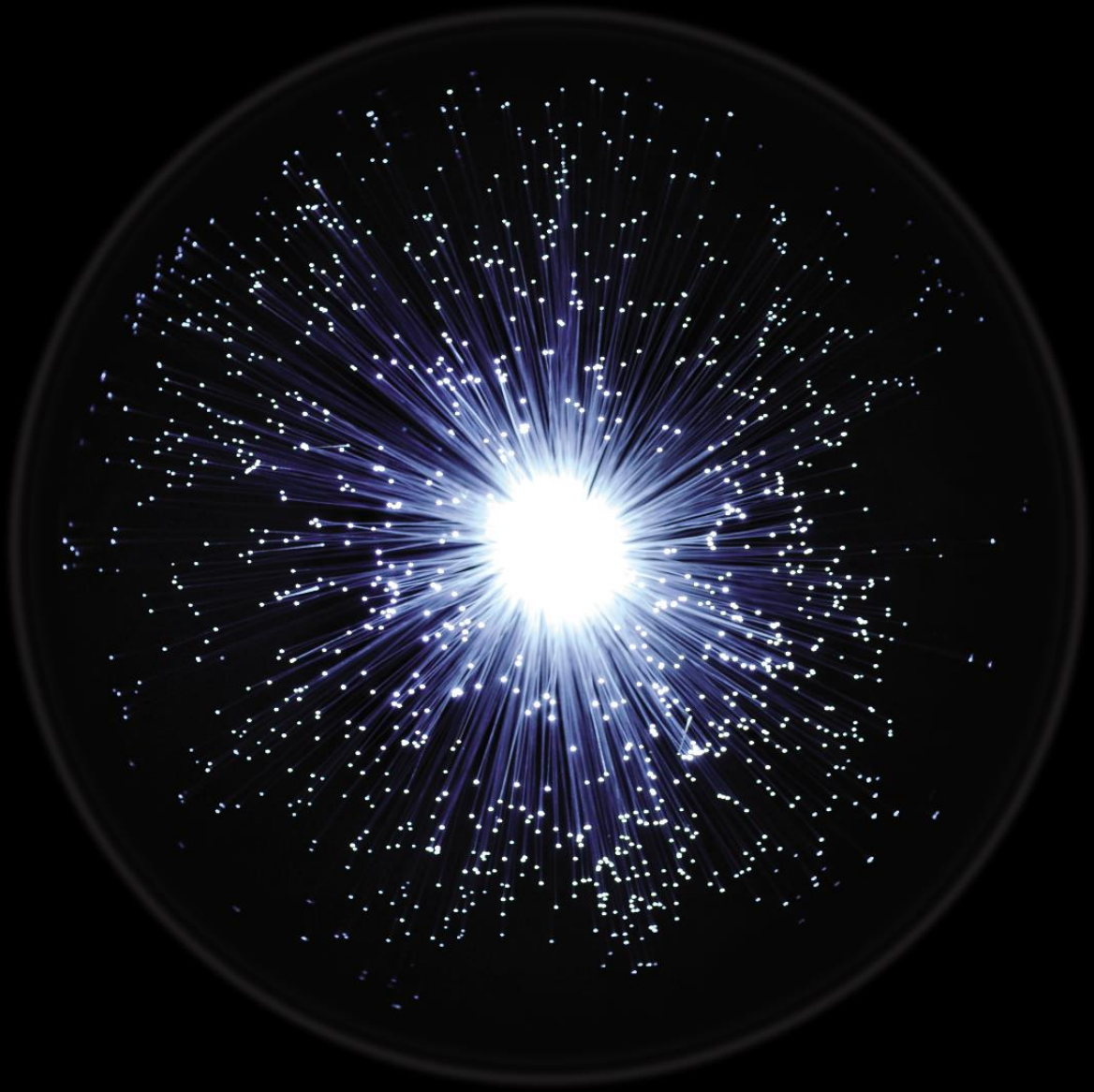
Deloitte.



M&A Making the deal work

Advisory

Table of contents

Deloitte.

