



**HEALTHCARE DEALBREAKERS**

# **IT Nightmares That Could Kill the Deal**

---

**August 23, 2023**

© 2023 PYA, P.C.

WE ARE AN INDEPENDENT MEMBER OF HLB—THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

# Introductions

---



**Barry Mathis**

Principal

[bmathis@pyapc.com](mailto:bmathis@pyapc.com)



pyapc.com  
800.270.9629

ATLANTA | CHARLOTTE | HELENA | KANSAS CITY | KNOXVILLE | NASHVILLE | TAMPA

# Discussion Agenda



**What is reviewed during an IT due diligence assessment?**



**How could cybersecurity influence an investment or acquisition decision?**



**What are the five biggest risks of IT when closing a deal?**



**What are the five steps to a successful IT diligence assessment?**

A blue-tinted background image showing a hand holding a pen and writing on a tablet. The tablet screen displays some data, including the text 'GF10G12' and a line graph. The image is slightly blurred, creating a professional and technical atmosphere.

What is reviewed during an IT due diligence assessment?

The due diligence process provides the acquiring company with a complete picture of the current state of the target company's IT landscape. It helps in identifying hidden risks, potential synergies, integration challenges, and areas where negotiation or price adjustments might be warranted. It also supports the post-acquisition integration planning to ensure a smooth transition and alignment with the strategic goals of the combined entity.

# What's Included – Top 10



## IT Infrastructure and Architecture

- Hardware, software, and network components
- Data centers and cloud services
- Scalability and performance metrics
- Disaster recovery and business continuity plans

## Data Management and Integrity

- Data governance policies
- Data quality and consistency
- Database design and management
- Data security and privacy measures

## Security and Compliance

- Security policies and procedures
- Compliance with regulatory requirements (e.g., GDPR, HIPAA)
- Incident response and risk management
- Vulnerability and penetration testing

## Software and Applications

- Custom software development practices
- Off-the-shelf software licenses and compliance
- Integration with existing systems
- Intellectual property rights

## IT Operations and Support

- IT service management processes
- Helpdesk and support structures
- Vendor management and outsourcing agreements
- SLAs (Service Level Agreements) and performance metrics

# What's Included – Top Ten



## Financial Analysis

- IT budget and expenditure
- Current and future capital expenses (CAPEX) and operating expenses (OPEX)
- Stalled IT initiatives

## Human Resources and Organizational Alignment

- IT staffing levels, skills, and competencies
- Organizational structure and alignment with business strategy
- Change management capabilities

## Strategic Alignment

- Alignment of IT strategy with overall business strategy
- Technology innovation and future growth opportunities
- Identification of synergies or conflicts with the acquiring company's technology

## Contractual Obligations and Liabilities

- Review of all IT-related contracts, such as vendor agreements, licenses, and leases
- Potential legal liabilities, including intellectual property infringement or pending litigations


## Integration Planning

- Assessing the feasibility of integrating the target's IT system with the acquiring company's system
- Estimating integration costs and timeline
- Identifying potential challenges and risks in integration
- Incident response and risk management
- Vulnerability and penetration testing

A blue-tinted background image showing a hand pointing at a laptop screen. The screen displays some data, including the text 'GF10G12' and a line graph. The image is slightly blurred, focusing on the hand and the text on the screen.

How could cybersecurity influence an investment or acquisition decision?





Cybersecurity can significantly influence investment or acquisition decisions in many ways, given the importance of information integrity, privacy, and system availability in today's digital world.

# How Could Cybersecurity Influence a Decision?



**Regulatory Compliance:** Ensuring that the target company is compliant with all relevant cybersecurity regulations is vital to avoid legal penalties and maintain customer trust.

**Cost of Remediation:** If a target company has poor cybersecurity practices, the acquiring or investing entity might need to invest significant resources to improve its cybersecurity infrastructure.

**Intellectual Property Protection:** If a company's intellectual property is not well-protected, it may be susceptible to theft or espionage.

