Sector / Asset & Specific Focus Notes

Part of the Buyer-Side Legal DD Series

The Problem with the Generic Lens

One of the most common weaknesses in buyer-side legal due diligence is that the team approaches every target with the same generic lens. The checklist may be long, technically correct, and even comprehensive on paper, yet the review still misses the real point of the acquisition. A software company is not bought for the same reasons as a hospital, a payment platform, a retail chain, or a real estate holding vehicle. Even within the same sector, one buyer may be acquiring a business for its licenses, while another is really buying the customer base, the data, the founder team, or a strategically important site.

That is why a serious due diligence exercise must always include a sector- and asset-specific focus analysis. The legal team must decide, early and explicitly, what deserves the greatest attention. This is not a matter of convenience. It is a matter of judgment. In a real transaction, there is never enough time to read everything with the same intensity. The role of a good due diligence lawyer is therefore not just to review documents, but to know where to zoom in.

What Is the Buyer Truly Paying For?

At the beginning of this exercise, junior lawyers should be taught to ask a simple but powerful question: **what is the buyer truly paying for?** The answer will usually sit in one or more of the following areas:

Technology & IP

The technology and intellectual property

Regulatory License

The regulatory license to operate

Land or Concession

The land or concession

Customer Base

The customer base and recurring contracts

Brand & Distribution

The brand and distribution network

Data & People

The data, the key people, the supply chain, the recurring cash flow, or the company's strategic market position

Once that answer is identified, the rest of the legal review must be reweighted accordingly.

A useful internal test is to ask five further questions. If one thing breaks after closing, what destroys the value of the deal? What cannot be replaced within three to twelve months? What depends on third-party consent or regulatory approval? What is concentrated in one contract, one founder, one license, one site, or one dataset? And finally, what risk could survive closing and become the buyer's hidden problem? These questions do not replace the ordinary checklist. They tell the team where the checklist must bite hardest.

Software, Technology, SaaS, and Platform Businesses

When the target is a software or technology business, the legal team must resist the false comfort that comes from the absence of heavy physical assets. These businesses often appear "clean" because they do not own large factories, fleets, or land banks. Yet many of the most serious risks are invisible on the balance sheet. The real value usually sits in the code, the product architecture, the customer subscriptions, the platform's data layer, and the ability of the company to keep operating and scaling without interruption.

Ownership of Technology

Juniors must not be satisfied with a simple statement that "the company owns the software." They must ask who actually wrote the code, whether founders, employees, and contractors signed proper assignment language, whether any material development work was outsourced to agencies, and whether any code or core functionality came from an affiliate, predecessor, or legacy company. In these businesses, title to IP is often more fragile than management suggests.

Open-Source Software

Open-source software requires its own distinct review. A platform may depend heavily on open-source components without having a mature governance process. The legal team should therefore examine whether code scans were performed, whether there is any policy for approving open-source usage, and whether the product contains reciprocal or copyleft components that could impose broader source disclosure or licensing obligations than the buyer expects. This point is often underestimated until very late in the deal.

Software & Tech: Customer Contracts, Data, and Key-Person Risk

The next area of focus is the customer contract layer. The buyer may think it is acquiring a scalable software business, but the contract set may reveal long-term low-priced legacy deals, severe service-level obligations, broad indemnities, source code escrow arrangements, or even provisions under which customers own valuable deliverables or customisations. The platform may appear highly valuable commercially while being legally burdened in ways that directly erode the deal thesis.

Data and privacy issues also sit at the center of technology due diligence. The legal question is not only whether the business complies with privacy law in some abstract sense. The real question is whether the buyer will be able to use, migrate, combine, analyze, or monetise the data after closing in the way it expects. That requires close reading of privacy notices, customer commitments, vendor restrictions, and local law.

Finally, technology businesses often carry key-person risk in a sharper form than other sectors. A company may nominally own the code base, but in practice the knowledge may be trapped with one founder, one CTO, or a very small engineering team. Infrastructure accounts, repositories, and admin credentials may even sit under personal rather than corporate control. That is not just an operational issue. It is a legal due diligence issue because it affects continuity, ownership, and post-closing control.

