WHITEPAPER

ideals.

The strategic imperative of regulatory due diligence

Introduction

Regulatory due diligence is a targeted assessment of an organization's compliance with legal and regulatory obligations. It serves as a risk management tool, allowing acquirers to uncover hidden liabilities, such as pending fines, expired permits, or unresolved litigation, that could jeopardize deal success or disrupt post-transaction operations.

This whitepaper explores how to build a thorough regulatory due diligence framework, including industry-specific checklists, defined stakeholder roles, and technology solutions to mitigate risks such as GDPR penalties, antitrust blockades, and environmental fines.

Disclaimer:

This material is provided for general informational purposes only and should not be construed as legal advice. Regulatory requirements vary by jurisdiction and transaction type. Always consult qualified legal counsel for advice tailored to your situation.

Why is regulatory due diligence critical in M&A and cross-border deals?

In mergers, acquisitions (M&A), or strategic partnerships, regulatory missteps can result in substantial financial penalties or failed transactions. For example, a U.S. firm acquiring a European tech startup could inherit GDPR violations if the target lacks proper data consent mechanisms, exposing the buyer to fines of up to 4% of global turnover.

In cross-border deals, particularly in heavily regulated sectors, such as energy or healthcare, conflicting regulatory environments can create operational and compliance challenges.

For example, EU regulations may mandate CO2 storage systems for oil producers, while U.S. rules may be less stringent. Proper due diligence helps identify liabilities that can be renegotiated (e.g. seller-funded retrofits) or require pricing adjustments.

ideals.

Key scenarios and use cases

Different industries face distinct regulatory risks, making robust due diligence non-negotiable. Below are common scenarios that make thorough regulatory due diligence a necessity:

Data privacy (e.g., GDPR, CCPA, HIPAA)

A target company's failure to secure customer consent for data collection or inadequate breach response protocols can lead to multimillion-dollar fines, with an average of $4.88 million per data breach. For healthcare deals, HIPAA non-compliance (e.g., unencrypted patient records) may derail the transaction.

Financial services (e.g., SEC, FCA)

Acquirers must verify AML/KYC procedures and capital reserve requirements. A bank with lax transaction monitoring systems could face enforcement actions. For instance, in November 2024, the UK's Financial Conduct Authority (FCA) fined Metro Bank £20.5 million for significant failings in its transaction monitoring systems between 2016 and 2020. The bank failed to properly monitor over 60 million transactions worth £51 billion for money laundering risks.

Antitrust/competition law

Mergers in concentrated markets require pre-approval from regulators such as the Federal Trade Commission (FTC) or the European Commission. Overlooked market dominance risks, such as a healthcare giant acquiring a regional competitor, can trigger forced divestitures, antitrust investigations, and merger cancellations.

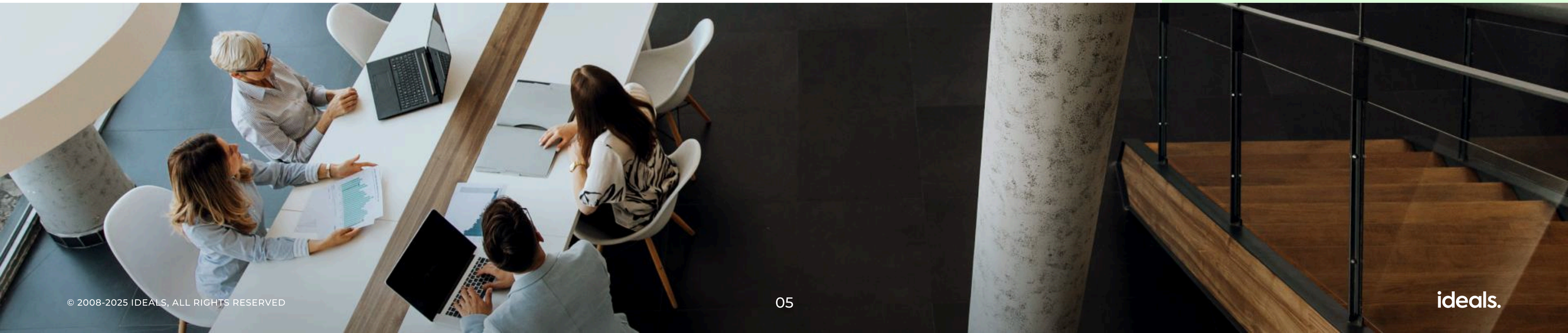
For example, in January 2024, the FTC sued to block a $320 million acquisition of Community Health Systems by Nova Health due to the risks posed by significant consolidation.

