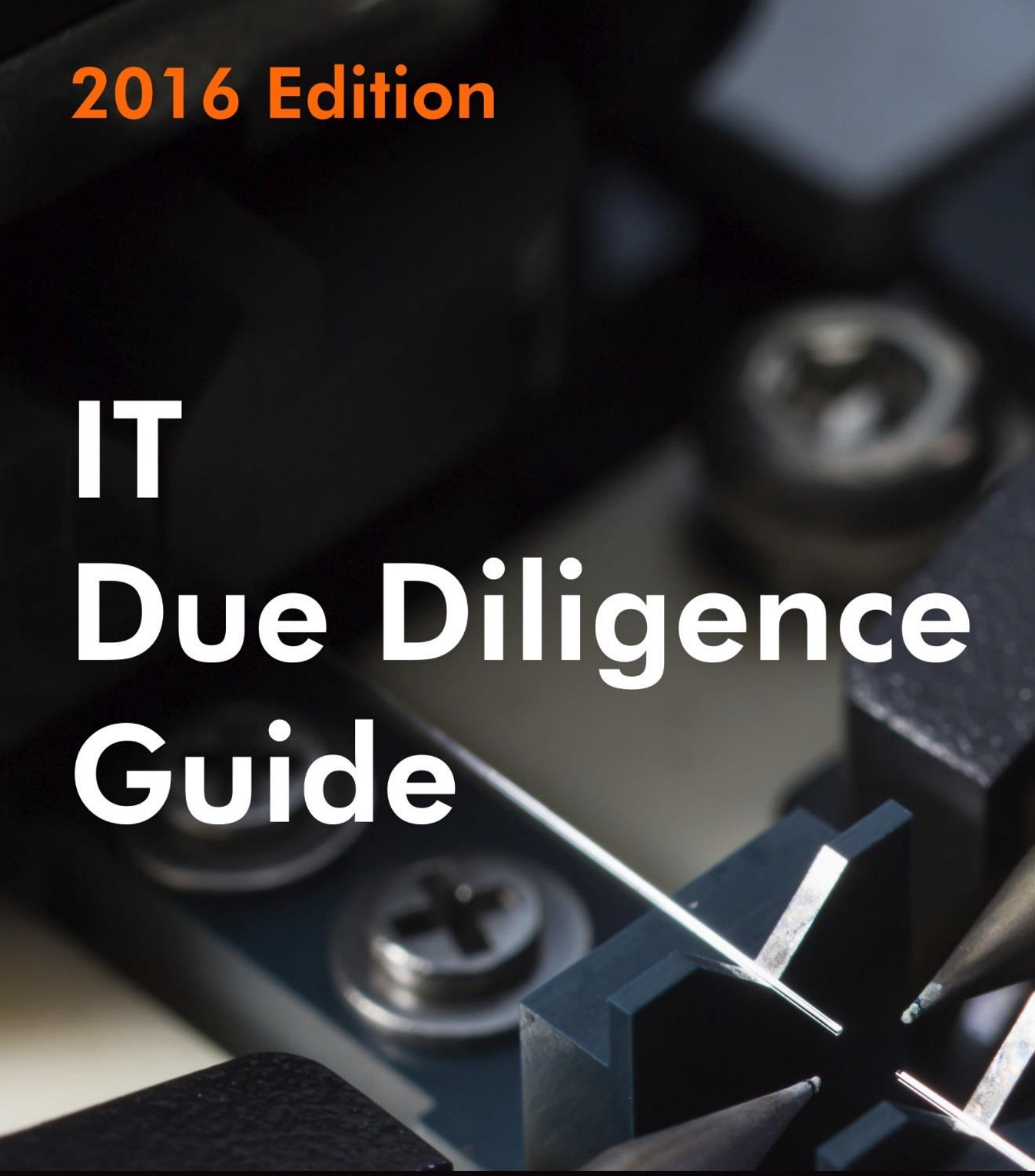

2016 Edition

IT Due Diligence Guide

Jim Hoffman

ISBN: 978-0-9961348-3-5

TABLE OF CONTENTS

INTRODUCTION TO THE 2016 EDITION

The need to include an IT review during M&A due diligence is greater than ever. Identifying IT shortcomings that can put a company's (and a deal's) future at risk is critical. Other issues that are uncovered that may not rise to the level of cancelling a transaction can still carry a high price tag to address, and it's important to find these problems prior to the deal closing.

