version controls on critical documents (e.g. patent disclosures, pipeline notes)? Version control systems (like Git) might be used for code or R&D data – their history should be extracted.
- **Data Integration Readiness:** If a deal goes through, the acquirer's teams will likely need to migrate or merge data. Assess how facile this would be: Are there ETL (extract-transform-load) tools currently used? Is the data in open formats? For example, pharmaceutical companies often hold lab measurement data – if in proprietary LIMS, migrating to a new system can be very complex. Determine the existence of APIs or data standards (e.g. CDISC standards for clinical data) that ease interoperability.
- **Analytics and Reporting:** Does the target use business intelligence tools (like Tableau, PowerBI) or custom analytics? Understand the reporting architecture. For example, historically, some pharma struggle to compile compliance documents across disjointed systems. Integrated systems, by contrast, allow real-time visibility: as one analysis noted, when an ERP is integrated with MES and LIMS, it can "collect the MES batch records for approval along with the inspection data from the LIMS… providing improved visibility of information" (www.pharmtech.com). Due diligence should note if such beneficial integrations exist (a positive), or if absent (a red flag).
- **Data Security and Privacy:** We treat security separately above, but data assets themselves may have privacy considerations. Patient data (HIPAA) or personal employee data (GDPR) require controls on access and anonymization. Also check data residency: for example, China's regulations may restrict moving genetic or clinical data out of the country. Diligence must ensure that merging operations won't inadvertently violate such laws.

If possible, due diligence teams do light "data audit" tasks: for example, asking to inspect a random clinical database for encrypted fields, or to see if personally identifiable information is scrubbed for analytics. They may also check data retention policies (pharma companies often

must keep certain records for 10+ years). A historian's disorganized record-keeping could become a compliance gap during an FDA audit of the post-merger entity.

Key risks if overlooked: Loss or corruption of critical data through poor migration could shut down operations (e.g. inability to release products due to missing batch records). Unauthorized data exposure (e.g. a private clinical dataset) can lead to legal liability. Intellectual property leak or theft (if transfer of assets is mishandled) could erode the deal rationale. Conversely, discovering valuable data assets (e.g. a large de-identified patient database, or proprietary analytical algorithms) can enhance the value proposition of the acquisition.

5.4 Cybersecurity and Compliance

Scope: Determine the security posture of the target company and any vulnerabilities. Key activities:

- **Security Policy Review:** Ensure the target has up-to-date security policies (acceptable use, incident response, encryption standards). In pharma, policies must cover regulated data (controlled substances logs, clinical PHI). Evaluate whether these policies are enforced (e.g. regular security training, audits).
- **Controls and Tools:** Inventory the technical security controls: firewalls, IDS/IPS, endpoint protection, SIEM systems, encryption of data at rest. For example, does the LIMS store data encrypted? Are backups offline and encrypted? Are patches managed systematically? Check for multi-factor authentication on critical systems. The workflow should also include physical security of servers (locked cages, access logs).
- **Penetration Testing and Audit Findings:** Request the results of any recent penetration tests or vulnerability assessments. Ask if any high-severity issues were found and how they were remediated. Also review past audit findings from external parties (e.g. FDA security inspections, customer security audits, or ISO 27001 audit reports). If the target sells products, check whether it has ever had a data breach and how it responded.
- **Privacy Impact:** As noted, scrutinize privacy controls. For any e-health or patient data (e.g. in medical devices or trial portals), verify that privacy notices and data sharing rules are in place. For supply chain and CRM systems, even if covered U.S. healthcare laws do not apply, GDPR and other local privacy laws may.
- **Cyber Insurance and Liability:** An ancillary but important point: does the target have cyber insurance, and what are the coverage limits? The acquirer needs to know exposure should a breach invoke the target's insurance – or gaps if existing coverage lapsed.

Given the criticality of cybersecurity, many acquirers treat this part of diligence almost as a separate mini-project. As one authority put it, cybersecurity due diligence is now "nonnegotiable" as it can preserve deal value (www.researchgate.net). Any severe gaps (e.g. lack of any firewall on manufacturing networks, or unpatched HMI systems on a production line) would be indexed as high-risk items, often requiring contractual protection (indemnities) or even price reduction.

