TREXIN INSIGHT PAPER

August 25, 2020

TECHNOLOGY DUE DILIGENCE

It doesn't have to take very long.

Every year, billions of dollars are allocated to technology-specific mergers and acquisitions. In the end, protecting the initial merger and acquisition (M&A) investment is key and a significant variable of that protection is obtained through proper IT M&A due diligence. Nothing is out of scope. It is essential that all talent, processes, products, and systems are analyzed for effectiveness and reintegration. You must weigh questions about their strategic impact on future goals or relevance of inclusion.

Technology valuation often plays a strong part in both the pre-M&A and post-M&A stages. Typical issues often raised include growth uncertainty, internal controls structure and compliance, and liability exposure.[1] Whether it be an M&A or current state analysis to attract buyers, technology investigations and assessments can provide high-level essential intelligence on your organization's strengths, risks, and opportunities. There are multiple cases of failed IT due diligence during the M&A cycle, such as Marriott's Starwood acquisition cybersecurity breach or the UK's Sabadell purchase of TSB where customers encountered multiple costly glitches on newly migrated systems. These failed cases are extreme examples of a proper lack of IT due diligence and executions.

Trexin's leaders have decades of experience leading large and small technology due diligence engagements, ranging from assessing security procedures, costs and strategies for outdated systems, analyzing the gaps between new strategies and existing governance and organizational models, etc. Whether you require outside expertise/assistance or are preparing an internal assessment, our firm believes a well-defined structured approach can be extremely simple and swift. Trexin's key insight is that it is often good enough to complete technology due diligence in matter of days rather than weeks or months, enabling M&A decisions to be made rapidly and represent a competitive advantage versus slower players.

The reality is that a go/no-go decision can be driven by qualitative risk analysis, delaying quantitative cost-of-remediation estimation to a later phase. Trexin has been successful leveraging two techniques—arranging the due diligence process in an "Early Knock Out" tree, and "Follow the Data"—which we discuss in the following sections.

Trexin's key insight is that technology due diligence can be completed in days, by focusing on two techniques.

1. "Early Knock Out" Tree

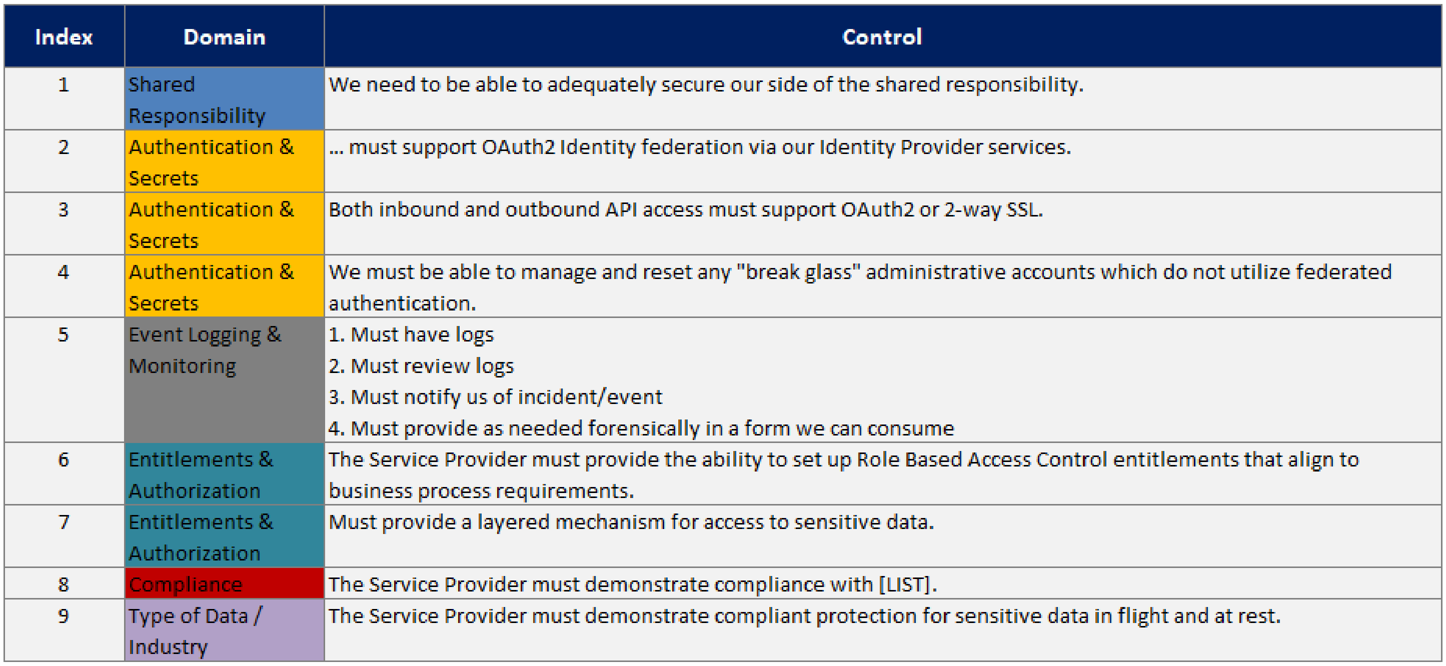
You the reader may well have participated in lengthy questionnaires, perhaps as a vendor or for clearance such as security. If the purpose is to gather information about someone for a database, then understandably the questionnaire is as lengthy as the applicant can bear. But if the purpose is due diligence, then reordering the questions can dramatically reduce the time to complete the assessment. Essentially, Trexin recommends creating a hierarchical tree of yes/no questions arranged to "knock out" applicants as soon as a critical risk/flaw is uncovered. The key "ah ha" is to