According to the Boston Consulting Group, 63% of acquisitions are completed by companies that purchase no more than one company per year. [1] It's not reasonable to expect that such companies have resources dedicated to M&A, let alone an IT due diligence expert. This book can help to fill that gap.

2015 and early 2016 saw the trends of substantial data breaches and related public relations disasters continue. Examples included Costco, CVS and a giant breach (as in 78 million+ records) at the American health insurer Anthem. And who can forget the fallout from the Ashley Madison debacle? Smaller companies are by no means immune to the same types of attacks.

The year also saw the expansion of underground hacker markets,[2] where one can purchase stolen credit card data, online banking credentials, passports and hacking software, complete with 24/7 customer service, free trials and money-back guarantees. Or perhaps you're looking for a million stolen frequent flyer miles, a hacking tutorial or the login and password for a Gmail account? All are available.

This means the threats to all companies and the related risks in M&A transactions are increasing. A 2015 UBM Tech survey of 185 IT professionals at medium and large companies revealed that 76% of those surveyed were only "somewhat" or "not very" confident that they can prevent a cyberattack, and that's probably an optimistic number. Three percent of the survey respondents felt that they were "almost certain to get breached." [3] A 2015 KPMG survey showed that only 53% of healthcare systems (i.e. hospital chains) in the US consider themselves ready to defend against a cyberattack. [4]

In fact, many security experts now see hacking as something that can't be prevented, accepting the fact that it's almost inevitable when a skilled and determined criminal is involved, and more as something to be quickly detected and mitigated.

These developments have led to a new way of thinking during IT due diligence. Not that many years ago, a hacking incident would have probably been difficult to get past when evaluating a company. With so many large company data breaches demonstrating how hard it is for even organizations with supposedly sophisticated IT resources to protect against determined hackers, it seems unfair and unrealistic to look at past IT security shortcomings at a smaller target company as a deal killer. The focus now must be on lessons learned, process improvements and the current level of vigilance at the target.

For 2016, the *IT Due Diligence Guide* has been expanded and updated to address the latest IT security concepts. Questions have been added, explanations have been revised and there is a new appendix listing helpful resources. Recognizing the need for specialized expertise in certain situations, a new section discusses additional audits and reviews to consider including during an IT due diligence project. Finally, a post-transaction IT integration plan template is now part of the book package.

AUTHOR'S NOTE

I've been lucky to work in a number of companies that have been very active in M&A.

I've participated in due diligence projects on both the buy and sell side. In some cases I've lead the due diligence team, in some I've worked on only the technology aspects, and sometimes I've been the only person responsible for the entire due diligence effort. The values of the transactions have been as low as a $50,000 investment and as high as a $375 million company sale.

I've been involved in the acquisition and evaluation of technology companies for over twenty years. The due diligence process explained in this book includes the practices that I've found to uncover the most useful information during due diligence.

The book is certainly not an academic exercise. It focuses on real-world examples and experiences. My goals were to provide information that I was only able to gain through trial and error and to give the reader a head start on the IT due diligence process through the advice in the book and the additional material such as the report templates and data collection spreadsheets.

This book is intended to be a valuable tool in a broader due diligence effort that should involve legal, financial and accounting experts, at a minimum. The information in the book can provide an excellent base for further discussions involving technology subject matter experts, and should not be the only resource related to technology due diligence.

I'm located in the United States, and my due diligence experience is based on US transactions. Although I believe that the majority of the information in the book is applicable in most places in the world, there may be some local differences in the due diligence process and customs.