Pharmaceuticals/healthcare

FDA violations, such as incomplete clinical trial documentation or manufacturing flaws, can delay product launches or lead to recalls. For example, BEO Pharmaceuticals received an FDA warning letter, constituting significant violations of Current Good Manufacturing Practice (CGMP) regulations, including inadequate quality control procedures and failure to investigate batch discrepancies. Such issues typically trigger deal price renegotiations, delay closures, and require extensive indemnities to protect buyers from post-deal liabilities.

Environmental compliance

In energy or manufacturing sectors, undisclosed violations (e.g. improper hazardous waste disposal) may result in cleanup liabilities or permit revocations. In January 2025, Stericycle Inc., a national provider of hazardous waste transportation and disposal services, agreed to pay a $9.5 million civil penalty to resolve allegations of violating federal hazardous waste management regulations under the Resource Conservation and Recovery Act (RCRA).



ideals.

Stakeholders involved in regulatory due diligence

Successful regulatory due diligence requires collaboration across:

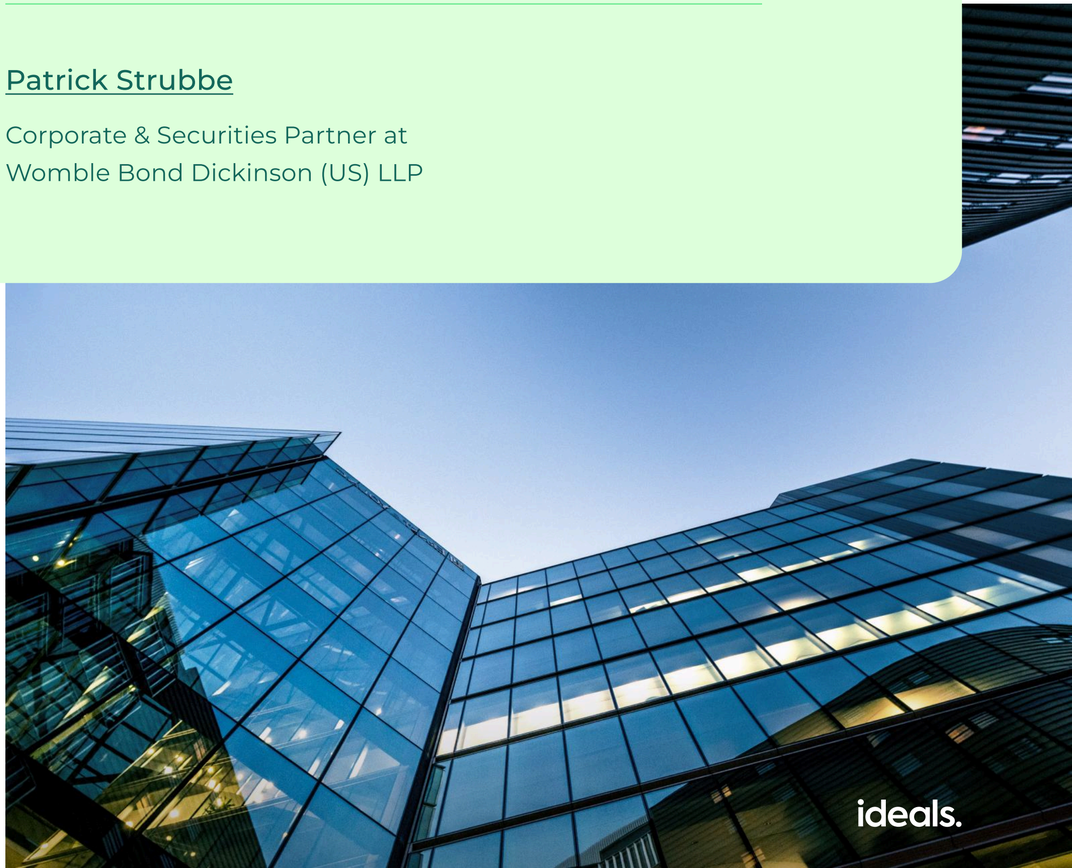
- **Legal teams.** Jurisdictional advice, indemnification clauses, and contract structuring.
- **Compliance officers.** Internal audits, policy reviews, and employee training records.
- **External counsel.** Local regulatory expertise (e.g. Brazil LGPD, APAC export controls).

