WHITEPAPER

ideals.

IT due diligence checklist

Chapter 1

Understanding IT due diligence

Information technology (IT) due diligence systematically evaluates a target company's technology infrastructure, systems, and processes during mergers, acquisitions, or investments. It identifies risks, opportunities, and alignment with the acquirer's strategic goals, directly influencing deal valuation and post-transaction success.

In this whitepaper, we explain how IT due diligence mitigates hidden risks and validates growth potential — along with a sample IT due diligence checklist to help you assess IT infrastructure, security, and compliance in your next transaction.

UNDERSTANDING IT DUE DILIGENCE

How IT impacts valuation and risk

A company's IT environment is crucial in shaping its financial value and risk profile. Outdated infrastructure and technical debt can lower valuation due to the high costs of necessary upgrades, with organizations spending an average of $2.9 million on technology modernization.

Cybersecurity vulnerabilities, such as unpatched systems and weak data governance, further expose businesses to breaches, regulatory fines, and reputational damage. The financial impact of such risks is substantial, with the global average cost of a data breach exceeding $4.8 million.

Non-compliance with regulations like GDPR, HIPAA, or SOC 2 can derail deals and result in significant penalties. For example, enforcement actions under HIPAA (the Health Insurance Portability and Accountability Act), a U.S. law safeguarding patient health data, have led to settlements and fines totaling $144.8m million since 2003.

UNDERSTANDING IT DUE DILIGENCE

Common challenges in IT due diligence

IT due diligence presents several challenges that can complicate assessments, increase risks, and impact post-transaction success:

Legacy systems and fragmented data architectures

They hinder a comprehensive evaluation of IT assets. Outdated systems obscure critical insights, making it difficult to assess operational efficiency, security, and integration feasibility.

Undocumented processes and shadow IT

They create operational blind spots. Unauthorized applications and unaccounted systems introduce security vulnerabilities, compliance risks, and unexpected costs, making it harder to gain a complete understanding of the IT landscape.

Integration risks

They arise when the target company’s IT infrastructure relies on incompatible platforms or follows a misaligned IT culture. These gaps can inflate post-merger costs, delay synergies, and undermine the transaction’s strategic goals.

Scalability limitations in the target’s technology stack

They may hinder future growth. If the IT infrastructure is not designed to support expansion, additional investments in system upgrades or cloud migration may be required, adding to the overall cost of acquisition.

ideals.

UNDERSTANDING IT DUE DILIGENCE

Preparing for an effective IT due diligence process

Before launching an IT due diligence assessment, companies should take key preparatory steps to ensure a thorough and efficient evaluation:

Define the scope

Prioritize focus areas such as cybersecurity audits, software inventories, and disaster recovery plans. A clear scope helps streamline the process and ensures that critical risks and opportunities are properly assessed.

Clarify objectives

Align the assessment with the acquirer's strategic goals, whether focused on full integration, carve-out strategies, or standalone operations.

Assemble a cross-functional team

It should include IT auditors, cybersecurity experts, compliance officers, and business stakeholders. Their combined expertise ensures a comprehensive review of the target's technology landscape.

Establish timelines and risk priorities

Concentrate on high-impact areas such as data integrity, vendor contracts, and pending IT liabilities. A structured timeline ensures key risks are identified early, allowing for informed decision-making.

Chapter 2

Four key components of IT due diligence

FOUR KEY COMPONENTS OF IT DUE DILIGENCE

1. IT infrastructure & systems

A target's IT infrastructure forms the backbone of its operations. Assessing hardware, software, cloud environments, and network architecture reveals technical debt, scalability potential, and compatibility with the acquirer's systems.

This evaluation ensures the technology stack supports current and future business needs while avoiding costly post-transaction surprises.

Steps to follow:

1. **Inventory existing assets.** Catalog servers, endpoints, software licenses, and cloud subscriptions to identify redundancies or gaps.

2. **Evaluate system age and performance.** Determine if hardware or legacy software requires immediate upgrades.

3. **Analyze cloud architecture.** Catalog cloud service providers (AWS, Azure, etc.), deployment models, and cost structures to assess the flexibility and security of the company's cloud architecture.

4. **Map network architecture.** Identify single points of failure, bandwidth limitations, or outdated protocols affecting reliability.

5. **Review disaster recovery plans.** Test backup systems and recovery time objectives (RTOs) to gauge resilience against outages.

6. **Benchmark infrastructure.** Compare infrastructure maturity with peers to highlight competitive advantages or risks.