Key risks if overlooked: A cyber-attack shortly after acquisition can inflict both direct costs (remediation, ransom payment) and reputational damage. For instance, an acquirer might pay a premium $X based on disclosed revenue, only to later find a data breach that triggers multi-million-dollar fines or patient lawsuits. On the other hand, demonstrating strong cybersecurity (e.g. recent penetration test with no critical issues) can reassure the buyer and justify more confidence (perhaps even slightly higher pricing) in the deal.

5.5 IT Organization and Personnel

Scope: Assess the people and processes side of IT. Specifically:

- **Organizational Structure:** How is IT managed? Does the target have a CIO/CTO function? How decentralized is IT across divisions or geography? A very fragmented IT organization (different software management per site, no central architecture governance) can make integration much more difficult.
- **Staff Expertise and Retention:** Identify key personnel (e.g. lead network engineer, ERP manager, laboratory systems analyst). Often, small pharma or biotech rely heavily on a few experts with tribal knowledge. Losing these individuals mid-integration could be disastrous. Therefore, diligence should list critical roles and consider retention strategies (even as simple as collecting thorough documentation on each key system from these people).
- **Development and Operations Culture:** In some acquisitions, a large pharma may buy a nimble biotech with an entirely different IT culture and pace (e.g. agile development, cloud-native deployments). Understanding these differences can help gauge post-merger clashes. For example, if one side enforces strict change management and the other side frequently patches live systems, reconciling such practices is non-trivial.
- **Policies and Standards:** Check whether the target follows any IT governance frameworks (e.g., ITIL for service management, COBIT for governance). Are there written SOPs for IT processes (incident handling, change control)? Or is "how-it's-always-done" based on memory? Well-defined processes suggest predictable integration; ad-hoc operations may require a lot of rebuilding.
- **Outsourcing and Partners:** Note which IT functions are outsourced (e.g. helpdesk services, co-located management, development contractors). These contracts may need early renegotiation. Heavy reliance on external consultants, without in-house expertise, could create bottlenecks post-merger if those consultant contracts are not continued.

The due diligence team often interviews the target's IT leadership (and sometimes the CEO/CFO) about these topics. For example, in an Alacrita case study, a pharma buyer assembled a due diligence team "including a former executive of a major surgical products corporation… a pharmaceutical physician… and an experienced market researcher" (www.alacrita.com), showing how specialized expertise augments the buyer's understanding. Similarly, IT-related interviews should include the target's CIO/IT managers *and* end-user department heads, to gauge awareness of any latent IT issues (sometimes business users notice data quality problems or inefficiencies before IT does).

Key risks if overlooked: Cultural and personnel issues can stall projects. In the earlier-cited bank example, the lack of CIO involvement and integration planning led to two years of delay (www.researchgate.net) (www.researchgate.net). In pharma, a related risk is losing domain experts – e.g., a key microbiologist who also maintained lab software. A robust integration often requires retaining and onboarding such experts on the new team. Lack of HR planning for IT staff during diligence is a common pitfall.

Domain	Example Checklist Items	Impact if Overlooked
Infrastructure	- Data center locations and capacity - Network architecture (redundancy, bandwidth) - Cloud utilization and costs - Disaster recovery plans (RPO/RTO)	Outages or data loss; unexpected capital expenses; inability to scale; regulatory fines for downtime
Software & Applications	- ERP/CRM/LIMS/MES versions and patch status - Licensing contracts and transferability - Custom vs. COTS apps - Integration points between systems	License audit failures; critical system obsolescence; broken workflows; high integration cost
Data & IP Assets	- Data inventory (clinical, R&D, manufacturing data) - Data quality and encryption - Intellectual property databases and patents - Data retention policies	Loss of key data; inability to merge databases; privacy breaches; weakened competitive position
Cybersecurity & Privacy	- Security policies and training records - Firewall/VPN and endpoint security configs - Past breaches/incident history - Regulatory compliance (HIPAA, GDPR)	Security breaches; data leaks; regulatory penalties; damage to reputation
Organization & Culture	- IT team structure and size - Key personnel list & retention risks - Vendor and partner contracts (outsourcing)	Knowledge gaps; project delays; service disruptions; culture clashes

Table 2: Major domains and sample checklists for IT due diligence in pharma deals.