Eight keys to a successful treasury integration

By Chi Yun Lee, Carina Ruiz Singh and Gaurav Sharma

Treasury's evolving role in M&A

Traditionally, the Treasury function's main responsibilities have revolved around protecting a company's liquid assets and helping Finance perform its core functions effectively. In recent years, however, these responsibilities have been evolving and expanding. C-suite executives expect today's Treasury organization to serve as a strategic advisor to Finance, the Chief Financial Officer (CFO), and the overall business. Now more than ever, Treasury executives and professionals should stay in front of rapidly shifting business requirements to support growth, company liquidity, financial risk management, and marketplace expectations for performance.

Included in Treasury's evolving role is providing strategic support for M&A transactions, especially post-deal integration. This support can be extensive and complex. For example, an acquiring company likely will be taking on debt to finance the deal, raising equity, changing its working capital requirements, and adding liquidity risk that the Treasury team will need to manage going forward.

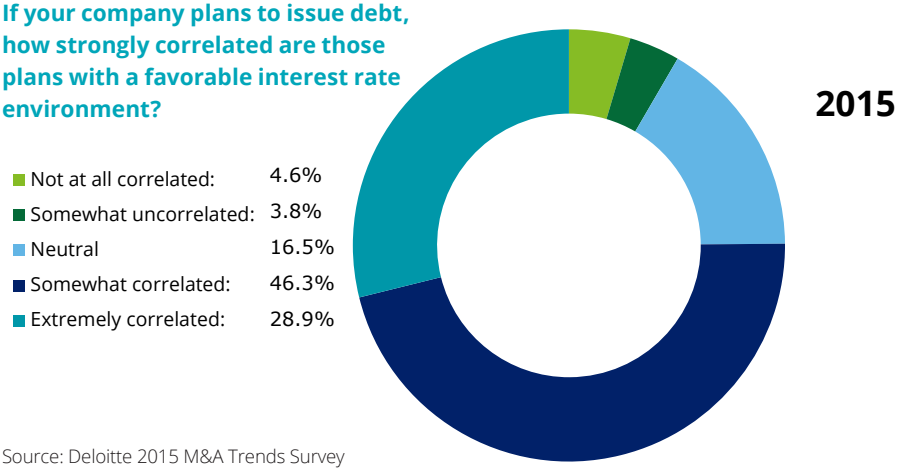
This is in addition to new regional and global footprints that will likely require adjustments to funding models, cash concertation pools, and an increased focus on cash visibility to support the newly combined businesses.

There are eight keys ways that Treasury can solidify its role as a strategic advisor and showcase its value during M&A integration:

1. Take the lead on overall deal financing and debt management
2. Collaborate with external groups, including banks, vendors, and outside consultants
3. Collaborate with internal groups such as Tax, Legal, IT, and the broader Finance organization
4. Prepare treasury systems for Day 1 readiness and beyond
5. Prepare for potential regulatory changes
6. Maintain and improve core treasury operations throughout the integration
7. Advise on integration management
8. Plan for post-Day 1 organization optimization

Figure 1: How today's deals are financed

If your company plans to issue debt, how strongly correlated are those plans with a favorable interest rate environment?



Source: Deloitte 2015 M&A Trends Survey

1. Take the lead on deal financing and debt

In the preliminary stages of an M&A transaction, Treasury is often asked to work with the CFO and other stakeholders to assess and identify a preferred financing structure for the deal. This activity places Treasury in a critical position to later enable an effective post-deal integration.

Low interest rates have made debt considerably cheaper in recent years, driving significant and sustained M&A activity. Figure 1 shows the importance of readily available, cheap debt for companies looking to acquire other firms. Expected interest rate increases have further encouraged M&A, with companies raising $290 billion in debt to finance acquisitions in 2015 (roughly triple 2014's level).[1]

In the current leveraged deal environment, the Treasury function can map out funding mechanisms for a potential acquisition, examining available cash, equity, and debt instruments to create an optimal capital structure. Furthermore, Treasury's involvement in due diligence related to acquiring company debt and risk exposures is critical to meeting the organization's post-acquisition debt obligations and risk profile.