Finally, let me state that this book is not a substitute for obtaining expert professional advice. Acquisitions and mergers are inherently complex. Both sides in a transaction should retain expert legal, financial, accounting and subject matter experts to represent their interests.

Thank you for purchasing the book.

Jim Hoffman
March, 2016

DOCUMENT CONVENTIONS

Throughout the book, I'll refer to the acquiring or investing company as *AcquiringCo* and the target company as *TargetCo*.

The majority of the book is structured as a series of topics with questions from the IT due diligence checklist that comes with the book. Each question is followed by an explanation of why the question is being asked and what the responses might tell *AcquiringCo* about *TargetCo*, and maybe most importantly, any appropriate next steps and follow-up questions that will help you to draw out the most useful information during the process.

Each due diligence request is marked with one or more of the following icons:

	**Informational request.** Many of these due diligence request responses will serve as the basis for further discussion. It would not be surprising if *TargetCo* can't supply all of the information requested, or if large company best practices are not being followed. These issues can usually be remedied after the transaction closes without significant expense or risk. These requests can also be used to begin integration planning.
	**Important request.** Depending upon the answer received, you may have concerns about *TargetCo's* qualifications or professionalism. Issues identified can be addressed, but there may be significant expense involved.
	**Critical request.** Unsatisfactory responses to these requests may be significant enough to consider abandoning the transaction or considering an allowance or adjustment in the transaction pricing or other terms.
	A question that should only be asked when you're face to face with the *TargetCo* staff. Don't include this question in your written due diligence request list.
	A data collection spreadsheet for this due diligence request is included with the book materials.

CHAPTER ONE

IT Due Diligence Overview

First, what is due diligence?

I like the definition in Wikipedia:

"The examination of a potential target for merger, acquisition, privatization, or similar corporate finance transaction, normally by a buyer." [5]

Due diligence can also be used for an internal review during a strategic planning or budgeting process, or prior to an investment without an acquisition, but most of the time it's related to an acquisition or merger. In addition, some proactive companies perform a "self-audit" due diligence on themselves in anticipation of a sale of the company.

IT due diligence is a specific focus on the technology-related products, services and resources of an organization.

Until fairly recently, IT due diligence too often wasn't considered critical to the overall due diligence process, even when the target was a technology company. In some cases, I've seen the people running the financial aspect of the deal treat IT due diligence as little more than an afterthought.

Fortunately that's changing. In a survey on the ITDueDiligenceGuide.com website, 88% of M&A professionals indicated that technology is now an important part of their due diligence projects. That's very encouraging, and it makes it all the more important to do an effective job since IT due diligence is now much more in the spotlight.

The Big Picture

IT due diligence has two broad goals.

The first is to determine whether or not the deal should go forward as planned – are there any insurmountable risks? If something truly troubling is identified, the transaction could be abandoned. More likely, you might uncover

issues that warrant a change to the price of the deal. For example, if you discover a software licensing issue that would cost $250,000 to remedy, that might very likely result in an adjustment to the purchase price.

Assuming that the deal will go forward, the second goal of the due diligence process is to gather information such as network diagrams, vendor lists and product plans. This will also include the identification of potential new products and opportunities for cost savings. These efforts set the stage for integration of the target.

Transaction Strategy

Before the IT due diligence process begins, it's very important that everyone involved understands the overall strategy behind the transaction.

Very often, *AcquiringCo* is hoping to leverage *TargetCo's* technology in its own business, and the plan is to integrate the *TargetCo* employees and operations. In this case you care very much about all of the operational details at *TargetCo* and the logistics of integration, and this is usually the deepest due diligence dive.

Sometimes the goal is simply to become an owner or investor in *TargetCo* and to run it as a standalone company. If so, it's most important to understand that the business is solid, to identify potential cost savings and to confirm go-forward expenses, but it's less critical to consider things like consolidating data centers or integrating teams of employees.