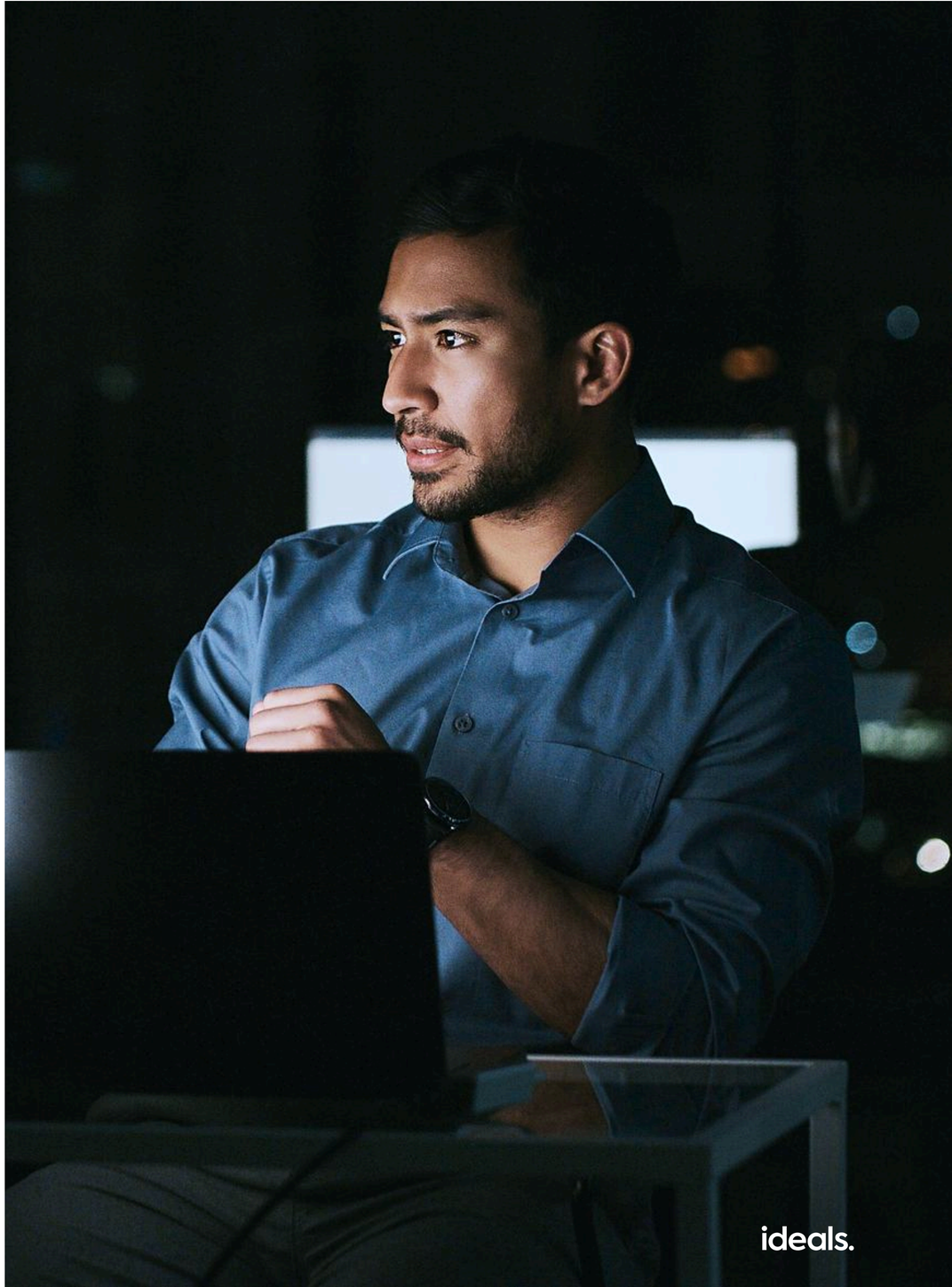
FOUR KEY COMPONENTS OF IT DUE DILIGENCE

2. Data security & cybersecurity risks

Cybersecurity vulnerabilities and data governance gaps are among the top deal-breakers in modern transactions. Despite their outsized impact on valuation, cyber risks often remain undervalued during M&A investment reviews.

“Cyber resiliency might not be a top priority for investors when building and reviewing their portfolios – but it absolutely should be,” says Caroline Escott, Senior Investment Manager for Sustainable Ownership at Railpen.

This due diligence component focuses on identifying vulnerabilities, past breaches, and compliance with regulations to mitigate legal, financial, and reputational risks.