Throughout these assessments, evidence-based arguments should be developed. For instance, if the target's MES and ERP systems are well-integrated (as in the Wyeth example that slashed batch review time from 36 hours to 4 hours (www.pharmtech.com)), that is a positive factor. Conversely, if one finds that the target's IT spend (23% of capex per a cited 2013 figure) is concentrated in outdated systems (www.researchgate.net), that signals potential modernization costs. Strong documentation (audit logs, validation protocols) should support all conclusions.

6. Data Analysis and Evidence

Empirical research on M&A and IT integration further underscores the analysis above. A landmark ISACA study reviewed 141 mergers and concluded: *firms with high IT integration capabilities outperformed others* post-merger (www.researchgate.net). Similarly, the academic literature on M&A performance in pharma and tech suggests that well-planned acquisitions (with due diligence) can improve innovation outcomes. For example, a recent Frontiers in Public Health study on Chinese pharmaceutical companies found that "technology mergers and acquisitions can promote the performance of pharmaceutical companies," especially when accompanied by R&D investment (www.frontiersin.org). This indicates that acquiring tech (whether R&D or IT systems) has positive value, but the mention of "performance" hinges on effective integration – something due diligence facilitates.

By contrast, studies of merger failures reiterate the themes of our cautionary tales. Management research (e.g. Wharton's analysis of P&G–Gillette) repeatedly emphasizes that cultural and operational mismatches (including IT mismatches) are primary failure reasons (www.mckinsey.com) (www.ansarada.com). The takeaway is that the evidence aligns with common sense: thorough due diligence (including IT scrutiny) correlates with smoother integration and higher post-merger return on investment (ROI).

Industry surveys also provide insight. According to McKinsey circa 2004, acquirers often overestimate synergies by not having enough granular data (www.mckinsey.com). More recently, Accenture reported that only ~25% of executives routinely conduct tech due diligence, despite the fact that 74% say technology is a growth enabler (windsordrake.com). That gap – a "big risk" as Accenture phrased it (windsordrake.com) – suggests that many deals still inadequately assess IT. The implication is that companies undertaking pharma M&A may often underinvest in technical due diligence; our analysis here argues that this is a vulnerability they can ill afford.

Finally, certification metrics can quantify readiness. For instance, one can compare M&A intermediation performance for deals where targets hold ISO 27001 or similar. While specific public data is scarce, anecdotal experience indicates that targets with robust information security programs often sail through negotiation faster (and at higher valuations) than those without.

On the opposite side, evidence from large M&A research includes persistent failure rates. The oft-cited McKinsey statistic is that ~50-75% of mergers "fail" to deliver expected returns (depending on how measured) (www.mckinsey.com). While not all failures are avoidable, many are attributed to lack of detailed diligencing. As one analyst bluntly writes: *"the consolidated organization exposes itself to a number of anticipated, unknown and unintended risk factors"** (www.researchgate.net). IT due diligence aims precisely to convert some of those unknowns into knowns.

7. Case Studies and Examples

Though many M&A details are private, several relevant examples illustrate the principles described:

- **Ferring Pharmaceuticals IT Modernization (2014)**: In one case study of IT implementation (not an M&A, but instructive for integration goals), Ferring replaced its paper-based batch record system with an integrated MES and electronic batch record (eBR) system (www.pharmamanufacturing.com). The executives noted that process transparency and QA needed improvement, and they explicitly tied eBR implementation to accelerating market lead times while meeting regulatory requirements. This example demonstrates how an IT upgrade (handled outside a merger) can reduce cycle times and enforce compliance. In an M&A context, finding whether the target has or lacks similar modern systems would alter integration cost/benefit: a target still on paper would demand urgent IT investment, whereas one already on eBR would be a synergy multiplier.