Red Flags

- Missing IP assignments
- Key repositories or domains held in personal names
- Absence of any open-source scan despite software being the core product
- Customer contracts that leak ownership rights
- Unresolved security incidents
- Overdependence on third-party APIs and cloud vendors

Deal Responses

- Closing conditions for assignment and account transfer
- Special indemnities for IP and cyber issues
- Escrow arrangements tied to technical remediation
- Retention packages for key technical staff
- Post-closing covenants on open-source compliance and credential migration

Healthcare, Life Sciences, Medtech, and Pharma

In healthcare and life sciences, the company is not merely a commercial enterprise. It is embedded in a dense regulatory environment. The buyer is often paying not only for the products or revenue stream, but for the ability to continue operating inside that regulatory framework. As a result, legal due diligence in this sector must look beyond ordinary corporate and contract review.

The first question is always what approvals, registrations, and licenses are essential to the business. These may be tied to a product, a facility, a specific legal entity, or even an individual. The team must determine whether they are transferable on a change of control and whether any reapproval or notification process would create delay or uncertainty. A business can look healthy until one discovers that its most important product approval or facility license is not robustly portable.

Product compliance and quality systems are equally important. GMP, GCP, GDP, inspection reports, warning letters, corrective action plans, product recalls, and adverse event reporting must all be reviewed with care. In these sectors, not every serious regulatory problem has already become a formal penalty. Sometimes the danger sits in a pattern of inspection observations, delayed remediation, or marketing practices that stretch beyond approved use.

Healthcare: Clinical Data, Commercial Models, and Red Flags

Where clinical or scientific assets are involved, the due diligence focus must extend to the ownership and usability of data. Trial agreements, research collaborations, investigator arrangements, and patient consents must all be checked. It is a mistake to assume that the company can freely use all the data in its possession for future commercial or development purposes. Often the contractual and regulatory restrictions are much narrower than the buyer expects.

The commercial model also matters. In many healthcare businesses, revenue depends not only on ordinary sales contracts, but on reimbursement approvals, formularies, state purchasing mechanisms, or public tender access. The legal durability of those arrangements can be just as important as the underlying product.

This sector also carries heightened anti-corruption and promotional compliance risk, especially where relationships with healthcare professionals, hospitals, or public institutions are involved.

Typical Red Flags

- Non-transferable approvals
- Unresolved warning letters
- Product recall patterns
- Unclear ownership of clinical data
- Sales structures that create problematic incentive arrangements

Deal Responses

- Closing conditions tied to core approvals
- Special indemnities for regulatory and product liability exposure
- Escrows linked to pending inspections or claims
- Covenants requiring quality-system remediation

Financial Services, Fintech, Payments, Lending, and Insurance

In financial services deals, the legal team must always come back to one central question: **can this company lawfully hold, move, intermediate, safeguard, or advise on money or financial products in the way it currently does?** Revenue growth or technological promise is not enough. The legal foundation of the business is often decisive.

1 Licensing Perimeter

The team must understand exactly which regulated activities the target performs and whether those activities fit within the scope of the licenses or exemptions on which management relies. In fintech especially, businesses often expand commercially faster than the legal perimeter analysis is updated. A platform that started in one category may quietly drift into another.

2 Safeguarding and Segregation

Where customer funds are involved, the review should not stop at policy statements. Juniors must examine whether reconciliation processes are documented, whether client-money requirements are genuinely followed, and whether the business's operating model creates any gap between what regulation requires and what operations are actually doing.

3 AML, KYC, and Sanctions

A fast-growing financial business may have built strong commercial traction on top of underdeveloped compliance infrastructure. The team should therefore study onboarding standards, monitoring systems, suspicious transaction reporting, sanctions screening, and internal remediation history. This area can be particularly dangerous because the problems often do not emerge from one dramatic event, but from accumulated weakness.

Financial Services: Resilience, Conduct Risk, and Deal Responses

Operational resilience and outsourcing also deserve real scrutiny. Many payment and fintech businesses depend heavily on one sponsor bank, one card scheme relationship, one fraud tool, or one cloud environment. The buyer may think it is acquiring a platform, while in reality it is acquiring a fragile web of dependencies.

Consumer protection and conduct risk cannot be ignored either. Lending disclosures, fee transparency, complaint patterns, sales practices, and redress exposure may materially affect value and enforcement risk.

Most Important Red Flags

- Business activities exceeding license scope
- Safeguarding failures
- Serious AML weaknesses
- Overdependence on key external partners
- Undisclosed regulatory correspondence
- Complaint volumes suggesting systemic consumer issues

Appropriate Deal Responses

- Regulatory consultation or non-objection conditions
- Special indemnities for AML and safeguarding risks
- Escrows tied to remediation
- Post-closing compliance uplift commitments

Energy, Utilities, Infrastructure, and Natural Resources

In energy and infrastructure deals, the value often lies not in ordinary corporate assets, but in a stack of legal rights that must work together: concessions, permits, site rights, environmental approvals, grid access, offtake arrangements, and project contracts. A project may look attractive in a presentation deck while being legally incomplete, commercially fragile, or difficult to transfer.