Deal financing

When mapping out deal financing, Treasury cannot work in a bubble. Effective collaboration is essential to perform financing activities in the most tax-efficient manner. For example, Treasury's capital markets group should work in tandem with Finance, Tax, Legal, and others to outline the timeline of integration activities. This collaboration can provide strategic support to the CFO and help identify the investment capacity needed to fulfill the new company's business and financial strategies.

It is important that Treasury establish early communication with external parties (e.g., banks, institutional investors, credit rating agencies, investment bankers) that are key players in financing processes such as cash forecasting for the combined entity, identifying synergies, and setting post-merger margin expectations. Doing so may avoid potential issues or late adjustments that can arise from misalignment between the company and these outside groups. Additionally, if the acquiring and target companies have different or overlapping financing partners, integration could provide an opportunity to reduce that total.

Typical Day 1 milestones for debt, funds flow, and solvency may include:

- Debt covenant reporting procedures
- Third-party debt/derivatives updates in treasury system
- Journal entries for all Day 1 activities
- Step plan including funds flow and journal entries
- Intercompany loans in treasury system
- Aligned practices for in-house banking, including changes to financing company structures

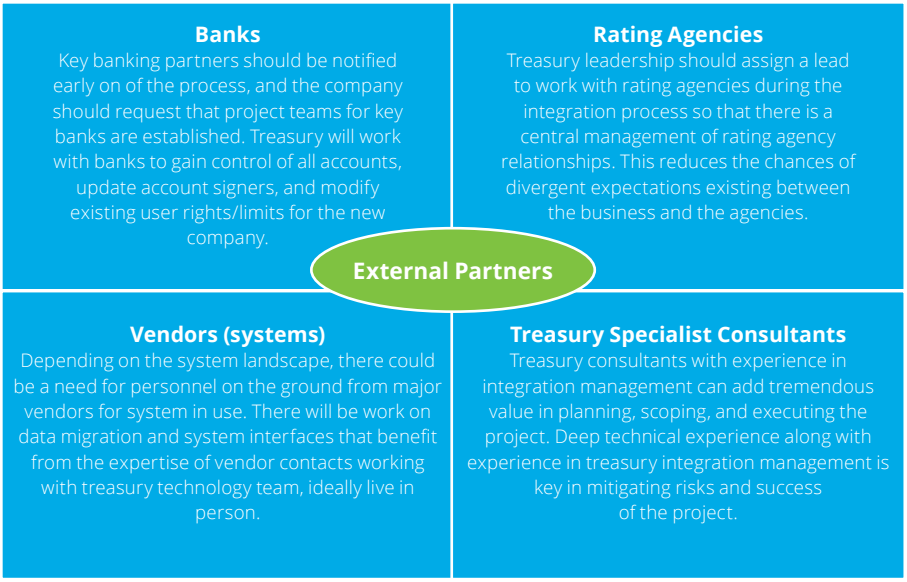
Debt management

Many of today's acquisitions are heavily leveraged, which may complicate raising funds, managing debt, and maintaining credit ratings. Companies should determine quickly and accurately what their fund flows will look like after integration to facilitate debt discussions. After identifying and helping to secure the financing mix, the Treasury team's focus should shift quickly to debt and covenant management. Early planning (e.g., creating templates to finalize covenant calculations and identifying team leads) allows executives to control conversations about the company's long-term position. In particular, Treasury organizations should stay in front of discussions about credit rating changes and market perceptions throughout an integration to mitigate third party views that that increase in debt negatively impacts the company.

2. Collaborate with external groups

Third-party service providers can be major contributors to the success of Treasury integration. Engaging third party service providers early provides more time to discuss potential execution paths and enables the Treasury team to leverage the collective knowledge bases of these external groups. Viewing external service providers as part of the company's integration execution team can create a more fluid integration environment and potentially strengthen their commitment to a company's successful integration. Key external providers typically include banks, rating agencies, vendors and Treasury specialist consultants (Figure 2):

Figure 2: External partners' roles in Treasury integrations



3. Collaborate with internal groups

Collaborating with internal stakeholders across Finance, Tax, and Legal can streamline critical integration processes. Integrations tend to go off the rails when teams are siloed – they focus only on milestones and activities that directly impact their work and don't pay adequate attention to interdependent areas and downstream impacts. By communicating early and often, teams can identify potential dependencies and gain buy-in from impacted groups before decisions are made.