[1] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/Real%20Estate/us-engineering-construction-ma-due-diligence.pdf

invert the objective from “does this company pass our assessment” to “let’s try to eliminate this company”. Essentially, survivors are winners! For example, let’s consider a typical Vendor Security Questionnaire, as a simple type of due diligence. If you arrange it by security domain there are 26 questions to ask/answer:

Index	Domain	Control
1	Shared Responsibility	All security controls in this list must be configurable using self-service…
2	Shared Responsibility	We need to be able to adequately secure our side of the shared responsibility.
3	Data Protection	Encryption of data fields must be…
4	Data Protection	We must be able to select which data fields are encrypted…
5	Data Protection	Secondary layers of encryption must be…
6	Data Protection	Key management activities must be…
7	Data Protection	We own, manage, and have sole custody of encryption keys…
8	Data Protection	Application, database, filesystem, and storage keys…
9	Data Protection	… access to the keys or any data protected by the keys.
10	Data Protection	Keys and key storage vaults must not be shared with or available to any other clients…
11	Data Protection	All systems that contain or process our data must implement logical segregation from other customers…
12	Authentication & Secrets	… must support OAuth2 identity federation via our Identity Provider services.
13	Authentication & Secrets	User or batch access… must also utilize our federated Identity Provider services.
14	Authentication & Secrets	Both inbound and outbound API access must support OAuth2 or 2-way SSL…
15	Authentication & Secrets	We must be able to manage and reset any “break glass” administrative accounts which do not utilize federated authentication.
16	Authentication & Secrets	We must control 2nd factor authentication of any "break glass" administrative accounts.
17	Pre-Production Environments	No privileges spanning Development, Testing, and Production environments.
18	Pre-Production Environments	No Production data in non-Production environments.
19	Use of Cloud Vendors & Services	Any vendors or other 3rd parties who provide functionality need to conform to this list as well.
20	Event Logging & Monitoring	1. Must have logs 2. Must review logs 3. Must notify us of incident/event 4. Must provide as needed forensically in a form we can consume
21	Entitlements & Authorization	The Service Provider must provide the ability to set up Role Based Access Control entitlements that align to business process requirements.
22	Entitlements & Authorization	Any Service Provider access to our data must be authenticated and authorized.
23	Entitlements & Authorization	Access to keys used to decrypt data must be tied to the currently logged in user/role.
24	Entitlements & Authorization	Must provide a layered mechanism for access to sensitive data.
25	Compliance	The Service Provider must demonstrate compliance with [LIST].
26	Type of Data / Industry	The Service Provider must demonstrate compliant protection for sensitive data in flight and at rest.