01

Identify the Core Project Right

This may be a concession, a generation license, a mining right, a PPP agreement, an extraction right, or some similar foundational permission. Examine term, renewal, revocation events, transferability, and dependence on government counterparties.

02

Land and Site Control

A project cannot operate if title, access, easements, rights of way, or corridor rights are incomplete. In resource deals, the distinction between surface rights and subsurface rights may also matter.

03

Map the Permit Stack

Environmental approvals, construction permits, operating permits, water rights, emissions rights, community or resettlement obligations, and any special local conditions. Often the greatest legal risk is not one missing permit, but a chain of permits that has one weak link.

04

Revenue Arrangements

Power purchase agreements, tariff approvals, or offtake contracts require close attention. The deal team must understand whether the revenue framework is durable, whether indexation or pass-through exists, and whether the project remains bankable under adverse scenarios.

05

Construction and Operations Contracts

EPC and O&M agreements must be tested for performance guarantees, delay exposure, and interface risk.

Typical red flags include incomplete transferability of concessions, unresolved land rights, vulnerable environmental approvals, unstable revenue frameworks, under-provisioned EPC liabilities, or unmanaged community and resettlement exposure. These often lead to closing conditions on permit and site status, special indemnities for land and environmental matters, escrows linked to remediation or dispute resolution, and covenants preserving project rights through closing.

Manufacturing, Industrial, and Logistics Businesses

Manufacturing and industrial targets derive value from continuity of production, facility status, supply chain resilience, customer relationships, and compliance systems. The legal risks are therefore often operational in nature, but no less material for that reason.

Facility Footprint

Ownership or lease status, permit validity, health and safety compliance, hazardous materials handling, and contamination history all matter. A plant that is technically running may nevertheless sit under serious legal and regulatory strain.

Supply Chain Dependence

The team should examine key supply agreements, single-source dependencies, import and export exposure, raw material pass-through mechanisms, and whether the company has real contractual protection if upstream costs or disruptions occur.

Product Quality and Liability

Warranty claims, recalls, certification systems, and quality control processes tell the legal team whether the business's operational reliability is legally robust or merely assumed.

Labour and Workforce

Union exposure, overtime practices, injury history, and reliance on agency labour are particularly important in this sector.

Customer-side risk often appears in the form of take-or-pay arrangements, liquidated damages, delivery penalties, and strict service-level obligations. In these businesses, the legal review must connect site condition, labor structure, supply chain terms, and customer obligations into one coherent picture. Red flags typically include permit or safety deficiencies, accident patterns, major supplier concentration, recall history, or hidden capex needed to keep facilities compliant. Deal responses frequently involve permit cure conditions, EHS and product liability indemnities, price adjustments for hidden capex, and escrows for unresolved site exposure.

Consumer, Retail, Brand, E-Commerce, and Distribution Businesses

Consumer-facing businesses often look deceptively simple from a legal perspective because the documents are familiar: leases, supply contracts, trademarks, customer terms, franchise or distribution arrangements, and marketing content. Yet their value can evaporate quickly if the brand, channels, supply rights, or consumer law position are weaker than they appear.

Brand Ownership

The first question is whether the target truly owns and controls the brand. Trademarks in core markets, domain names, social media accounts, creative assets, and co-branding or licensing arrangements should all be reviewed. It is surprisingly common to discover that the core brand is still held by a founder, an affiliate, or a foreign principal.

Channel Control

In many consumer deals, value depends on a portfolio of leases, marketplace access, or distributor relationships. The legal team must examine change-of-control provisions, assignment restrictions, exclusivity terms, and dependency on major landlords or platforms. A business that appears diversified may be heavily exposed to one marketplace algorithm or one shopping-center group.

Consumer Protection & Marketing Compliance

Return rights, promotions, auto-renewals, advertising substantiation, warranty disclosures, consumer complaints, and chargeback trends all reveal whether the company's customer-facing model is legally sound. Customer data and loyalty programs also deserve specific attention, especially where the buyer expects to leverage those assets post-closing.

Inventory Title & Supply Arrangements

Must be checked carefully, particularly in concession, consignment, or franchise structures where the ownership of stock may not sit where management assumes.