Finalizing the new legal entity (LE) structure is a significant area for organization-wide coordination. Treasury should work with both companies' Tax and Legal functions to assess how the LE structure of the acquired company will affect existing processes and policies. For instance, the target company's global footprint, current tax structure, and Treasury operational structure may not fully align with the acquirer's current model. The new LE structure also may generate additional regulatory requirements including cash pool locations, thin-cap rules, and repatriation limitations. From a Treasury perspective, the LE structure may have the greatest impact on the existing financing companies and in-house banks that either company has. Cash pools will have to be reassessed to legally comply within the new structure, and new bank accounts may be needed to support any future LEs that arise. Furthermore, any changes to the structure (e.g., incorporating other entities) should be closely coordinated with overall treasury systems and data migrations. Examples of internal collaborations that may aid Treasury during M&A integration are:

Internal Group	Sample Activities
Legal	**Bank account openings/country requirements, legal entity structure, resolution documents, pooling structures**
Tax	**Coordination/execution of local funding needs, cash movements, intercompany financing model**
Finance/Accounting	**AR/AP payment and receipt requirements, working capital alignment, reporting/recording**
IT	**Go Live coordination, data migration, system issue identification and resolution**

4. Prepare treasury systems for Day 1 readiness and beyond

Gaining value from Treasury department technologies requires a comprehensive implementation plan that is aligned with broader strategic initiatives that drive organization value. Treasury Management System (TMS) integration requires carefully assessing considerations that involve dependencies and groups inside and outside Treasury:

- **Strong understanding of overall system architecture:** Overlapping system functions may require system architecture and business decisions aimed at rationalizing data and process capabilities.
- **Data warehousing:** The combined companies likely will need a central data repository to support key treasury system requirements (e.g., cash forecasting). The repository should include data from Enterprise Resource Planning (ERP) systems, TMSs, and other sources from both companies to aid forecast modeling and reporting.
- **Overall ERP integration:** Treasury should define interdependencies and any data sourcing issues that may arise from multiple ERP instances.
- **Standardized integration:** The planned systems integration framework should be as standardized as possible to streamline cutover and data consolidation (e.g., integration tools).
- **Exposure reporting strategy:** Treasury should determine the consolidated company reporting requirements needed to support exposure and hedge management.

Treasury should foster strong relationships with internal IT resources, vendor representatives, and implementation/integration specialists to determine whether existing systems can be configured to support operations or if a full-scale TMS implementation is necessary to reach the target end state.

5. Prepare for potential regulatory changes

The ever-changing regulatory landscape has the potential to disrupt a smooth M&A integration, requiring integration teams to spend significant time positioning the new company to comply with current and pending regulations across the globe. Examples of recent changes include increases in central bank reporting, Report of Foreign Bank and Financial Accounts (FBAR), and base erosion profit sharing (BEPS).

Increasing the amount of central bank reporting around capital control and anti-money laundering (AML) regulations may require the Treasury team to maintain clear visibility into cash flows at a country level across entities old and new. The Treasurer's office also should prepare for the increased effort and time needed to gather, aggregate, analyze, and maintain data for Securities and Exchange Commission (SEC) reporting. Neglecting these responsibilities may severely impact the combined company's performance and regulatory standing.

