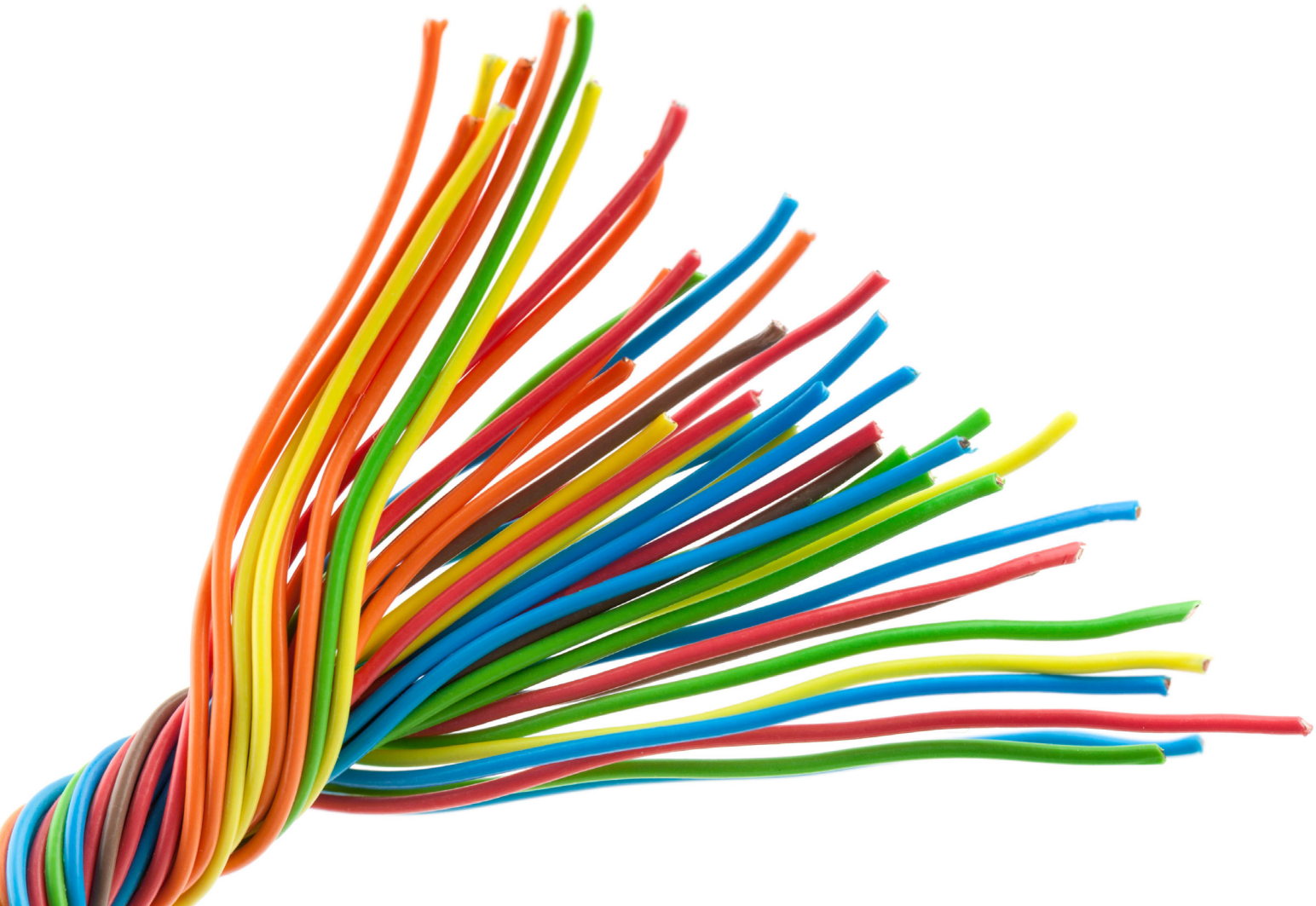
Deloitte.

Deloitte M&A Institute

Thinking logically about "Logical Separation"

Part of the *Wired for Winning* series on M&A technology topics



During a carve-out, asset sale or spin-off, there is often insufficient time or readiness to fully separate the Information Technology (IT) infrastructure—systems, applications, and/or co-mingled data on a server or in a database—by deal close. As a result, an increasing number of M&A deals include Transition Service Agreements (TSAs), a short-term arrangement in which the seller continues to provide services to the buyer. TSAs provide the buyer with the time required to stand up their own infrastructure over this interim period, while they provide the seller with additional time to physically separate the applications and infrastructure. However, they also pose a substantial risk for the seller as the applications and infrastructure are not separated, and this provides the seller with an unrestricted access. Key control functions (e.g., Operational Risk, Information Security, Legal) often require the buyer to put restrictive controls in place for the period of the TSA. The seller and buyer legal groups often have the most important role to play in making this determination, and provide guidance on the extent of separation needed.