Common red flags include weak ownership of the core brand, change-of-control risks in franchise or distribution rights, overdependence on a single channel, consumer complaint patterns, unsupported marketing practices, and unclear inventory title. These often lead to trademark cure conditions, special indemnities for consumer and marketing exposure, escrows tied to key lease or franchise risks, and covenants preserving brand standards and channel relationships.

Real Estate-Heavy Businesses, Hospitality, and Development Targets

Where the target is primarily a real estate holding or development vehicle, the company itself may merely be the legal wrapper around the underlying property rights. In those deals, legal due diligence must focus relentlessly on whether those rights are genuine, clean, transferable, and commercially useful in the way the buyer expects.

Title is the natural starting point, but it is not the end of the analysis. The team must review encumbrances, easements, access rights, co-ownership issues, and title history. At the same time, it must ask whether the current use of the property is lawful, whether zoning and planning conditions support the buyer's intended use, and whether the site carries limitations on development, density, or operations.

Permit stack analysis is also crucial. Development permits, construction approvals, occupancy certificates, tourism or hospitality permits, hotel management agreements, and branding arrangements may all be essential to value. In hospitality deals, a strong site can still lose significant value if the management or brand agreement is unstable or terminable on a change of control.

Environmental and site history issues must be integrated into the real estate review rather than treated as a distant specialist topic.

Typical Red Flags

- Defective title
- Unlawful use
- Missing occupancy permits
- Hidden site constraints
- Revenue contracts that can be disrupted by ownership change

Deal Responses

- Title and permit conditions
- Special indemnities for zoning or environmental defects
- Escrows for unresolved property issues
- Price adjustments for remediation costs or reduced usable area

Defense, Aerospace, Advanced Technology, and Sensitive Data Businesses

Some businesses sit inside a national security perimeter. In those transactions, the usual contract and corporate analysis is not enough. The legal team must understand how export controls, government contracting, facility clearances, foreign ownership restrictions, and controlled data rules shape the target's legal value.

1

Government Contracts

Often the core asset. Must be reviewed for novation or assignment restrictions, termination for convenience, audit rights, cost allowability, security requirements, and claims exposure. Ordinary commercial contract instincts are insufficient here.

2

Export Controls

The question is not only whether the company sells restricted goods, but whether it knows what it is selling, to whom, for what end use, and under what classification regime. Weak internal discipline in this area can turn into a major post-closing liability.

3

Foreign Investment Sensitivity

The buyer's nationality, ownership chain, access to facilities, and control over data or technology may themselves become regulatory issues. In some cases, the key legal question is whether this particular buyer can own it without triggering unacceptable governmental concern.

Security clearances, controlled data, access segregation, and cyber obligations tied to government contracts must all be tested. The major red flags here include inability of the buyer to obtain necessary national security approvals, non-transferable government contract rights, weak export compliance discipline, cyber failures affecting controlled systems, and supply chain exposure to restricted vendors or jurisdictions. These issues often require national security approvals as conditions precedent, special indemnities for export and contract claims, split-closing or interim structures, and post-closing compliance enhancements.

Data-Heavy, Adtech, AI, and Consumer Analytics Businesses

Some businesses are not primarily bought for software or brand, but for the dataset itself. In those deals, the central legal question is not simply whether data privacy law is observed in a generic sense. It is whether the data asset is lawful, transferable, and usable in the way the buyer expects after closing.

01

Data Provenance

How was the data collected? Was consent obtained if required? Were notices broad enough? Was the data licensed, purchased, scraped, inferred, or acquired through partnerships? These are not abstract compliance questions. They go directly to whether the core asset is usable.

02

Rights to Combine and Reuse

Can the buyer merge it with its own database? Use it for profiling, targeting, AI training, analytics, resale, or new monetization pathways? Are there restrictions in partner agreements, vendor terms, or local law that block those plans?

03

Adtech and Tracking Stacks

Cookies, SDKs, pixels, third-party vendor relationships, and cross-border flows should all be reviewed carefully.

04

AI Training Data Provenance

AI-focused businesses require an additional layer of review. Commercial teams often assume that because a dataset was accessible, it was lawfully usable for model training. That assumption is frequently wrong.

Red flags include weak or outdated consent frameworks, uncertainty around core dataset rights, adtech practices exposed to regulatory risk, and poor documentation of training data provenance. These issues often translate into data rights conditions, privacy-related special indemnities, escrows tied to regulator risk, and post-closing covenants on re-consent, segregation, and lawful migration.