BEPS – an initiative involving almost 90 nations – lays the foundation for a modern international tax framework aimed at taxing profits at the point of economic activity and value- creation. BEPS is expected to drastically affect the ways that liquidity models are structured, while significantly altering repatriation laws and requirements on local banking. At its core, the BEPS project intends to:

- Eliminate tax mismatches so that all income is taxed
- Align profits with value creation
- Increase consistent levels of transparency with tax authorities
- Implement tax law change in a coordinated fashion

There are several BEPS impacts at a company level, including areas that pertain specifically to Treasury:

- Entity financing–debt pushdown, instrument types, interest rates, funding structures
- Local banking requirements
- Working capital management–pooling, factoring, intercompany lending
- Repatriation–timing and manner of moving funds

6. Maintain and improve core Treasury operations

Sooner rather than later, Treasury leaders should determine what core operations can be combined by Day 1. The project plan should include integration execution and tracking for each of the key functions (bank accounts, cash management, risk management, regulatory, etc.).

Control of bank accounts and cash

On Day 1, the buyer's Treasury department should take control of the acquired company's bank accounts, banking portal access, signatories, and subsequent cash. This requires board resolutions, bank acceptances, and updated signature cards. Cash access should be enabled through technology, bank portal access, or account set-up in TMS, to make sure that appropriate control is provided to the acquiring company. Note that the number of the acquired company's banking partners and geographic locations can have a significant impact on the level of effort required to complete this process.

Visibility over cash–positioning and forecasting

Treasury should establish a cash management structure that provides a combined view of the new company's liquidity and cash needs. The time horizon for required visibility varies based on company liquidity and funding strategies. This is important for daily visibility (through bank portals or MT940s) and longer-term cash forecasting. Interim manual solutions may be required to provide full visibility if the legacy companies' technology platforms are still being integrated to enable an automated long-term solution.

To strengthen security around daily cash needs during integration, both acquirer and target companies should establish effective cash positioning processes. All cash movements should be monitored daily; this will aid overall understanding of Foreign Exchange (FX) exposures during the integration period, help identify additional capital needs, and provide insight into future covenant management requirements.

Detailed mid- to long-term cash forecasting is important during integration to give visibility into the combined organization's cash movement and needs. This will help Treasury understand each company's cash management strengths and weaknesses so it can effectively support the combined business. Depending on integration requirements, Treasury may attempt to create a combined cash forecast prior to Day 1. However, expenses may be volatile during integration due to overall project costs, which may lead to more significant deviations than usual. Treasury should regularly follow up with input groups to review these variances. Driving a dialog with other business functions to explain large variations will help further Treasury's knowledge and provide an additional communication channel during and after integration.

Risk management

Early in the M&A process, the Treasury M&A team should develop a clear understanding of what the combined company's treasury risk profile may look like after integration to aid risk mitigation planning. Combined companies can have a very different risk profile than either would as a standalone entity.

It is important to review which daily risk management tools are being used to confirm proper coverage during and after the transition. Examples of liquidity risk are:

- Credit facilities, overdraft lines, and other sources of credit such as commercial paper programs should be reassessed to provide additional short-term liquidity as needed
- Bank guarantees for the new company may have additional requirements, such as the need to have leases for local properties in certain jurisdictions
- FX lines may have to be adjusted or activated due to potentially irregular payment volumes and currencies during integration

Reassessing the new company's foreign currency and interest rate aggregate exposure is critical in managing the company's overall financial risks. Once exposure has been identified the Treasury team can determine which changes may be needed to risk management strategies or hedging executions to satisfy the new company's risk appetite. Changes related to FX risk may include:

- Adjusted hedging limits
- Updated authorized traders or trading limits
- New or revised ISDAs

M&A integration is an optimal time to refresh policies and procedures to align with an evolving risk profile, market standards, and regulatory requirements. Creating a standard and repeatable process for identifying, aggregating, and managing company risk should be a Day 1 focus.

Industry-specific risks

Specific industry requirements may impact how Treasury prioritizes tasks during the integration process:

- Oil and gas– Ensuring the accuracy of short-term forecasts is essential, as drastic swings in oil prices can affect a company's cash levels and needs
- Technology – Companies may encounter intellectual property (IP) location challenges, causing trapped cash issues that require tighter cash management
- Health care – High R&D costs may constrain working capital, creating covenant management challenges
- Financial services– Regulatory capital and liquidity requirements can change drastically based on the integrated institution's size increase
- Private Equity (PE) – Increasing debt-to-earnings ratios obtained in PE-backed buyouts exerts pressure on improving the company's operating matrix to repay debt. Treasury should keep a close eye on liquidity ratios to manage debt covenants. In addition, managing working capital is of paramount importance, as financial sponsors look to achieve returns as early as possible