Steps to follow:

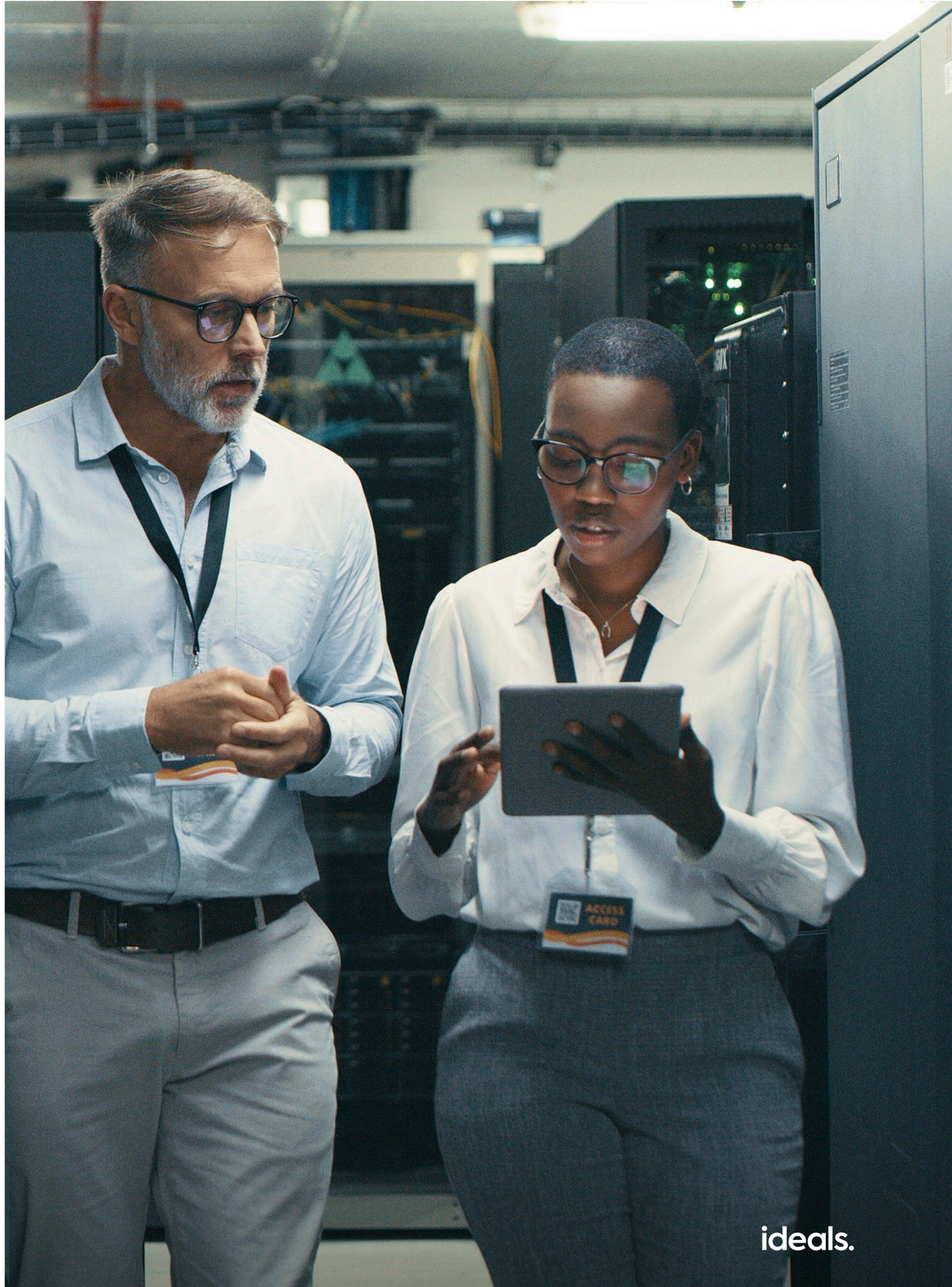
1. **Conduct a security audit.** Review firewalls, encryption standards, and access controls to uncover vulnerabilities.
2. **Assess compliance frameworks.** Verify adherence to GDPR, HIPAA, PCI-DSS, or industry-specific mandates through audits and documentation.
3. **Analyze cloud architecture.** Catalog cloud service providers (AWS, Azure, etc.), deployment models, and cost structures to assess the flexibility and security of the company's cloud architecture.
4. **Test vulnerability management.** Examine patch frequency, penetration testing results, and employee cybersecurity training programs.
5. **Evaluate data governance.** Scrutinize data classification policies, retention practices, and third-party data-sharing agreements.
6. **Review third-party risks.** Assess the security postures of vendors and partners integrated into the target's IT ecosystem.
7. **Validate cyber insurance coverage.** Confirm that policies align with potential threats and coverage limits address worst-case scenarios.

FOUR KEY COMPONENTS OF IT DUE DILIGENCE

3. IT contracts & third-party dependencies

Third-party contracts and vendor relationships can significantly impact operational stability and financial obligations post-transaction.

This review identifies risks tied to software licensing, service-level agreements (SLAs), and vendor lock-in, ensuring dependencies align with the acquirer’s strategy and compliance requirements.



Steps to follow:

1. **Inventory active contracts.** Compile all software licenses, cloud service agreements, and vendor contracts, noting renewal dates and termination clauses.