Franchise, Distribution, and Multi-Jurisdiction Platform Businesses

These businesses often look diversified because they operate across multiple locations, partners, or jurisdictions. In reality, their legal fragility often lies in the opposite direction: the business is only as strong as the patchwork of contracts, franchise rights, territory rights, local registrations, and operator relationships that hold it together.

Territory and Exclusivity Rights

Are the target's rights truly exclusive? Are those rights conditional on performance, minimum purchases, outlet openings, or local compliance? Are there side letters or local variations that alter what the master agreement appears to promise?

Network Structure

Which operations are company-owned, leased, franchised, sub-franchised, or run by distributors? Which local operators are financially weak or legally exposed? In these deals, the legal map of the network is often more important than the corporate chart.

Local Law and Disclosure

Franchise disclosure obligations, local registrations, and local licensing regimes must all be considered where relevant. It is a mistake to assume that a legally strong master agreement solves local law risk.

Brand Control and Sourcing

Brand control and mandatory sourcing obligations also require attention, especially if the principal can terminate on change of control or use performance defaults to weaken the network.

Typical red flags include fragile territory rights, change-of-control risks in master franchise or distribution agreements, local disclosure failures, and weak control over sub-franchisees or distributors. Common protections include principal consent conditions, special indemnities for disclosure or termination risk, escrows tied to network instability, and covenants preserving the structure through closing.

Asset-Specific Focus When the Sector Label Is Not Enough

Sometimes the best way to focus the review is not by sector, but by asking what single asset or asset class the buyer truly cares about.

Real Target Asset	Key Legal Focus Areas
Intellectual Property	Chain of title, transferability, registration gaps, infringement exposure, and any leakage of ownership to employees, contractors, customers, or affiliates
Regulatory License or Permit	Transferability, restrictions, qualifications, ownership caps, compliance history, and regulator relationship
Land, Site Rights, or Concession	Title, lawful use, permit stack, access, environmental history, and change-of-control effects
Customer Base or Recurring Revenue	Term, termination rights, pricing, assignment and change-of-control, dispute history, and concentration risk
Data	Provenance and lawful future use
Founder Team, Know-How, or Human Capital	Retention, restrictive covenants, undocumented knowledge concentration, personal control over systems or relationships, and change-of-control compensation

In each of these cases, the same principle applies: the legal team should not hide behind a generic checklist. It must reorganize the review around the asset that actually carries value.

How Sector-Specific Findings Should Be Reported

A junior lawyer should not report sector-specific diligence in vague statements such as "this is a fintech business, so regulation matters" or "this is a SaaS company, so IP is important." That is too abstract to be useful. A proper due diligence note should connect five things in one coherent line:

Value Driver

What the value driver is

Legal Dependency

What the sector-specific legal dependency is

Evidence

What documents prove it

Failure Scenario

What the likely failure scenario is

Deal Protection

What deal protection is required

> For example, the note should say that the value driver is recurring payment transaction volume through a licensed platform; that the legal dependency is safeguarding compliance and continuity of the partner-bank relationship; that the evidence lies in the license, the sponsor-bank agreement, and the safeguarding policy; that the failure scenario is regulatory restriction or partner termination disrupting continuity; and that the required protections are a closing condition for partner comfort, a special indemnity, and a post-closing compliance audit. **That is how sector-specific due diligence becomes decision-useful.**

Final Discipline for the Team

Before concluding this part of the review, the team should ask itself several hard questions:

- Has it clearly identified what the target is truly worth?
- Has the focus of the review actually shifted to match that reality, or is the team still performing generic checklist work?
- Have the sector-specific legal dependencies been identified?
- Have the fragile, non-replaceable assets been mapped?
- Are the likely failure scenarios reflected in the Issue Register?
- Has each major sector-specific risk been translated into a concrete deal lever?

> If the answer to any of those questions is no, the due diligence is not yet properly focused.

The practical lesson for juniors is simple but important. A checklist is a starting point, not the finished product. Real due diligence becomes valuable only when the legal team understands what drives value in the business and what could break that value after closing. A good buyer-side due diligence lawyer does not try to read everything equally. **A good lawyer knows where to zoom in.** That is where judgment begins, and that is what separates mechanical review from real transactional counsel.

ABOUT US

HERMAN
HENRY &
DOMINIC

Herman, Henry & Dominic is an experienced team of legal experts, based in Saigon and Hanoi. The firm believes in building strong relationship with clients based on trust and respect.

Herman, Henry & Dominic works under the motto: "Local Expertise & Global Standard."

Contact us at info@ezlawfirm.org.