7. Advise on integration management

Establishing goals

Treasury executives should clearly outline Day 1 and end-state integration goals. For Day 1, function leaders should use internal and external resources to make sure that integration activities do not disrupt regular business operations Specific attention should be paid to the combined company's liquidity needs so that obligations can be met. Treasury leaders also should develop a strategy and implementation plan to capture potential post-Day 1 synergies; for example, identifying and rationalizing duplicative roles and processes.

Planning and blueprinting

During integration visioning sessions, tension may be high as both acquirer and target teams see their Treasury processes as correct. Creating a clear and actionable framework for session participants to follow and engaging in active listening and collaboration should produce a blueprint that focuses on what is best for the combined company in both the short and long term. In addition, Treasury leadership should empower the Treasury integration management team, which typically is led by the treasurer or the assistant treasurer, to keep the integration on time and within scope.

Operating model

Oftentimes, companies go through an integration with the mindset "we can always change 'X' (process, people, technology) later." However, potential operating model improvements often fall by the wayside if they are not planned in advance. To increase integration effectiveness, team members should prepare both an interim operating model to support Day 1 readiness and a desired end-state model for post-Day 1 optimization. Every effort should be made to reach the desired end state during integration but it shouldn't come at the expense of a successful Day 1.

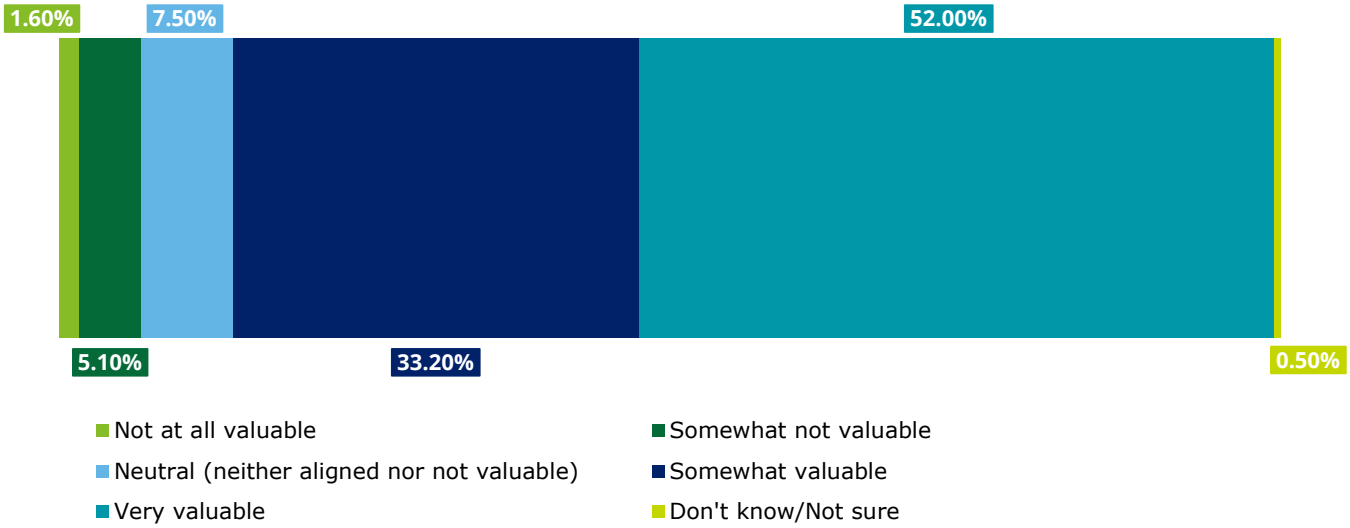
Treasury department size and sophistication should factor into the integration process. An early-stage company may have only a basic cash management function to incorporate, while a well-established company is likely to have detailed pooling structures, cash management strategies, debt, FX management, treasury technology, or even a fully functioning in-house bank. Company size also affects the number of full time employees (FTEs) that will be needed to support the combined business. While FTE requirements can vary depending on the complexity and scope of Treasury operations, a company typically needs two FTEs per $1 billion before reaching $10 billion in revenue; and one FTE per $1 billion after reaching $10 billion in revenue. Integration provides an opportunity to streamline Treasury operations and drive greater efficiencies.[2] The project plan should identify which Treasury activities (and positions) are the most critical to achieving Day 1 readiness and the end-state operating model.