A structured framework and robust checklists ensure these teams identify red flags early, such as GDPR consent gaps or antitrust triggers, avoiding costly fines or blocked deals.

> “In-house counsel need to look 10 steps ahead and understand where the risk ultimately could take their company

Patrick Strubbe

Corporate & Securities Partner at
Womble Bond Dickinson (US) LLP



Core components of a regulatory due diligence checklist

A regulatory due diligence checklist transforms broad compliance categories into actionable tasks. Below are the core components, each broken into specific items that demand scrutiny to uncover hidden risks and validate adherence:

- **Licenses, permits, and registrations.** Investigate valid business licenses (e.g. state-specific operational permits), industry certifications (FDA drug approvals, ISO 27001), and renewal deadlines for critical registrations (EPA air quality permits, export control licenses).
- **Industry-specific compliance.** Prioritize frameworks such as HIPAA (audit encryption protocols for patient records, Business Associate Agreements), MiFID II (validate EU trading transparency reports), and FDA cGMP (inspect manufacturing audit logs). For financial services, verify PCI DSS compliance for payment systems or SEC Rule 17a-4 recordkeeping.
- **Environmental and labor regulations.** Scrutinize EPA hazardous waste manifests, OSHA workplace injury logs, and I-9 employment eligibility documentation.
- **Antitrust/competition laws.** Analyze market share thresholds (Hart-Scott-Rodino filing requirements), exclusive supplier contracts, and past merger filings.
- **Data protection and cybersecurity.** Review breach response protocols (notification timelines under GDPR or CCPA), third-party vendor agreements (GDPR-compliant cloud storage terms), and encryption standards for sensitive data.
- **Export controls and sanctions.** Verify OFAC screening processes for restricted entities, end-use certificates for dual-use goods, and embargoed region sales records.
- **Ongoing litigation or enforcement risks.** Document active subpoenas (e.g. FTC investigations), unresolved consent decrees, and regulatory warning letters (FDA Form 483s).

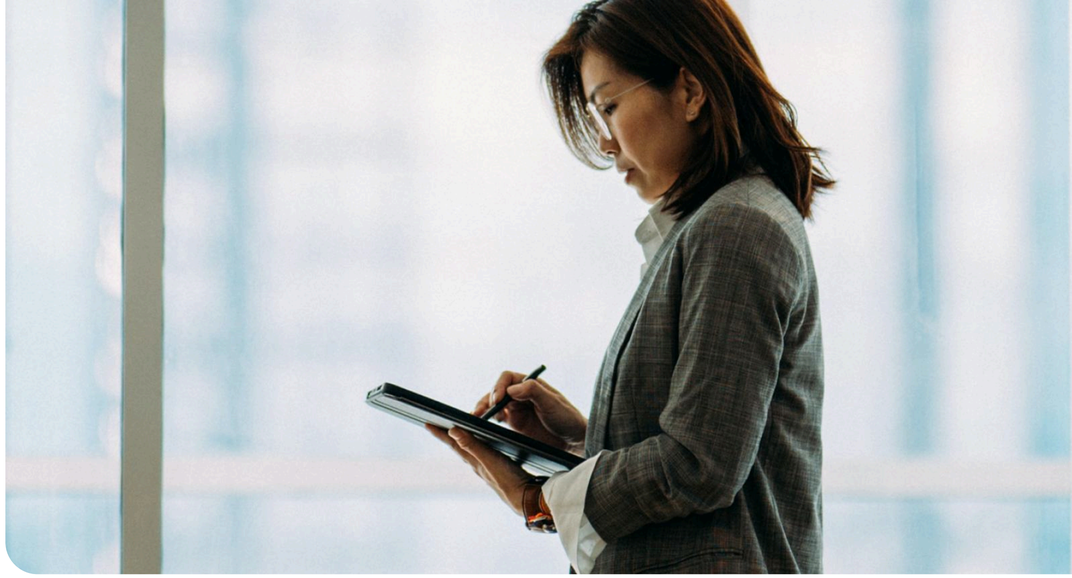
Sample regulatory due diligence checklist

A comprehensive checklist ensures no compliance stone goes unturned. Below is an expanded template with detailed items, organized to reflect real-world investigative rigor.