- **Purdue Pharma FDA Inspection (2008)**: The account in *Pharmaceutical Technology* describes how disconnected IT systems made FDA audits burdensome (www.pharmtech.com). The implication for due diligence is to quantify the efficiency savings; integrated systems reduced batch review time by 90%. If such data is available from a target (for example, internal metrics on batch approval times), it can be compelling evidence of IT value.

- **Manufacturing Integration and IT (Novartis)**: Though not a merger of two companies, Novartis integrated its PAS (Process Automation System) with its SAP ERP to streamline production order flow (www.pharmtech.com). The due diligence lesson is to seek evidence of standards use: Novartis was noted to use ISA-95/MESA standards to align SAP with MES processes. A target that already follows such industry standards will ease post-deal integration.

- **Crown Labs – Revance (2024)**: One recent large pharma deal in the "digitalization" category was Crown Laboratories' $924 million acquisition of Revance Therapeutics (www.pharmaceutical-technology.com). While the details are beyond the scope, the fact that Revance was categorized under "digitalization" suggests its platform included a digital drug delivery business. Due diligence in such a deal would have to examine how Revance's digital systems (perhaps for patient engagement or manufacturing) mesh with Crown's operations.

- **International Accenture Study (2015)**: Accenture periodically publishes insights (e.g. "Mapping DNA of M&A") that compile CEO views on tech. One finding (as summarized earlier) was that 74% of CEOs viewed technology as a growth enabler, but only 25% did full tech diligence (windsordrake.com). This real-world disconnect underscores cases like the banks example above {"post-merger integration had not progressed" (www.researchgate.net) (www.researchgate.net)}; it validates the narrative that neglecting IT is common and problematic.

- **Paul Keckley's Commentary (2015)**: In healthcare M&A, Navigant's Paul Keckley specifically called out inadequate tech assessment as a core error (www.fiercehealthcare.com). While not pharma-specific, this viewpoint from a healthcare research leader is highly regarded. Due diligence practitioners can cite Keckley as expert opinion: integrated analysis of people, roles, functions *and technology* is essential to gauge operating risk.

- **Bank Case Study (ERB)**: A (non-pharma) case study documented in a technology risk journal provides a cautionary tale: the European Retail Bank (ERB) acquisition described earlier (www.researchgate.net) (www.researchgate.net). The bank's executives focused on business synergies and did almost no advance IT planning. This vividly illustrates the worst-case scenario. Interestingly, the same source also notes that in recent years "more importance has been given to IT integration in M&As, but… in many instances risk is ignored or is considered a concern… postmerger" (www.researchgate.net). This implies that while awareness has grown, many deals still under-prioritize IT. For industries like pharma, where regulation demands robust systems, such an oversight can be even costlier.

Each example reinforces a theme: **technical diligence matters**. Whether the context is regulatory compliance, synergy capture, or integration pace, information technology is deeply woven into the pharmaceutical value chain. The next section discusses how to translate these findings into actionable integration planning, and looks ahead to trends that will shape technology due diligence.

8. Implications and Future Directions

The growing centrality of digital technology in pharmaceuticals has several implications for due diligence:

- **Strategic Leverage of IT Assets:** As pharmaceutical business models evolve (telehealth, direct-to-patient trials, digital biomarkers), IT systems become strategic assets, not mere overhead. Acquirers will increasingly target companies for their software platforms, data analytics, or AI capabilities. For instance, a company with a strong real-world data platform may command a premium. Due diligence must therefore value technology on par with patents or pipelines, asking not only "what's broken?" but also "what unique capabilities are we gaining?"

- **Cybersecurity as a Board-level Concern:** High-profile cyberattacks (including ransomware) have made boards anxious. By some estimates, over 30% of M&A deals now consider cybersecurity risk explicitly in valuation. In pharma, where intellectual property theft is lucrative to adversaries, this trend is intensified. Compliance with forthcoming regulations (e.g. Europe's Digital Operational Resilience Act) may also require acquirers to scrutinize targets' readiness for new cyber rules.