**Business Continuity Planning:** A solid cybersecurity strategy also includes robust business continuity planning. Investors or acquirers will want to ensure that the target company can continue to operate efficiently, even in the face of a cyberattack, minimizing downtime and associated revenue loss.



# How Could Cybersecurity Influence a Decision?



**Customer Trust:** Cybersecurity directly impacts customer trust. Any loss of customer data or other cybersecurity incidents can lead to loss of customers and revenue. An investor or acquirer will need to assess this aspect thoroughly.

**Insurance and Liability Considerations:** Understanding the cyber liability and insurance landscape related to the target company can also influence the decision.

**Integration Challenges:** A misalignment in cybersecurity practices between the acquiring and target companies could lead to integration challenges and unforeseen expenses.

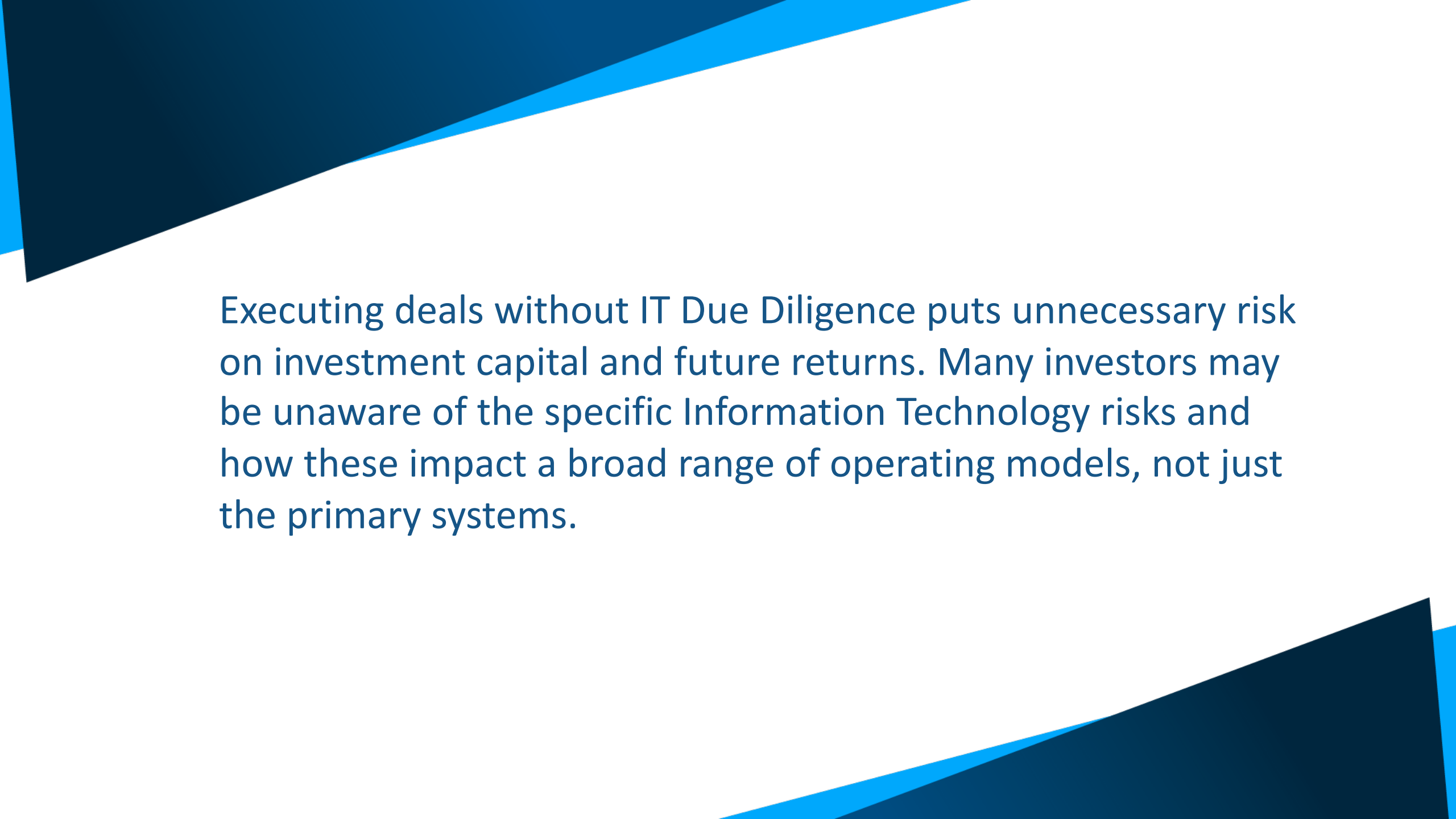
**Long-term Strategic Alignment:** Investors or acquirers will want to ensure that the cybersecurity strategy of the target aligns with their own long-term business objectives and risk tolerance.