In the case of a startup, it's possible that *AcquiringCo* is mainly interested in the people at *TargetCo* and the ideas they can generate. The plan might even be to eliminate the products that *TargetCo* currently offers. In that case, you'll care much less about the details of how the technology has been implemented or how up to date the web servers are, for example, and you'll need to focus on the people at *TargetCo* and their skills.

The strategy behind the deal will determine how you spend your time, the questions you ask and the content of the report you write, so it's critical that everyone on the team understands it.

The Due Diligence Steps

How does a seller find a potential buyer? One of the best things to do is to network with others in the same industry or niche. Obviously, networking has many other benefits, but one of the most significant is getting to know the people you may later look to as potential acquirers or partners. These relationships don't develop overnight, so you should probably be networking years before you hope to sell.

Even if someone is not actively marketing their company for sale, they may appear on the radar of a competitor, a private equity or venture capital firm, and could receive an unsolicited inquiry about their interest in selling.

Before getting past the most basic of conversations about the sale of a company, it's in both parties' best interest to sign a non-disclosure and/or confidentiality agreement. The buyer will understandably want to know more details about the seller's business than the seller would wish to provide without any protection, and the buyer will probably also disclose some of their future business plans at this stage. It's important that both sides are protected as they exchange initial information, and a qualified attorney should be involved on each side to review the confidentiality agreement. The seller will need to engage an attorney who's worked on company transactions before, so this may be someone other than their existing attorney if they already have one.

Once a confidentiality agreement is in place, there is normally a period of initial, informal due diligence. This means the buyer is seeking enough information, at a high level, to determine whether the business is worth buying. Is it profitable? What are the products? What are next year's revenue projections?

At this stage, it's not unreasonable for the buyer to ask for at least summary financial statements and projections. This isn't full-blown due diligence, however. Even though the seller has signed a confidentiality agreement, they should be selective in the information they provide to a potential acquirer, especially if they're competitors. Once the information is out, it's out. Things like customer lists, contracts and detailed future product plans are usually not divulged at this point.

If the seller knows at this point that there is an issue that might cause the buyer concern, such as a significant lawsuit or a government investigation, it's

wise to disclose it to avoid wasting everyone's time. On the other hand, if the seller just signed a new customer to a five year contract that's going to increase its revenue by 20%, they should consider providing at least some level of detail as it could increase the price the buyer is willing to pay.

If the potential acquirer gets to the point where they want to move ahead with a purchase, they will typically present a letter of intent, or LOI. The LOI summarizes the terms of the proposed deal and will usually include items such as the purchase price, any earn-out (a future performance-based payment) and an employment agreement summary for key executives and staff at *TargetCo*. It will also normally indicate other terms, such as deadlines, exclusivity and the fact that the business should continue to be run in its normal fashion.

If the seller wishes to proceed with the deal and didn't get an attorney involved up to this point, they'll definitely want to do so before signing the LOI. Without proper language, the LOI can effectively become a sale contract.

This part of the transaction can benefit from additional outside advisors. An accountant can be very helpful in putting together projections and presenting financial information in the best way.

In addition, if the seller hasn't been through a business sale or purchase before, they may want to obtain a financial advisor familiar with their industry to help with the negotiation process. This expert can educate the seller as to what's reasonable to discuss and what's not during the informal due diligence process, and can serve as a guide throughout the more detailed due diligence to come after the LOI is signed. They should also be familiar with how similar companies have been valued in recent transactions.

After the LOI is signed, the parties will normally enter the formal due diligence phase.

The IT Due Diligence Process

The first step in IT due diligence is to establish contact with *TargetCo*. This is typically a senior executive. I'll usually have a phone call with this person to gather some high-level background information on the company, schedule a site visit and determine the appropriate *TargetCo* technical contact.

Prior to the call, I gather public information from *TargetCo's* website and other sources such as Google and LinkedIn, and review any relevant information that

may have already been gathered during legal and financial due diligence, if that's already occurred (which is typical). Many times in the overall process, IT due diligence doesn't occur until there's a comfort level with the financial and legal due diligence. There's no need to get down to more detailed investigation if the big picture isn't attractive to *AcquiringCo*.