Category	Checklist Item	Stakeholders
1. Licenses, permits, and registrations	• State/local business licenses (e.g. cannabis dispensary permits, aviation FAA Part 135 certifications) • FDA premarket approvals (PMA) for medical devices • EPA National Pollutant Discharge Elimination System (NPDES) permits • Bureau of Industry and Security (BIS) export licenses for dual-use technologies • State alcohol distribution licenses (e.g. TABC in Texas) • REACH registrations for EU chemical compliance	• Legal Team • External Counsel
2. Industry-specific compliance	• Healthcare. HIPAA-compliant patient data encryption (AES-256), FDA Form 483 inspection responses • Finance. FCA SMCR certifications for senior managers, MiFID II transaction reporting • Tech. CCPA/GDPR data deletion workflows, PCI DSS certification for payment gateways • Pharma. FDA Drug Master Files (DMFs), EMA clinical trial authorization (CTA) documents • Energy. FERC pipeline safety compliance, state renewable portfolio standards (RPS)	• Compliance Officers • External Counsel

Category	Checklist Item	Stakeholders
3. Environmental and labor regulations	• EPA Toxic Release Inventory (TRI) filings • OSHA Form 300A annual injury summaries • Department of Labor (DOL) wage/hour audit reports • ISO 14001 environmental management certifications • State-specific sick leave policies (e.g. NY Paid Family Leave) • EEO-1 Component 1 workforce diversity reports	• Compliance Officers • Legal Team
4. Antitrust/ competition Laws	• Pre-merger notification filings (Hart-Scott-Rodino) • Pricing strategy documents (risk of price-fixing allegations) • Territorial exclusivity clauses in distributor contracts • CFIUS filings for foreign investments in sensitive sectors • Past DOJ/FTC consent decrees (e.g., behavioral remedies)	• External Counsel • Legal Team
5. Data protection and cybersecurity	• SOC 2 Type II reports for cloud providers • Data Processing Agreements (DPAs) with GDPR Article 28 clauses • NIST SP 800-171 compliance for federal contractors • Incident response plans tested within the last six months • Data residency maps for cross-border transfers (e.g. EU-US DPF) • Penetration testing reports for critical IT systems	• Compliance Officers • Legal Team
6. Export controls and sanctions	• Automated OFAC/Denied Parties List (DPL) screening systems • End-User Statements (EUS) for high-risk exports (e.g. semiconductors) • ITAR Technical Assistance Agreements (TAAs) • Deemed Export Rule compliance for foreign employees • EU Dual-Use Regulation (Regulation 2021/821) filings	• External Counsel • Legal Team
7. Ongoing litigation or enforcement risks	• Pending DOJ False Claims Act (FCA) qui tam lawsuits • SEC Wells Notices or ongoing Accounting and Auditing Enforcement Releases (AAERs) • National Labor Relations Board (NLRB) unfair labor practice charges • State Attorney General investigations (e.g., privacy violations) • EPA Administrative Penalty Orders (APOs)	• Legal Team • External Counsel

Customization tips for industry and jurisdiction



Tailoring your regulatory due diligence checklist ensures it aligns with the unique risks of your transaction. Below are actionable strategies to refine the process for specific industries, jurisdictions, and deal complexities:

Industry adjustments: Align with sector-specific risks

- **Healthcare.** Review Stark Law, Anti-Kickback compliance, physician contracts, and referral relationships.
- **Technology.** Integrate audits of AI systems for algorithmic bias, particularly for compliance with the EU AI Act (transparency requirements) or NYC Local Law 144 (automated employment decision tools).
- **Energy.** Include EPA Methane Emissions Reduction Program (MERP) compliance checks for oil and gas assets, focusing on leak detection and repair (LDAR) reports.

Jurisdictional nuances: Navigate regional complexity

- **European Union.** Expand GDPR checks to include documented Data Protection Officer (DPO) appointments and records of cross-border data transfers under the EU-US Data Privacy Framework.
- **Asia-Pacific.** Review China's Anti-Monopoly Compliance Certifications for cross-border mergers and Japan's APPI requirements for anonymized data retention policies.
- **Middle East.** Incorporate the UAE's Export Control Regulations for dual-use goods, including military-grade encryption tools or aerospace components.