But reordering the questions to ask just the critical ones first, there are only 9:



Index	Domain	Control
1	Shared Responsibility	We need to be able to adequately secure our side of the shared responsibility.
2	Authentication & Secrets	… must support OAuth2 Identity federation via our Identity Provider services.
3	Authentication & Secrets	Both inbound and outbound API access must support OAuth2 or 2-way SSL.
4	Authentication & Secrets	We must be able to manage and reset any "break glass" administrative accounts which do not utilize federated authentication.
5	Event Logging & Monitoring	1. Must have logs 2. Must review logs 3. Must notify us of incident/event 4. Must provide as needed forensically in a form we can consume
6	Entitlements & Authorization	The Service Provider must provide the ability to set up Role Based Access Control entitlements that align to business process requirements.
7	Entitlements & Authorization	Must provide a layered mechanism for access to sensitive data.
8	Compliance	The Service Provider must demonstrate compliance with [LIST].
9	Type of Data / Industry	The Service Provider must demonstrate compliant protection for sensitive data in flight and at rest.

Moreover, a failure on any of those critical questions forces a Knock-Out even earlier. As an additional bonus, creating this tree requires a strategic discussion with Business Leaders that we usually find benefits them as well (e.g., “You say this factor is critical. So are you willing to walk away from the deal if the answer is weak? No? Well then, let’s talk through this…”).

2. “Follow the Data”

In essence, due diligence isn’t about assessing strengths, it is about uncovering weaknesses (which are risks that need to be managed either by mitigation or by adjusting the valuation of the deal). In the decades that Trexin subject matter experts have led or been involved in technological due diligence, one key technique has never failed to uncover weaknesses in a matter of days. That technique is to focus on how data is stored and managed, at rest and in flight, throughout the Software Development Lifecycle (SDLC). There are several factors that contribute to the success of this technique:

- Data has always been a key proprietary asset for companies, although arguably Coca-Cola’s formula is easier to hide than the terabytes and petabytes crunched by today’s giants (e.g., Google, Facebook, Amazon).
- Data is arguably more valuable today, with the advent of Data Analytics, Machine Learning/Deep Learning, etc. at the forefront of driving more business value.
- Data is harder to protect than in pre-Internet days, due to sheer size, interconnectivity, and more sophisticated dark techniques.
- Non-production environments are typically (and understandably) less rigidly controlled and monitored than production environments. Attacks are easier, either directly on production data pulled into these environments, malicious code injected in these environments, or system access breached in these environments.

Our experience shows that tracing data (and code production) from the beginning through the end of the SDLC quickly uncovers the cut corners and unmonitored environments that represent some of the biggest vulnerabilities and risks in the entire enterprise.

Final Thoughts

Technology leadership and expertise will continue to be a primary driving role in ensuring an M&A transaction or current state innovation is executed properly. Over the last few years, the IT function has become more and more relevant to the success of transactions. Nevertheless, the impact of the target's IT consistently remains underestimated, which leads to differing ways of handling the IT function during the due diligence process. Assessments leveraging our "Early Knock Out" and "Follow the Data" techniques enable you to quickly document baseline risks, conceptualize talent vacancies across your human capital, codify product and migration roadmaps, realize IT supervision and management competency levels, understand system vulnerability and ageing, seize on pockets of capitalization, and harvest existing information. An IT due diligence report is an ideal first step towards promoting your IT attractiveness to buyers or stabilizing IT needs during an M&A integration.

We hope that these insights help you with your challenges. For any follow-up questions, comments, or concerns – please reach out to Trexin Consulting as we would love to continue the conversation.

This TIP was written by Trexin's Chief Security Officer and Technology Capability Lead, Glenn Kapetansky, and Joe Oliva, a Trexin Associate. They welcome comments and discussion on this topic and can be reached at glenn.kapetansky@trexin.com and joe.oliva@trexin.com.