On the phone call with the business contact, I always like to agree on a "cover story" for the site visit. Since in most cases the transaction isn't public knowledge, you'll need to be on the same page as your *TargetCo* contact as to why you're there. Typical explanations are "we're exploring a business relationship," "we're considering a partnership" or "the owners wanted an independent review of our technology."

Whatever is decided, be sure that if you'll have a future relationship with the staff at *TargetCo* that the cover story isn't an outright lie, as that's certainly a poor way to begin your relationship.

It's also important to gain an understanding of who at *TargetCo* has knowledge of the transaction (so you can speak freely with them) and who doesn't.

After your initial contact with *TargetCo*, your next step typically is to reach out to a designated technical contact and provide them with a list of due diligence requests. This is the checklist that came with the book and is available on the website.

You should edit the checklist depending on the overall deal strategy and the particular business you're investigating. The checklist is intended to be comprehensive, and it's unlikely that you'd want to ask every question in every due diligence effort.

Preferably, you'll get a response to many of the items on the list before your site visit, which is the next step.

The Site Visit

The heart of the IT due diligence process is the site visit.

For a small acquisition, the site visit might only last one or two days, and it can be a week or longer for a larger transaction. However long it takes, the daily process I follow is the same.

During the site visit, you should be able to meet with key IT staff, or even all of them if the company is not too large. If appropriate, you'll also want to schedule product demos and set aside time for presentations on things like system architecture and database layouts.

You're there to obtain more detailed information based on the previous information you've received, either through the prior submission of the due diligence requests from the checklist or your on-site observations and interviews.

I normally spend the evening of each day onsite reviewing my notes and using them to create follow-up questions.

Gathering information onsite is critical. If you rely solely on the responses to your due diligence requests, you can potentially miss important things that you'll only see if you're walking around and talking with people.

One of my favorite examples of what you can see only in person happened during a site visit to a company where the CIO was very proud to show me the data center he'd built. It was fairly standard except for the big blue tarp over the racks. When I asked him what it was for, he said they had to cover things up because the forecast called for rain, and the roof leaked.

Another example occurred at a company whose office was on a lake. While I was walking around the outside of the building, I could see a line about five feet up on the walls of the building. I asked someone what it was from and they said it was where the water had risen the last time the lake flooded. It wasn't really a problem they said, because the servers were on the second floor...

No one is going to put things like this in a response to your checklist requests – you have to see them with your own eyes.

The IT Due Diligence Report

After the site visit, you'll want and need to create a final report that details your findings and recommendations. During the process of creating the report, it's normal to have follow-up questions for your technical contact as you review the information you gathered. A sample IT due diligence report template is included with the book.

As a final step, depending on the information found during the overall due diligence process, a "go / no-go" decision is made about the deal. If the

transaction closes successfully, then the information gathered during due diligence is critical to the integration process.

Integration

IT due diligence has many benefits when it comes to determining and confirming the value of a technology transaction, but it can prove to be at least as valuable in planning the post-transaction integration. IT due diligence can assist in the integration process in a number of ways.

Staffing

The first is staffing planning. If the target company is being folded into the acquiring company, it's critical to have a good sense of the strengths, weaknesses and personalities of the *TargetCo* technology staff. This will allow you to make better decisions when planning an integrated IT or software development team.

If you determine through IT due diligence and integration planning that there will be skill gaps in the combined company, proper budgeting can take place and recruiting can begin sooner.

If a premise of the transaction is that IT staff cuts and the related expense reduction will be possible, IT due diligence can identify whether this is really practical. For example, are there key proprietary systems or tools used by *TargetCo* that are maintainable by only the person who developed them? That person had better not be on the list of people to be terminated after the transaction closes. IT due diligence can confirm whether staff reductions are feasible, and if so, the best way to achieve them.

If the *TargetCo* staff will be required to conform to *AcquiringCo* standards in the areas of coding, security and other technology processes, training can be planned prior to deal close so the integration of the teams can begin right away.