As IT services may comprise more than 50 percent of a TSA agreement's scope, the seller's and buyer's operational leadership must address three very important questions: What is the extent of safeguards that the Control Functions require to be put in place to mitigate the risk of unauthorized access to each other's data, especially since it resides (for the TSA period) in the same place? How many safeguards are enough? What are cost implications?

Complicating factors

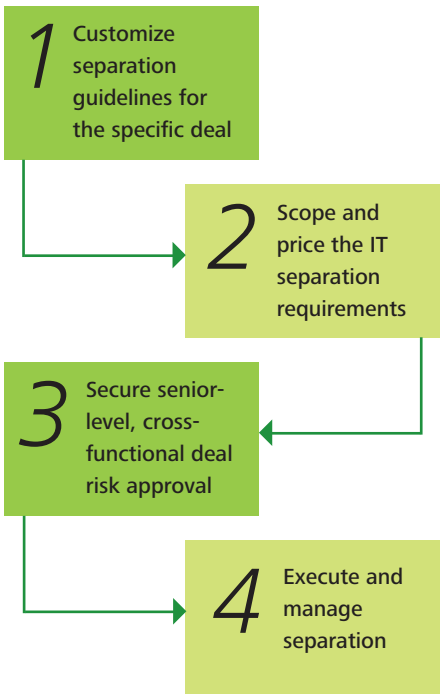
There is no simple answer to the conundrum of how much TSA-related IT security is enough—each situation is unique, with the risk profile of the industry and the companies themselves serving as influencing (and complicating) factors. A recent rash of high-profile data breaches is prompting some corporate Control Functions (e.g., Legal, IT Security, Finance, Regulatory, Audit) to call for a complete physical separation of IT systems and databases as soon as possible after a deal closes. This is particularly true for the seller, as typically it is their IT infrastructure that they want to safeguard. However, a complete separation may take up to two years to finalize, may be costly, and may add considerably to IT departments' workloads. In the meantime, employees at both companies need IT access—but who gets how much?

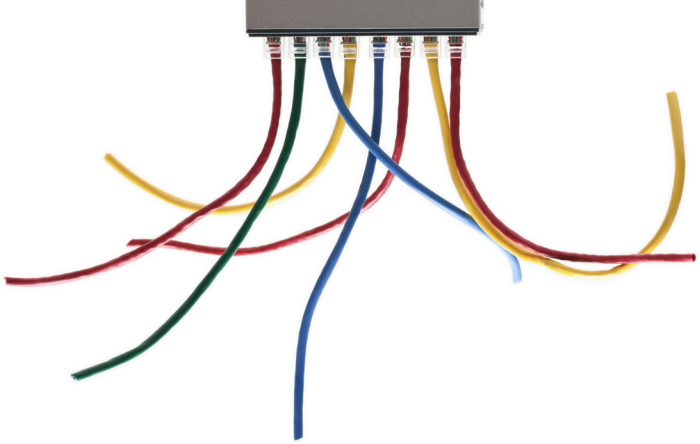
We have seen some companies adopt a "black or white" mindset when controlling TSA-related access. One risk-averse approach is to set requirements based solely on the seller's internal third-party access/data privacy policies. While this is a reasonable place to start, operational leaders may find that meeting the full requirements of securing third-party access (e.g., firewalls, data separation, split application layers, etc.) can be onerous, expensive, and often not feasible in a fast-paced M&A deal environment. The opposite approach is to provide access controls only around the most sensitive systems and applications, which can expose a company to internal and external cyber threats. Both approaches can be counterproductive to a deal's goals and ultimate value. In order to minimize churn, it's important to engage the Control Functions early in the requirements definition process to ensure alignment with business objectives.

Fortunately, a "logical separation" approach can provide IT executives with a halfway house between the two extremes by putting in place sufficient controls and monitoring processes to protect a co-mingled IT infrastructure until complete separation takes place.

Standardized approach to determine level of separation

Based on our experience, each provider of TSA services needs to thoughtfully (but quickly) set IT-related guidelines that are based on a holistic review of deal terms and the combined risk posture of the two organizations. Following the standardized approach detailed below can help determine the level of necessary separation:





1. Customize separation guidelines for the specific deal
We have seen that business-oriented operational or technology owners typically drive guidelines definition, with inputs from Control Functions, the deal team, and technology staff.