- **Regulatory Evolution:** Agencies like the FDA are modernizing guidelines (e.g. guidance on software validation, or on cloud security). Likewise, data privacy laws (like GDPR) are constantly being interpreted. M&A teams must keep abreast of these changes. For example, if a target's cloud platform is not compliant with new FDA draft guidance on cloud service providers, the buyer may need to remediate.

- **AI and Analytics in Due Diligence:** On the positive side, acquirers are starting to use data science in the diligence itself. Advanced document analysis tools can scan millions of contracts and code repositories to pinpoint risks. EY notes that artificial intelligence is beginning to revolutionize due diligence by improving efficiency and insight (flevy.com). In practice, an acquirer might employ text-mining AI to review years of email or code change logs to detect anomalies. Pharma buyers could see AI-assisted analysis of clinical data quality or automated checks of regulatory filings during diligence.

- **Accelerated Timelines:** The M&A cycle continues to compress, with due diligence windows sometimes very short (2–4 weeks). This means that diligence teams may increasingly rely on frameworks and playbooks. For example, creating a standardized "pharma IT due diligence checklist" (similar to Table 2 above) allows faster triage. However, speed cannot sacrifice depth: thoroughness is as critical as ever.

- **Cross-Border and National Security Considerations:** As globalization advances, some governments (notably the U.S. CFIUS) are scrutinizing cross-border deals for tech transfer and data control issues. Pharma M&A often involves sensitive technology. IT diligence must therefore include geopolitical risk assessment: e.g. does the target use critical Chinese or Russian tech? Are there restrictions on transferring certain data or equipment internationally? These questions are gaining prominence.

- **Convergence of Pharma with Technology Companies:** The lines between "tech M&A" and "pharma M&A" are blurring. Pharma companies are acquiring digital health startups, software platforms, telemedicine providers, etc. This means that pharmaceutical acquirers must adopt IT due diligence practices common in Silicon Valley deals. Knowledge of intellectual property, software development life-cycle, cybersecurity, and user data privacy (HIPAA is one piece, but consumer digital health data brings many facets) will be important.

In summary, the future of pharma M&A will be shaped heavily by technology trends. Acquirers that maintain rigorous, forward-looking IT diligence will be better positioned to realize deal value and avoid pitfalls. Conversely, those that treat tech as an afterthought risk missing the real sources of synergy or downplaying critical risks.

9. Conclusion

In the high-stakes world of pharmaceutical mergers and acquisitions, the rigor of due diligence can determine whether a deal creates value or becomes a cautionary tale. This report has shown that **IT system assessment is a pivotal component of due diligence**. IT underpins all parts of a pharma business – from laboratory research to manufacturing execution to sales – and thus any gaps or incompatibilities in technology can vitiate the expected benefits of a merger.

The evidence is clear: studies find that acquisitions with strong IT integration capabilities perform better (www.researchgate.net), while failures often stem from insufficient technical scrutiny (www.ansarada.com) (www.researchgate.net). For pharma companies, the regulatory

overlay heightens the stakes – systems must meet FDA, data privacy, and quality standards without fail. Therefore, buyers cannot afford to neglect IT in their diligence checklist.

This report has mapped out the terrain of IT due diligence in pharma M&A. It spanned the landscape of applications (ERP, MES, LIMS, etc.), infrastructure (data centers, cloud), data and IP, security, and organizational factors. We highlighted how each domain can harbor hidden liabilities or untapped value, with examples from industry sources. We also outlined best practices – using multidisciplinary teams, structured checklists, and evidence-based risk scoring – to conduct a thorough assessment. Throughout, citations from pharma case studies, expert commentary, and research reports have underpinned the analysis (see citations in text).

In practice, companies undertaking acquisitions should heed these findings by:

- **Engaging IT experts early.** Involve CIOs, CISOs, and experienced tech consultants from the outset to identify issues that finance/legal teams might miss.
- **Prioritizing security and compliance.** Given pharma's regulatory burden, ensure that due diligence explicitly covers FDA, HIPAA, and other relevant rules as they pertain to IT.
- **Quantifying Risks and Costs.** Rather than just cataloging problems, attempt to quantify remediation costs or delay penalties; feed those into the valuation.
- **Planning Integration Thoughtfully.** Use the diligence results to build a realistic IT integration roadmap, rather than assuming "we'll figure it out after close."