Validating Cost Savings

IT due diligence also helps to achieve the anticipated cost savings that are expected from integration. Many technology transactions assume that there will be expense reductions in areas such as telecom contracts, hosting, hardware, software licensing, etc. IT due diligence can confirm that these potential savings exist, and identify the path to achieving them.

Licensing is an important area to review. There may be a cost involved in transferring key software licenses to a new organization. Don't assume that an "enterprise" license simply converts to the new, larger enterprise without additional license fees.

Similarly, a termination notice date for a high cost contract may arrive just after the transaction close date. If IT due diligence occurred prior to closing, this date should have been identified and the integration priorities planned to accommodate contract termination and the technical and operational steps required to achieve the expense reduction.

Developing Staff Trust

If you're able to include someone from *AcquiringCo's* technology staff in the IT due diligence process, it can help the integration process by way of whatever rapport the teams developed during the due diligence site visit. If the IT due diligence team made the *TargetCo* staff feel comfortable, that can lessen the post-deal jitters that are natural when a company is acquired.

Integration Plan Development

When a public company is involved in the transaction, it's often difficult for the two parties to cooperate in the integration planning process prior to the closing of the deal. In the case of private parties, there may be more flexibility. In any case, at least the *AcquiringCo* can begin to make integration plans based on its due diligence.

The integration of even a fairly small company may take three to six months. A plan for such a long effort takes time to develop. If the planning can take place prior to the closing of the deal, it makes it more likely that the integration can get off to a good start and ultimately be successful.

Depending on the intent of the integration, the following issues may need to be addressed in the plan, and all can be shaped by the information gathered during IT due diligence:

- Post-transaction product strategy and offerings
- Physical space (offices, data hosting, etc.)
- Email, phone system and network integration
- Security and coding standards
- Technology conversions

- Risk identification
- Integration plan metrics

As you can imagine, it's better to start working on these things before the transaction closes, and with a detailed understanding of the underlying technical issues at *TargetCo*. Good due diligence leads to a good integration plan and a good integration plan increases the chances of a successful integration.

CHAPTER TWO

Due Diligence Requests

The following chapters organize the due diligence requests into logical categories matching the sections in the IT due diligence checklist that comes with the book.

It would be very unusual for every one of these questions to apply to a particular due diligence effort. I recommend that you utilize the initial information gathering process to determine the due diligence requests that are most applicable to *TargetCo*. If you overwhelm your contact with a huge list of requests upfront, you'll likely get pushback from *TargetCo* and you'll also probably soon hear from the unhappy person in charge of the overall due diligence effort at *AcquiringCo*.

Keep the initial due diligence request list limited to the items that will help make your onsite visit more productive, and cover the other issues that you think are important in person.

The IT due diligence checklist template included with this book is numbered. It's a good idea to number the requests, as it makes it easier for you to track the responses and for your *TargetCo* contact to indicate the request to which they're responding. There is less confusion for everyone if the files provided by *TargetCo* as they respond to the due diligence requests include the item number in the file name.

Many due diligence projects utilize a virtual "data room." This is a service or website that manages all of the documents and other information gathered during due diligence and securely stores it. The checklist includes a column to indicate the location or identifier in the data room if you're using one.

Finally, some questions are sensitive or otherwise best asked in person instead of in writing, and those are noted in the discussion where applicable, along with the appropriate icon.

CHAPTER FIVE

Software Development Process

DUE DILIGENCE REQUEST

A description of the version control process and system(s) utilized.

WHY THIS IS IMPORTANT

A version control system allows every change to a project's source code to be tracked and stored. Think of it as the vault for the software, which in many cases can be a company's most valuable asset.

Sometimes a new version of a software product or website can cause unexpected problems in the real world, even when it's been tested prior to being released. In that situation, a version control system allows the company to "roll back" the software to an earlier, stable version very quickly and easily. A version control system also protects against accidental deletion of source code on a developer's computer.

Popular version control systems include Git, GitHub, Bitbucket, Microsoft Team Foundation Version Control and Subversion.