Following is a list of important considerations:

- **Deal Construct**—The nature of the deal (spin-off, carve-out, and asset sale to strategic or financial buyer, joint venture) can impact risk and separation considerations. In the case of joint ventures or structures where the seller retains some control in the sold entity, for example, we have observed fewer separation requirements as a result of alterative management controls.
- **Deal and TSA Timeline**—The extent of logical separation varies by the deal and TSA timelines. Longer TSA durations often require more logical separation while quick TSA exits may require less. It's also important to realize that logical separation needs to be completed on Day 1, so sufficient time should be allocated for separation or the scope should be narrowed to meet the timeframe.
- **TSA Set-up Cost**—The two parties need to determine which funds the logical separation effort. We have seen this paid for by the seller (which often has to deal with the fall-out of not separating), by the buyer (for receiving the TSA services), or as a 50-50 split.
- **Competitive Nature of Buyer**—Logical separation is often more extensive for companies that either currently compete with each other or are likely to do so in the future. In one instance, we found extensive logical separation for a travel business because the seller believed that the buyer might enter the same market segment in which they are operating.
- **Potential Buyer TSA Needs**—If all IT infrastructure and applications are being TSA'd, logical separation is much more important. The fewer services the buyer needs (e.g., if it already has an IT infrastructure in place by Day 1), the less the amount of logical separation that is required.
- **Regulatory Environment**—Data privacy laws in various countries and industries (e.g., financial services) often require extensive logical separation on Day 1. A country-by-country and industry-specific analysis can help to determine where regulatory requirements may call for more separation.
- **Legal Environment**—In addition to regulatory requirements, country specific laws (e.g. use of customer/employee PII) or other legal requirements concerning sensitive information must be factored in to business decisions which will impact degree of pre-close logical/physical separations.
- **Current Risk/Audit Open Items**—Current risk/legal/audit open items and any recent attacks on the company's IT environment should be reviewed to determine the level of logical separation based on acceptable operational risk.
- **Internal Informational Security Guidelines**—A company's information security guidelines are an important input to and guardrails for separation guidelines. Expect the Chief Information Security Officer (CISO) to play an important role in scoping and finalizing the guidelines.
- **Legacy Approaches to Deals and Existing Tools**—General company guidelines on deal-making often include separation-related leading practices or lessons learned. Additionally, companies typically buy tools for a specific deal with the intent to use them for future deals. Reusing legacy approaches and existing tools should be considered when developing separation guidelines.
- **Not Competing with Ultimate Goal to Exit TSA**—Logical separation is a priority that has to compete with other inflight IT projects and the eventual physical separation. This could mean a heavy burden on existing IT resources. The opportunity cost of such separation should be weighed against other IT projects and the time to Day 1.
- **IT Asset Logical Separation Suitability**—Not all types of IT assets can be logically separated. Confirm with technical teams what is operationally feasible in parallel with discussions with Control Functions.

Finally, when defining guidelines, it is important to build flexibility into the timeline to enforce control measures. While a majority of these controls should be in place by Day 1 others can be migrated in 30, 60, 90, 180 days, depending on level of risk and time available.

2. Scope and price the IT separation requirements

The IT services addressed in a TSA separation plan should include all shared services with the divested or spun-off entity. Those services which typically receive the greatest focus include:

Area	Key components (illustrative)
Back-end infrastructure	Shared office, data network, voice network, servers and storage
End-user services	End-user devices, messaging, instant messenger
Access infrastructure	Active directory, identity access management, intranet
Applications	Single sign-on, contact center, file shares, TSA applications (forward and conveyed)

In addition, the various separation approaches and levels can be categorized into the following groups to help frame the scoping and pricing process.

Separation approach	Description
As-is	**Description:** The buyer continues to have unrestricted access to all seller IT infrastructure and applications. • Minimal to no separation. **Technical Implication:** Co-mingled applications and infrastructure. Buyer continues to have unrestricted access. **Cost Implication:** No direct logical separation costs to be incurred.
Terminate service	**Description:** The two companies do not set up a TSA for a service (e.g., email, payroll). • The buyer moves to its own IT infrastructure and services. No separation. **Technical Implication:** None. Seller continues to operate its IT environment as-is. **Cost Implication:** No direct logical separation costs to be incurred; may incur wind-down costs to terminate technology services.
Physical separation	**Description:** The two companies are physically separated as of Day 1 Close. The buyer either moves to its own IT infrastructure or uses a physically separated IT infrastructure from the seller. • High degree of separation and longer lead times to physically separate, resulting in impacts to the Day 1 timelines (if not planned well in advance). **Technical Implication:** Substantial efforts for technology resources to physically separate. For applications, effort is required to separate databases and also restrict buyer user access to applications. For infrastructure, effort needed to remove buyer users from various infrastructure components (e.g., network, emails, end user devices, etc.) Also substantial effort for historical data migration. **Cost Implication:** Substantial physical separation costs may need to be incurred prior to Close to physically separate infrastructure. However, overall long-term separation costs may be reduced via a phased approach of pre-close logical separation followed by end state physical separation.