**Impact on Future Growth:** The state of a company's cybersecurity might affect its ability to grow, especially in sectors where digital innovation is key.



A blue-tinted background image showing a hand pointing at a laptop screen. The screen displays some data, including the text 'GF10G12' and '24.3M'.

What are the five biggest risks of IT when closing a deal?



Executing deals without IT Due Diligence puts unnecessary risk on investment capital and future returns. Many investors may be unaware of the specific Information Technology risks and how these impact a broad range of operating models, not just the primary systems.

# Five Biggest Risks of IT When Closing a Deal



## Data Security and Compliance

Data Breaches  
Compliance Issues



## Integration

System Compatibility  
Data Integration



## Cultural and Process Alignment

Different organizations may have different IT cultures and processes



## Intellectual Property (IP) and Licensing

Ownership Conflicts  
Software Licensing




## Hidden Costs and Liabilities

Undiscovered Liabilities  
Cost Overruns



A blue-tinted background image showing a hand pointing at a laptop screen. The screen displays some data, including the text 'GF10G12' and a line graph. The image is slightly blurred, focusing on the hand and the text on the screen.

What are the five steps to a successful IT diligence assessment?



In this new era of M&A, the definition of due diligence is expanding well beyond conventional financial metrics to include a company's digital strategy, capabilities, strengths, and weaknesses as well.



# Five Steps To a Successful IT Diligence Assessment



## Preparation and Planning:

### Define Scope and Objectives:

Understand the key objectives, strategy, and scope of the acquisition.

### Assemble the Team:

Create a team of experts including IT, legal, financial, and business professionals.

### Collect Preliminary Data:

Gather initial data about the target's IT systems, processes, contracts, assets, and personnel.



## Assessment of IT Infrastructure and Systems:

### Evaluate IT Assets:

Assess hardware, software, licenses, and other technology assets

### Analyze Network and Security:

Understand the robustness and potential vulnerabilities of the network and security measures.

### Review Compliance:

Ensure adherence to legal and regulatory requirements, industry standards, and best practices.



## Integration Planning:

### Alignment with Business Strategy:

Understand how the target's IT can align or adapt to the acquiring company's overall business strategy.

### Create Integration Roadmap:

Develop a detailed plan for integrating technology systems, teams, and processes.

### Assess Culture and Change Management Needs:

Consider the human factor in IT integration.



## Risk Analysis and Valuation:

### Identify Risks:

Highlight potential risks including technological obsolescence, security flaws, compliance issues, or integration challenges.

### Perform Financial Analysis:

Determine the monetary value of the IT assets and any potential liabilities or additional costs.

### Mitigate Risks:

Develop strategies to mitigate identified risks.



## Execution and Post-Merger Integration:

### Finalize Contractual Obligations:

Ensure that IT-related terms are clearly defined in the acquisition contract, including warranties, representations, and indemnities.

### Implement Integration Plan:

Execute the integration roadmap, aligning technology and processes,

### Ongoing Monitoring and Optimization:

Establish continuous monitoring and optimization strategies.

# How can we HELP?

---





A national healthcare advisory services firm  
providing consulting, audit, and tax services