2. **Assess compliance and penalties.** Verify adherence to licensing terms (like Microsoft Enterprise Agreements) and identify risks of non-compliance or audit exposure.

3. **Evaluate vendor performance.** Analyze SLAs for uptime guarantees, support responsiveness, and penalties for missed benchmarks.

4. **Identify critical dependencies.** Flag vendors providing essential services (like cloud hosting and SaaS platforms) and assess redundancy or exit strategies.

5. **Review financial obligations.** Scrutinize data classification policies, retention practices, and third-party data-sharing agreements.

6. **Audit data ownership terms.** Confirm the target retains ownership of data stored in third-party systems and ensure portability post-transaction.

7. **Map integration challenges.** Identify technical or contractual barriers to migrating services to the acquirer's preferred vendors.

FOUR KEY COMPONENTS OF IT DUE DILIGENCE

4. IT team & internal processes

The competency of the IT team and the efficiency of internal processes directly affect system reliability and innovation capacity. A staggering 77% of organizations face operational disruptions due to IT skills gaps, exposing risks like staff shortages and training deficits.

This reflects the urgency of evaluating team expertise during due diligence to mitigate hidden innovation and maintenance liabilities.

Steps to follow:

1. **Evaluate team structure.** Review roles, reporting lines, and staffing levels to identify skill gaps or over-reliance on key personnel.

2. **Assess technical expertise.** Audit certifications, training programs, and familiarity with emerging technologies like artificial intelligence (AI) and large language models (LLM).

3. **Review incident management processes.** Analyze response times, escalation protocols, and root-cause analysis practices for IT outages or breaches.

4. **Document key workflows.** Map IT service management (ITSM) processes, such as change management, patch deployment, and user access provisioning.

5. **Benchmark operational efficiency.** Compare metrics like ticket resolution times or system uptime against industry standards.

6. **Identify knowledge silos.** Flag undocumented processes or tribal knowledge that could disrupt operations during staff turnover.

7. **Align with strategic goals.** Determine if the team's priorities (like innovation vs. maintenance) match the acquirer's long-term vision.

Chapter 3

IT due diligence checklist example

This structured checklist provides a prioritized framework for evaluating a target company's IT ecosystem during mergers, acquisitions, or investments. Categories are rated by **priority** (criticality to deal success) and **complexity** (effort required to assess), enabling teams to allocate resources effectively.

1. IT infrastructure & architecture

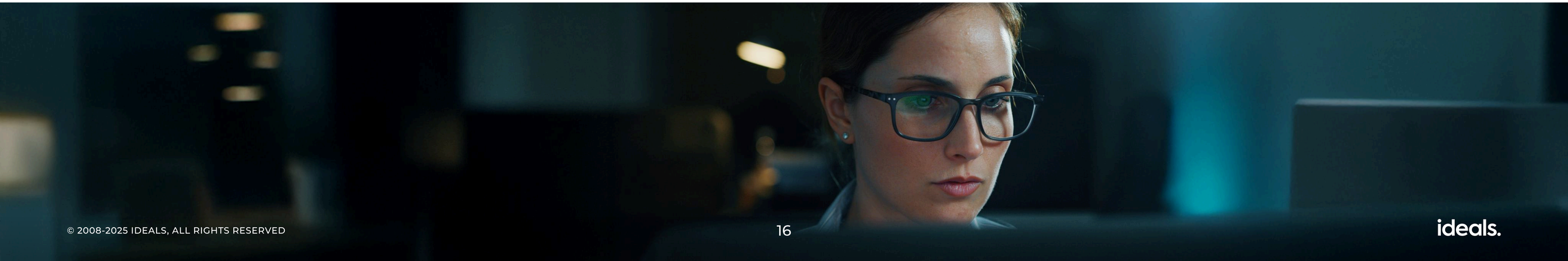
Priority High Complexity High

- [ ] Assess the stability, scalability, and integration readiness of core systems.
- [ ] Inventory hardware assets (servers, endpoints, network devices).
- [ ] Evaluate the lifecycle status of critical systems (e.g., legacy ERP, databases).
- [ ] Audit cloud environments (AWS, Azure) for configuration, cost models, and scalability.
- [ ] Map network architecture to identify single points of failure.
- [ ] Review disaster recovery plans and test backup restoration processes.
- [ ] Assess data storage solutions for redundancy and accessibility.

2. Data security & cybersecurity

Priority High Complexity High

- [ ] Identify vulnerabilities and ensure proactive safeguards are in place.
- [ ] Conduct penetration testing and vulnerability scans.
- [ ] Review access controls (multi-factor authentication, privileged accounts).
- [ ] Analyze historical breach logs and remediation effectiveness.
- [ ] Verify encryption standards for data at rest and in transit (AES-256, TLS 1.2/1.3).
- [ ] Audit employee cybersecurity training programs.
- [ ] Confirm endpoint detection and response (EDR) tools are operational..



ideals.