Bridge knowledge gaps

- Engage environmental engineers to assess brownfield sites for CERCLA liability risks, such as undisclosed soil contamination.
- Retain sanctions attorneys to review transactions involving Russia or Belarus under OFAC Directive 4, ensuring no indirect dealings with restricted entities.
- Hire pharmacovigilance experts to audit adverse event reporting systems for pharmaceutical targets, ensuring compliance with FDA 21 CFR Part 314.

How Ideals can support your regulatory due diligence

Ideals Virtual Data Room (VDR) is a secure, cloud-based platform designed for managing sensitive documents throughout the entire M&A cycle, from target screening and due diligence to post-merger integration

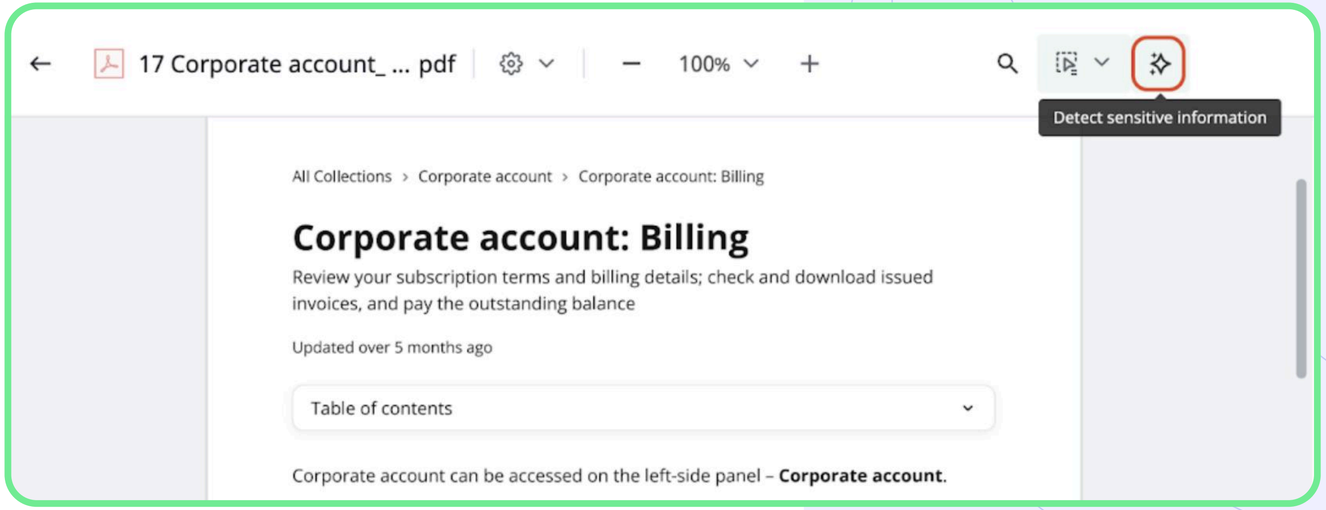
We support regulatory due diligence through efficient document management, military-grade security, and M&A-tailored tools:

1. AI tools.
2. Military-grade security and granular access permissions.
3. Due diligence checklist.
4. Q&A workflows: Real-time collaboration between legal and compliance teams.
5. Comprehensive audit trails.

1. AI tools

Ideals VDR centralizes high-volume compliance documentation with scalable storage, bulk uploads for entire indices (e.g. 5,000+ FDA trial records), and auto-indexing. Here are our core document management capabilities:

- **Bulk processing.** Import HIPAA audit logs or SEC filings via drag-and-drop, with automatic folder numbering aligning to CFR citations.
- **Secure collaboration.** Share encrypted links to GDPR-sensitive documents, expiring post-review to prevent unauthorized retention.
- **Leverage AI-driven efficiency.** Use automated redaction of PII/PHI for CCPA/GDPR compliance, intelligent search across thousands of documents (e.g., extracting “antitrust clauses”), and enterprise-grade translation of technical reports (e.g., REACH safety data) into 100+ languages.



AI redaction tool inside Ideals VDR

ideals.