Looking to the horizon, digital transformation trends (AI, cloud, real-world data platforms) will only make IT an even more prominent part of deal calculus. M&A teams should therefore continue to evolve their approaches – leveraging data analytics in diligence, building cross-industry checklists, and staying alert to emerging threats and opportunities in health IT.

Ultimately, by taking a comprehensive, evidence-based approach to IT due diligence, pharmaceutical companies can better ensure that their acquisitions deliver the promised innovation and growth, rather than succumbing to preventable operational failures. The citations and data in this report make it clear that **the cost of skipping this step is far greater than the investment required to do it right**.

IntuitionLabs - Industry Leadership & Services

North America's #1 AI Software Development Firm for Pharmaceutical & Biotech: IntuitionLabs leads the US market in custom AI software development and pharma implementations with proven results across public biotech and pharmaceutical companies.

Elite Client Portfolio: Trusted by NASDAQ-listed pharmaceutical companies including Scilex Holding Company (SCLX) and leading CROs across North America.

Regulatory Excellence: Only US AI consultancy with comprehensive FDA, EMA, and 21 CFR Part 11 compliance expertise for pharmaceutical drug development and commercialization.

Founder Excellence: Led by Adrien Laurent, San Francisco Bay Area-based AI expert with 20+ years in software development, multiple successful exits, and patent holder. Recognized as one of the top AI experts in the USA.

Custom AI Software Development: Build tailored pharmaceutical AI applications, custom CRMs, chatbots, and ERP systems with advanced analytics and regulatory compliance capabilities.

Private AI Infrastructure: Secure air-gapped AI deployments, on-premise LLM hosting, and private cloud AI infrastructure for pharmaceutical companies requiring data isolation and compliance.

Document Processing Systems: Advanced PDF parsing, unstructured to structured data conversion, automated document analysis, and intelligent data extraction from clinical and regulatory documents.

Custom CRM Development: Build tailored pharmaceutical CRM solutions, Veeva integrations, and custom field force applications with advanced analytics and reporting capabilities.

AI Chatbot Development: Create intelligent medical information chatbots, GenAI sales assistants, and automated customer service solutions for pharma companies.

Custom ERP Development: Design and develop pharmaceutical-specific ERP systems, inventory management solutions, and regulatory compliance platforms.

Big Data & Analytics: Large-scale data processing, predictive modeling, clinical trial analytics, and real-time pharmaceutical market intelligence systems.

Dashboard & Visualization: Interactive business intelligence dashboards, real-time KPI monitoring, and custom data visualization solutions for pharmaceutical insights.

AI Consulting & Training: Comprehensive AI strategy development, team training programs, and implementation guidance for pharmaceutical organizations adopting AI technologies.

Contact founder Adrien Laurent and team at https://intuitionlabs.ai/contact for a consultation.

DISCLAIMER

The information contained in this document is provided for educational and informational purposes only. We make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

Any reliance you place on such information is strictly at your own risk. In no event will IntuitionLabs.ai or its representatives be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from the use of information presented in this document.

This document may contain content generated with the assistance of artificial intelligence technologies. AI-generated content may contain errors, omissions, or inaccuracies. Readers are advised to independently verify any critical information before acting upon it.

All product names, logos, brands, trademarks, and registered trademarks mentioned in this document are the property of their respective owners. All company, product, and service names used in this document are for identification purposes only. Use of these names, logos, trademarks, and brands does not imply endorsement by the respective trademark holders.

IntuitionLabs.ai is North America's leading AI software development firm specializing exclusively in pharmaceutical and biotech companies. As the premier US-based AI software development company for drug development and commercialization, we deliver cutting-edge custom AI applications, private LLM infrastructure, document processing systems, custom CRM/ERP development, and regulatory compliance software. Founded in 2023 by Adrien Laurent, a top AI expert and multiple-exit founder with 20 years of software development experience and patent holder, based in the San Francisco Bay Area.

This document does not constitute professional or legal advice. For specific guidance related to your business needs, please consult with appropriate qualified professionals.