3. Compliance & regulatory adherence

Priority High Complexity Medium

- [ ] Validate alignment with legal and industry-specific mandates.
- [ ] Confirm GDPR, HIPAA, or PCI-DSS compliance through audit reports.
- [ ] Review data retention policies and deletion practices.
- [ ] Assess third-party vendor compliance (like SOC 2 reports).
- [ ] Validate privacy consent mechanisms for customer data.
- [ ] Check for pending regulatory investigations or unresolved violations.

4. IT contracts & third-party dependencies

Priority Medium Complexity High

- [ ] Uncover risks tied to vendor lock-in or unfavorable terms.
- [ ] Catalog software licenses (Microsoft, Oracle) and verify compliance.
- [ ] Identify auto-renewal clauses or termination penalties in contracts.
- [ ] Evaluate SLAs for uptime guarantees and support responsiveness.
- [ ] Assess dependencies on niche vendors with limited alternatives.
- [ ] Confirm data ownership rights in cloud/SaaS agreements.

5. Financial impact & cost analysis

Priority High Complexity Medium

- [ ] Quantify hidden costs affecting valuation or integration budgets.
- [ ] Calculate total cost of ownership (TCO) for critical systems.
- [ ] Identify pending capital expenditures (like hardware upgrades).
- [ ] Review IT budget trends and ROI on recent tech investments.
- [ ] Estimate costs to migrate data from legacy systems.
- [ ] Assess potential penalties for non-compliance (like GDPR fines).

6. IT team & operational processes

Priority Medium Complexity Medium

- [ ] Evaluate workforce competency and process efficiency.
- [ ] Review IT staff skills (certifications, cloud expertise).
- [ ] Analyze incident response times and change management workflows.
- [ ] Document knowledge silos or reliance on outsourced teams.
- [ ] Audit IT service management (ITSM) tools (like ServiceNow).
- [ ] Assess alignment between IT priorities and business goals.

7. Scalability & integration readiness

Priority High Complexity High

- [ ] Ensure systems adapt to growth or integrate with the acquirer’s environment.
- [ ] Test application programming interface (API) compatibility between the target and acquirer platforms.
- [ ] Evaluate the scalability of cloud workloads during peak demand.
- [ ] Identify custom-code dependencies hindering upgrades.
- [ ] Review the roadmap for retiring legacy systems.

Chapter 4

Conducting IT due diligence with Ideals

IT due diligence often faces challenges such as fragmented data collection, insecure document sharing, inefficient collaboration, and compliance blind spots.

Ideals is a leading virtual data room (VDR) platform that empowers businesses to securely manage confidential documents during critical processes like due diligence and M&A. It addresses challenges with IT due diligence through tailored features to enhance efficiency, security, and end-to-end control throughout the process.

CONDUCTING IT DUE DILIGENCE WITH IDEALS

VDR Checklist

Ideals VDR provides a Checklist feature that streamlines IT due diligence by replacing fragmented Excel/email workflows with a secure, centralized platform for managing document reviews.

Key benefits:

Ensure audit-ready accountability

Every action related to the checklist is tracked (editing, uploading, downloading, sharing) and automatically logged with user details.

Accelerate reviews

Centralized checklists with real-time editing and granular permissions eliminate back-and-forth emails, while direct XMSL uploads preserve existing workflows.