2. Military-grade security and granular access permissions

Ideals VDR applies customizable permissions and enterprise-grade safeguards, ensuring compliance teams collaborate efficiently without compromising sensitive data:

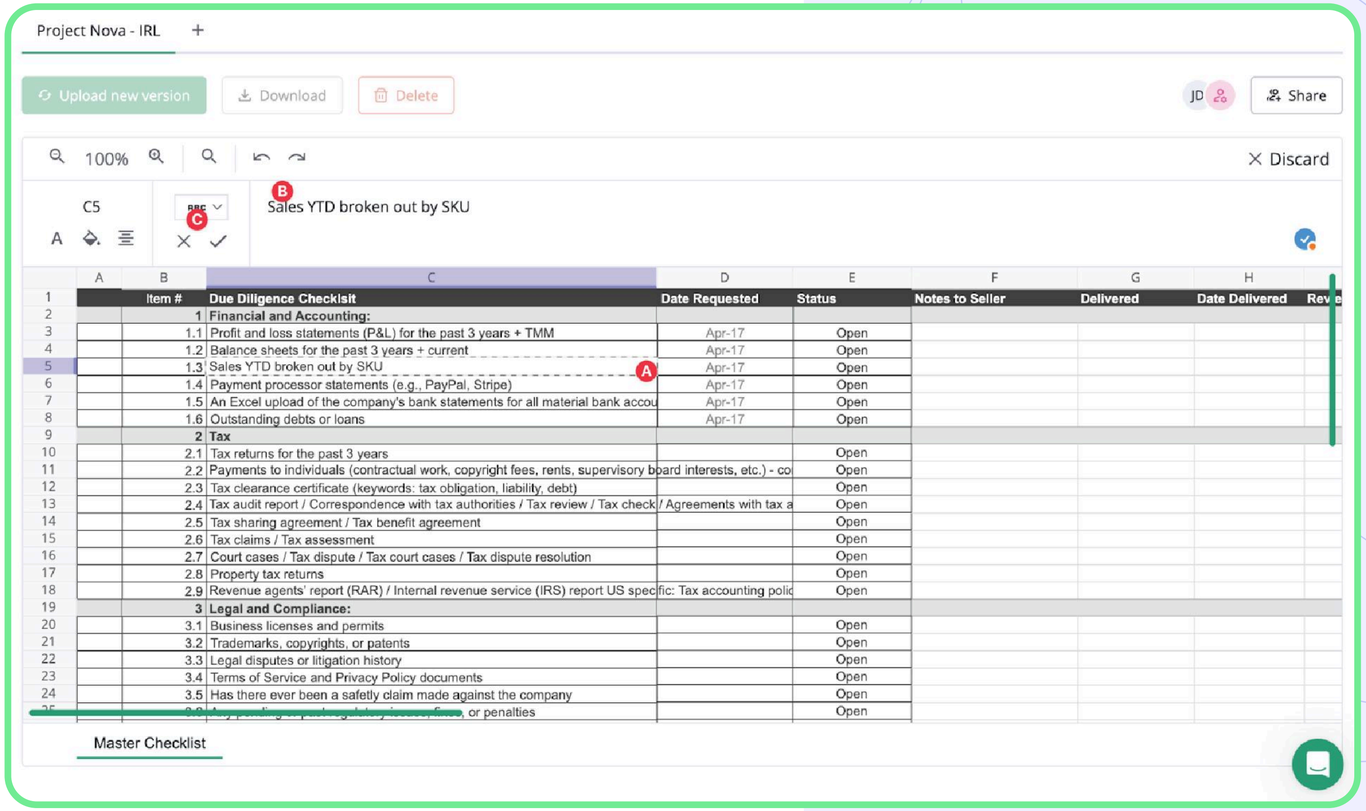
- **Tiered document permissions.** Assign “Encrypted download” for FDA documents requiring 2FA and disabling screenshots.
- **Role-based editing controls.** Restrict financial models to “Formulas Off” mode (editing disabled) or grant “Manage” rights solely to compliance officers for OSHA logs.
- **Dynamic access adjustments.** Revoke “Original Download” permissions for antitrust evidence post-review or expire external counsel's access to ITAR files post-deal.
- **Military-grade encryption.** AES 256-bit protects data at rest, while SSL/TLS secures cross-border transfers of GDPR-sensitive records.
- **Compliance-ready infrastructure.** SOC 2/ISO 27001-certified data centers in nine regions ensure 99.95% uptime, with redundant backups for audit trails.
- **Proactive safeguards.** Enforce 2FA for export control reviews and automate real-time backups of OFAC screening logs, ensuring uninterrupted due diligence.

ideals.