Even when there is only a single developer, a version control system is very useful. If *TargetCo* doesn't use any type of version control process or tool, it's often a sign of amateur software development.

DUE DILIGENCE REQUEST

A description of the process for approving and developing new software products or features.

WHY THIS IS IMPORTANT

You want to know if there is good control over the company's technology direction. There are many potential follow-up questions. Is there a plan or just

reaction to problems? Does *TargetCo* have the business domain experts to develop its own ideas, or are all product features the result of customer suggestions? Is there a product manager? Are requirements documents developed? A traditional practice is a functional requirements document, which explains *what* the new feature or product does, and a technical specifications document, which defines *how* it is to be developed.

Are new market opportunities carefully considered, or are resources committed without adequate research and thought? Does *TargetCo* perform competitive and market analysis before embarking upon new product efforts? You want to get a sense of the care of the decision-making at *TargetCo* before they start spending *AcquiringCo's* money.

Be particularly wary of a company that developed its main product based on the needs of one early or large customer. In this situation, the product that has been built may meet the specific needs of that one customer, but may not be something needed or desired by the market at large. If this client is the source of most new product or feature ideas, consider it a warning sign.

DUE DILIGENCE REQUEST

A description of any outsourced software development arrangements and copies of the related agreements.

WHY THIS IS IMPORTANT

If *TargetCo* outsources or offshores any critical software development or IT functions, there are a number of issues to investigate:

- What is *TargetCo's* future ability to support the software if it was not developed in-house?
- How well-documented is the software?
- Does *TargetCo* physically possess or own the legal rights to the source code? There are many issues around contract language and proper copyright assignment when it comes to contracting for software development. You can easily end up not owning the rights, even for custom development, without the proper contract language in place. At the same time, in certain states and countries, you can inadvertently

Does the *TargetCo* software development team perform code reviews? In a code review, programmers examine each other's source code to provide a "second set of eyes" to identify bugs and vulnerabilities and to help ensure that the original developer implemented a good solution. Code reviews can be very helpful in identifying security risks.

Source code review tools exist that can automatically scan source code for these types of common errors. This may be an option worth considering if your high-level investigation of *TargetCo's* security awareness during software development reveals any areas of concern.

DUE DILIGENCE REQUEST

A description of the software development coding standards used by the company.

WHY THIS IS IMPORTANT

A professional software development organization, no matter the size, will have this. A coding standards document lays out the in-house programming standards, naming conventions and the specific technology choices that will be used in the company's software development efforts.

Without a defined and enforced process, every developer may create software source code with a different style and technique. This makes is difficult for another employee to take over the work, and for a new employee to come up to speed on the company's source code. A lack of coding standards can make the company very dependent on a specific employee to always be available to support a piece of software.

I've seen independent, individual developers with a coding and naming standards document to keep their own work organized and consistent, so it's not too much to expect that this exists in a company of any size or maturity.

DUE DILIGENCE REQUEST

Explain the company's mobile development strategy.

WHY THIS IS IMPORTANT

In 2014, various studies of Internet traffic showed that, for the first time, mobile usage of the Internet exceeded that of desktop. The gap widened in 2015. [7] This means that if *TargetCo* has a website, you'll want to be sure it works well on mobile devices.

This is especially important if there is any ecommerce component to the site. Companies without a website that is usable on phones and tablets will be at more and more of a disadvantage going forward, and could be losing sales.

In addition, in February 2015, Google announced that it would soon begin to more heavily weight the mobile-friendliness of websites when calculating its search result rankings. [8] If *TargetCo* counts on search engine traffic from Google, this should be a key consideration.

There are a number of software development approaches that can accomplish the task, including responsive web design, a designated mobile site or native mobile apps.

If no one at *TargetCo* can explain the thought process the company has gone through up to this point regarding mobile strategy, consider that to be a warning sign.

If *TargetCo's* market situation requires a mobile presence and one does not already exist, you'll want to consider that in the post-integration budget and the overall cost structure of the transaction.