Eliminate version conflicts

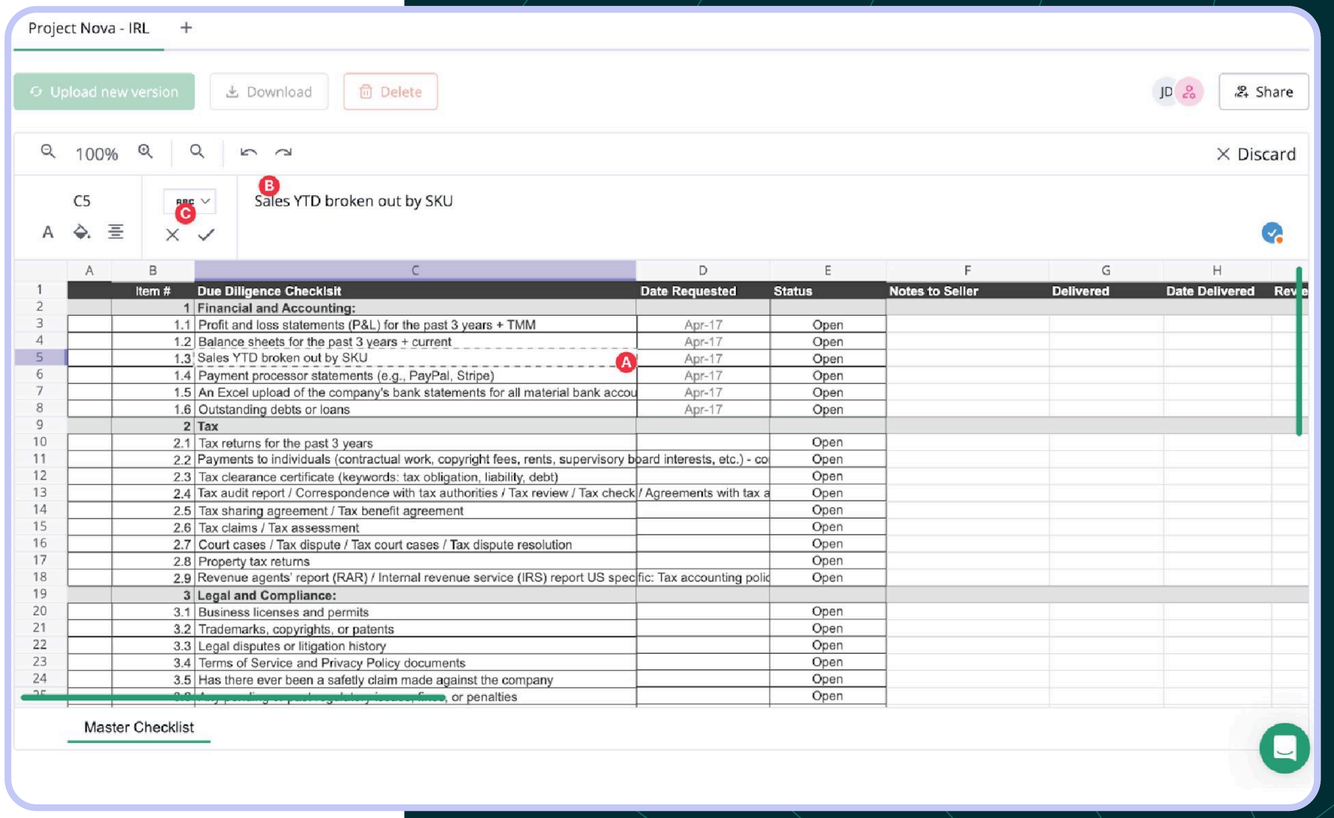
Upload existing checklists (like XMSL formats) directly into the VDR for real-time collaboration. This ensures all users work from a single, up-to-date version, eradicating duplicate files or outdated spreadsheets.

ideals.

CONDUCTING IT DUE DILIGENCE WITH IDEALS

How the VDR Checklist works

Users with corresponding permissions can upload checklists (e.g., XMSL templates), assign View-only or Edit permissions to user groups, and track progress via audit logs. Changes are saved in real time and immediately visible to authorized participants.



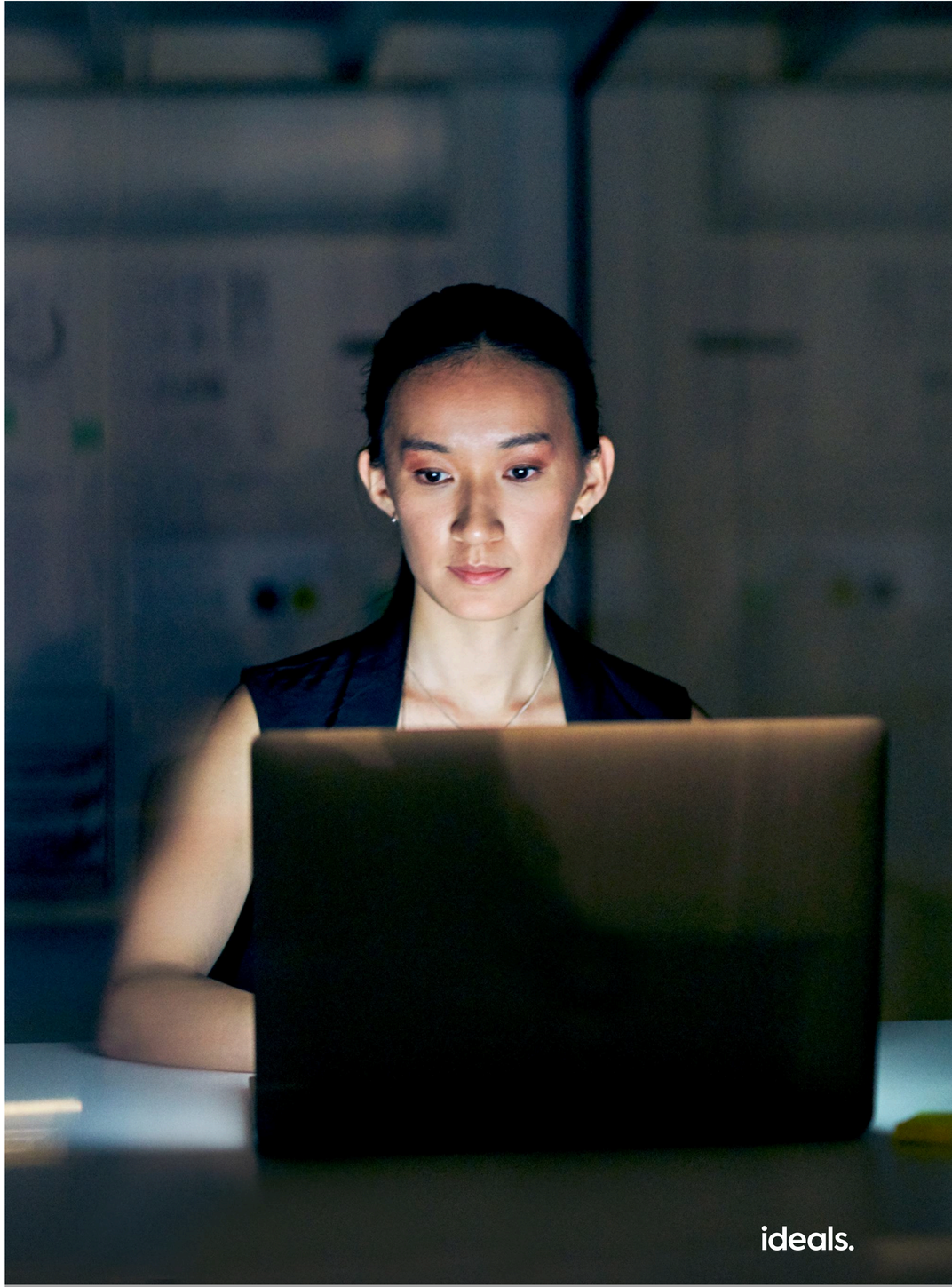
ideals.