3. Due diligence checklist

Our due diligence checklist feature tackles the chaos of multi-jurisdictional compliance by anchoring reviews in a single, version-controlled hub. Key features include:

- **Real-time compliance alignment.**
  Edit checklists directly in the VDR, ensuring live updates for GDPR, HIPAA, or antitrust reviews. Stakeholders instantly see changes to licensing requirements or litigation risks without email delays.
- **Role-specific permissions.**
  Restrict editing rights for sensitive items (e.g. export control logs) to compliance officers, while granting view-only access to external advisors, preventing unauthorized changes.
- **Audit-ready documentation.**
  Automatically log checklist edits, downloads, and permissions changes. This audit trail proves diligence to regulators if post-deal disputes arise.
- **Cross-border coordination.**
  Manage jurisdiction-specific checklists (e.g. EU REACH vs. EPA regulations) in parallel, with secure links to supporting documents like permits or sanction screenings.



Ideals integrated due diligence checklist feature

ideals.

4. Q&A workflows: Real-time collaboration between legal and compliance teams

Our Q&A workflow feature structures compliance communication, ensuring accountability and precision in cross-functional reviews:

- **Role-specific permissions.** Restrict drafting of antitrust-related questions to legal teams and HIPAA queries to compliance officers, preventing unauthorized access to sensitive topics.
- **Expert-driven accuracy.** Assign complex FDA cGMP or export control questions to in-house specialists, ensuring responses align with current regulations.
- **Audit-ready documentation.** Track edits, approvals, and rejections in activity logs, simplifying defense against post-transaction regulatory audits.
- **Streamlined cross-border coordination.** Answer coordinators route EU REACH compliance questions to regional experts, avoiding jurisdictional misinterpretations.
- **Approval workflows.** Answer approvers validate high-risk responses (e.g., sanctions screening processes) before submission, reducing liability.

QUESTION SIDE

QUESTION DRAFTER
Can draft questions, which are routed to question submitters with their Question team for review.

QUESTION SUBMITTER
Can submit questions to Answer team, which are routed from question drafters or created by themselves.

ANSWER SIDE

ANSWER COORDINATOR
Can answer or assign questions to experts, review and edit experts' answer.

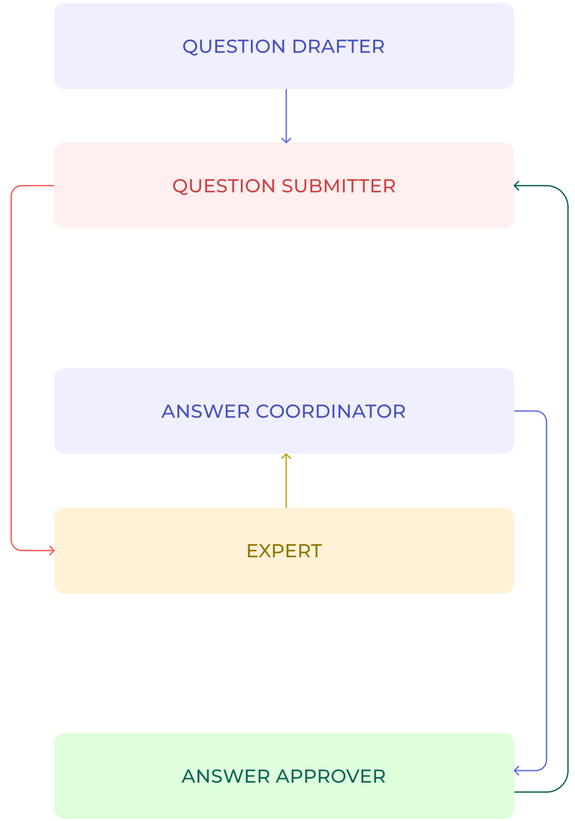
EXPERT
Can view and answer assigned questions, but can't see who initially raised the question.

- Auto-assign new questions to experts based on the category
- Include follow-up questions to auto-assignment

ANSWER APPROVER
Can answer or assign questions to experts, review and edit experts' answer.