Separation approach	Description
Logical separation—user access level	**Description:** The two companies restrict user access to IT infrastructure and applications. • An easier way to implement logical separation. • Examples include: – Restricting buyer employee admin-level access to seller servers – Restricting buyer employees from modifying application code by changing user access types **Technical Implication:** The extent of logical separation required dictates the technical implications. For applications, it's easier to logically separate through access controls, but it may not be possible in all instances. **Cost Implication:** Expect logical separation costs to be less at User Access Level versus full logical separation at database/application level. Will still need to incur physical separation costs post-close.
Logical separation—database/application level	**Description:** Logical separation at a database/application level is required when user access-level separation is not enough or not feasible. • Requires substantial changes to the code base. **Technical Implication:** Requires substantial effort from technology users. **Cost Implication:** Substantial logical separation costs may need to be incurred prior to Close to change database/application source code to create separation at DP/App. level. Will still need to incur physical separation costs post-close.
Monitoring/other controls	**Description:** Even after logically separating IT infrastructure, there may be some IT assets where logical separation is not possible or very costly. In such cases, additional monitoring controls (as requested by Information Security) are instituted. • Examples include: – Active directory monitoring through real-time monitoring tools – DLP scanning on new company emails and network access **Technical Implication:** For infrastructure, advanced monitoring is often put in place in addition to some logical separation for assets such as network, active directory, emails etc. **Cost Implication:** Logical separation costs will be incurred, plus any incremental IT/Security tools required to monitor environments for unauthorized data access.

3. Secure senior-level, cross-functional deal risk approval

The final step in finalizing a deal's required scope of separation is a presentation to senior-level business, operational, and control-function (e.g., Legal, IT Security, Audit) leaders to secure joint risk approval. The presentation should include overall considerations, proposed separation by area, mitigating controls, and any optionality that needs steering-level approval. Following group ratification, an official deal risk document should be stored for future reference. Also, a best practice before the final risk approval presentation is pre-syndication with major stakeholders from a cost, risk, deal, and other perspectives. It is not unusual for senior executives to ask for re-consideration in some areas, and it may take one to three plan iterations before final ratification is attained.

Do's and Don'ts for Logical Separation

As you work through separation decisions, the following Do's and Don'ts reflect our experience in working with our clients.

Do:

- Factor in Day 1 Close separation requirement timelines into decisions on when to set proposed Close Data
- View logical separation as a means to the eventual physical separation—minimize throwaway logical separation efforts, where possible
- Ensure Control Functions have a seat at the table early in the separation planning process
- Balance business needs and costs against legal guidelines—it's often possible to reduce costs by going with an alternate solution (e.g., application separation through mere access controls vs. logical separation at the application level)
- Ensure comprehensive understanding of costs (pre-close logical separation + end-state physical separation) in decision making process

Don't:

- Base your judgment purely on prior deals—each situation is unique. Regulations often change, and so does the business context. Treat each situation differently and engage stakeholders early
- Adopt a black/white approach; balance risk-based decisions with competing business/operational and Control Function objectives and requirements
- Focus exclusively on requirements from previous deals; risks, local country laws, and IT security best practices are ever changing
- Be compelled to logically separate each and every IT asset. Prioritize logical separation efforts—you will need your resources to work on other physical separation projects as well

Conclusion

Logical separation is becoming increasingly relevant in an M&A context and should be a front-burner issue for IT executives. When an asset sale or spin-off involves an IT services TSA, appropriate tools and restrictions should be put in place to both enable day-to-day operations and prohibit unauthorized access.

A few final considerations: Avoid entering into "analysis-paralysis" mode when selecting a separation approach because there are innumerable permutations and combinations. Ultimately, the decision on "how much is enough" is a risk-balanced opinion across external and internal stakeholders. Also, set the final steering committee risk approval dates at the beginning of the process and work backwards, with clear milestone deadlines along the way. Additionally, do not let the TSA readiness and associated logical separation effort get in the way of the ultimate risk-mitigation process, the final exit from TSA services. Speed to separation remains the most important principle of all.

Contacts

Asish Ramchandran
Principal
Deloitte Consulting LLP
aramchandran@deloitte.com

Sejal Gala
Principal
Deloitte Consulting LLP
segala@deloitte.com

Sahil Parmar
Senior Manager
Deloitte Consulting LLP
saparmar@deloitte.com

Ryan Gordon
Manager
Deloitte Consulting LLP
rygordon@deloitte.com