CONDUCTING IT DUE DILIGENCE WITH IDEALS

Eight levels of granular access permissions

Ideals' hierarchical permission system enables precise control over IT due diligence documents, balancing transparency with security.

With eight access tiers, from "No Access" to "Manage," administrators can tailor visibility and editing rights for user groups, ensuring sensitive data (like breach reports and vendor contracts) remains protected.



Key benefits:

Ensure compliance

Apply “Encrypted” permissions for GDPR-sensitive files, requiring authentication to access or edit.

Control workflows

Restrict “Manage” access to IT leads, preventing unauthorized deletion of critical infrastructure documents.

Mitigate data leaks

Use “Fence View” to mask sensitive network diagrams or compliance audits, preventing screen-capture attacks.

Streamline collaboration

Assign “View (Formulas Off)” to external auditors for Excel financial models, blocking unintended edits.

Track activity

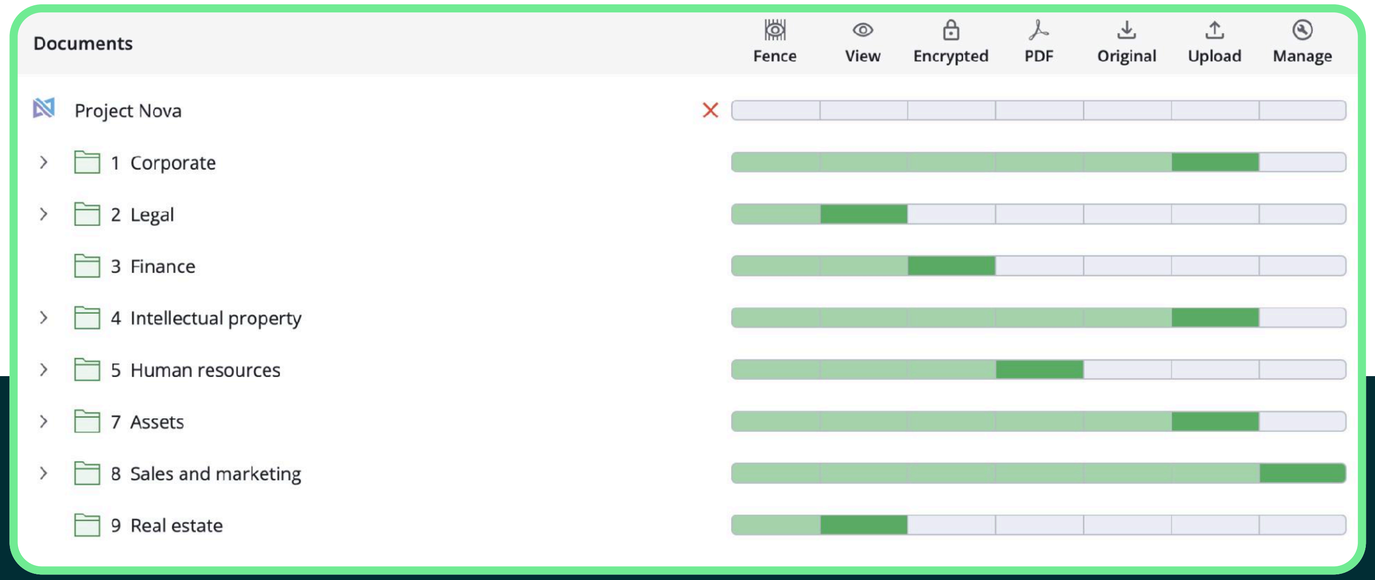
Monitor “PDF” or “Original” downloads in reports to simplify audit trails.