Available Q&A roles in Ideals VDR

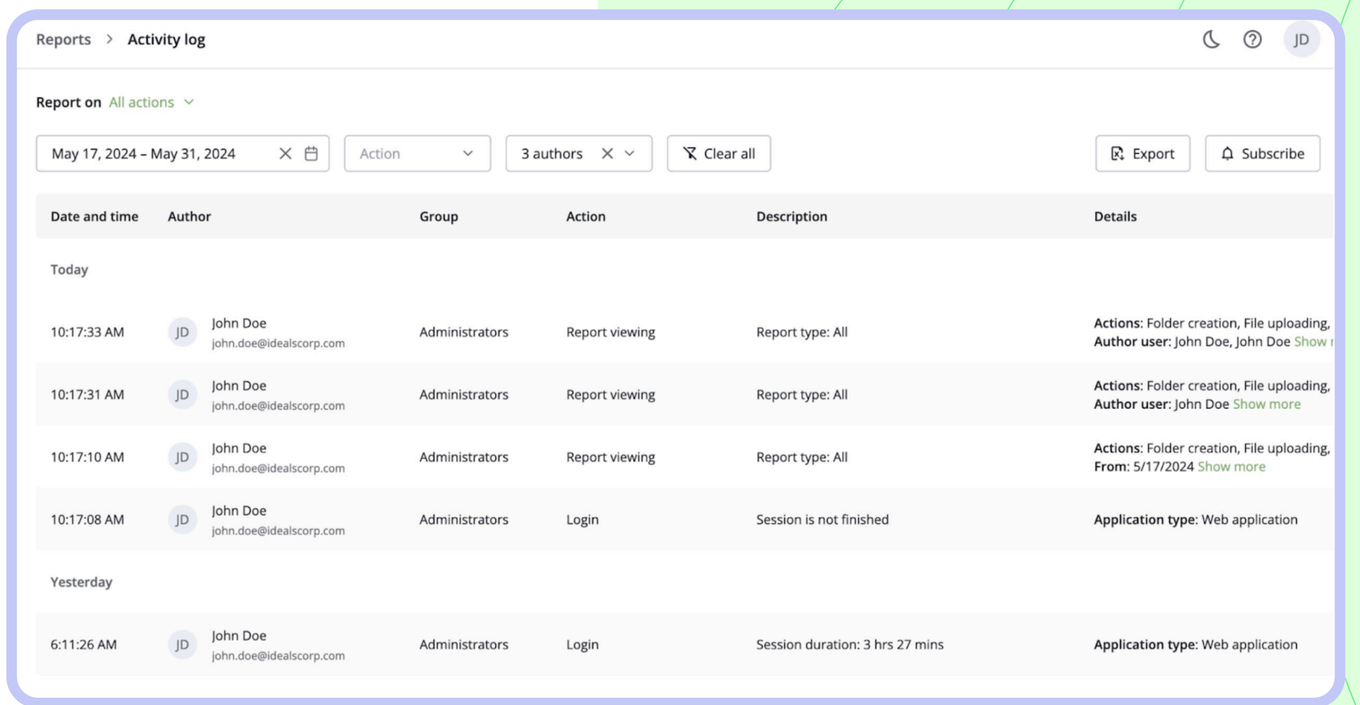
WORKFLOW PREVIEW



5. Comprehensive audit trails

Our activity log provides granular, compliance-ready tracking of every user action, from file access duration to document edits, ensuring transparency for high-stakes regulatory reviews:

- **Activity filters.** Filter logs by “Files and Folders” to prove GDPR-compliant data residency (e.g., EU patient records viewed only by authorized teams) or SEC-mandated record retention periods.
- **Role accountability.** Trace HIPAA-related document access to specific compliance officers or track external counsel’s review of export control licenses under ITAR.
- **Exportable compliance proof.** Download activity logs in Excel for FTC/DOJ submissions, including timestamps of antitrust document reviews by legal teams.
- **Automated reporting.** Schedule daily logs to compliance officers, highlighting OSHA training record access or EPA permit file updates.



Activity log functionality of Ideals VDR

ideals.

Start today and unlock:

- Live, expert-led VDR training tailored to your deal's compliance requirements.
- Full onboarding support to configure data room setup, permissions, and workflows.
- A dedicated project manager to streamline document preparation, Q&A workflows, and audit trails.

Get started

ideals.

idealsvdr.com