ideals.

CONDUCTING IT DUE DILIGENCE WITH IDEALS

How it works

Permissions cascade downward hierarchically, with admins assigning predefined or custom access levels to user groups, ensuring compliance with the principle of least privilege.



ideals.

CONDUCTING IT DUE DILIGENCE WITH IDEALS

Automated Q&A workflows

Ideals' Q&A workflows centralize and accelerate communication during IT due diligence, reducing delays in resolving technical queries.

Administrators configure roles (Question Drafter, Question Submitter, Answer Coordinator, Expert, Answer Approver), assign teams, and activate categories to route questions, such as cybersecurity vulnerabilities or compliance gaps, to relevant stakeholders.

Key benefits:

Speed technical reviews

Auto-route queries (like legacy system risks) to experts, minimizing manual coordination.

Enforce compliance

Audit trails for Q&A threads align with GDPR and HIPAA documentation requirements.

Limit exposure

Restrict answer visibility to assigned roles, mirroring granular permissions.

Reduce errors

Structured approval chains prevent unauthorized disclosures of sensitive IT configurations.

ideals.

CONDUCTING IT DUE DILIGENCE WITH IDEALS

How it works

Questions drafted by teams are auto-assigned to experts based on predefined categories (for example, “Infrastructure” or “Data Governance”). Answers undergo approval workflows, with threaded discussions and audit logs ensuring accountability.

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.

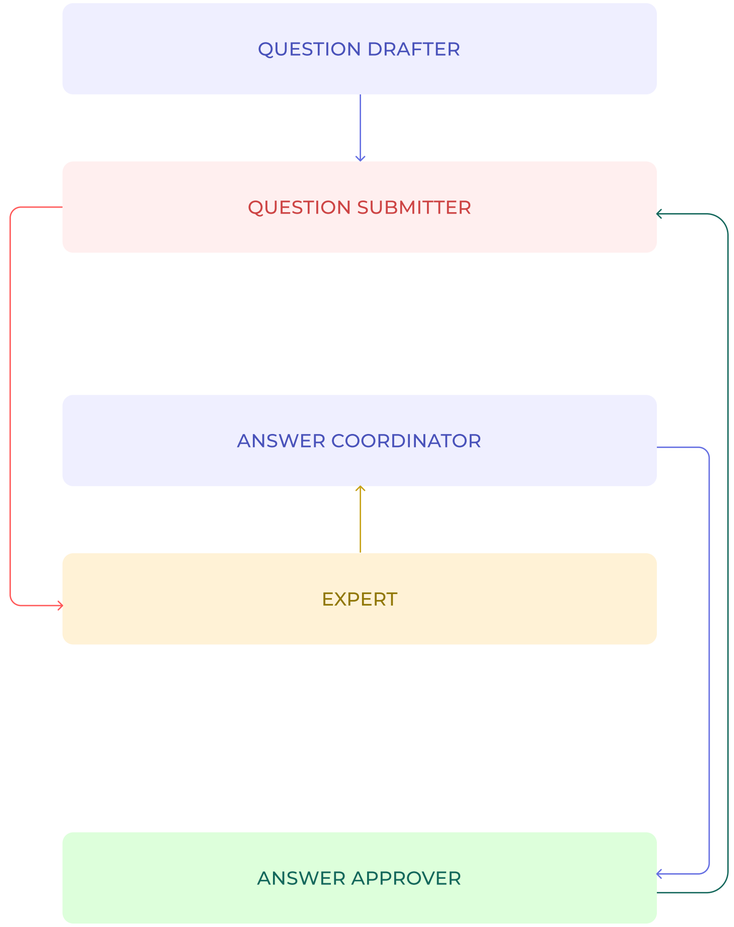
- Auto-assign new questions to experts based on the category
- Include follow-up questions to auto-assignment

ANSWER APPROVER

Can approve answer submission to Question team or reject it with comments available to Answer coordinator.

Available with the enterprise subscription after trial ends.

WORKFLOW PREVIEW



ideals.

ideals.

idealsvdr.com