IMO/governance
Senior executives should give acquirer and target companies' Treasury leaders clearly defined integration roles and responsibilities, leveraging their treasury expertise and company-specific knowledge. A Treasury integration management office (IMO) should provide project oversight, manage integration work streams, and log, track, and resolve key risk items that may arise (Figure 4). The IMO should serve as the central point of contact for non-Treasury groups during the integration process to help expedite the flow of information among various departments and functions. Through regular meetings and partnerships with Treasury process owners, the IMO should establish a clearly defined governance model that outlines how the project will be handled from a milestone and risk perspective.

Finally, the Treasury integration team will need to develop budgets to track overall Treasury integration costs against projected amounts. There likely will be expenditures for outside consultants and vendors involved with systems migration and cutover activities. These expenses should be monitored and reviewed on a periodic basis to verify that there is enough value-add to justify costs and that overall project risk management is sufficient.

Figure 4: IMO value

How valuable was the IMO or PMO to the overall success of the integration?



Source: 2015 Deloitte M&A Trends Survey

8. Post-Day 1 optimization

Assessing the organization
After Day 1, it is important to maintain focus on future-state Treasury goals and to develop key performance indicators (KPI's) for the business. Among typical metrics:

- Forecasting variance analysis
- Percentage of ACH payments
- Bank fee analysis
- Debt to capital ratio
- Free cash flow
- Debt maturity schedule

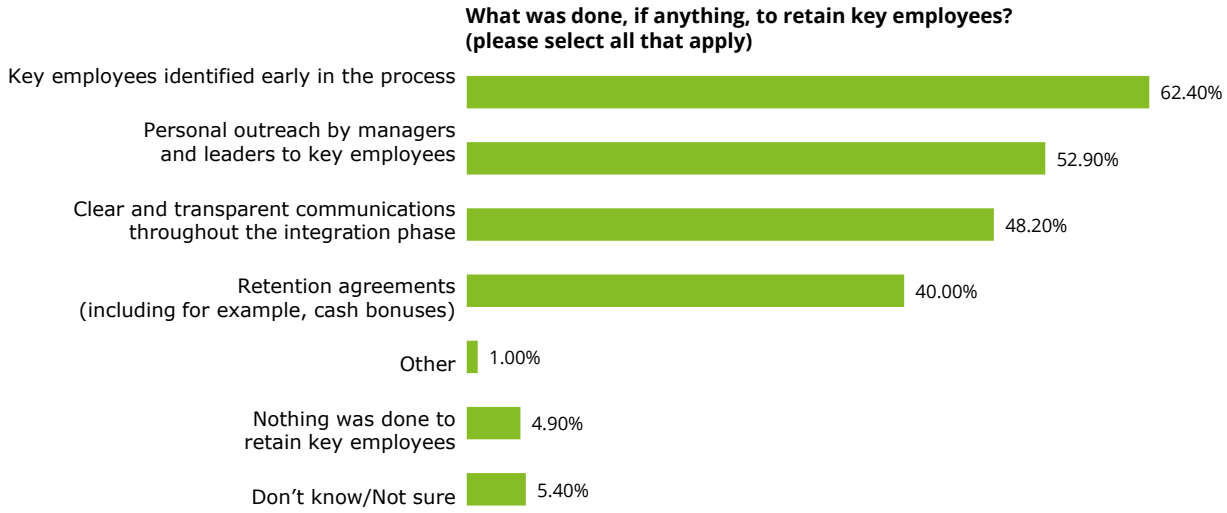
These and other metrics can help the Treasury team evaluate how its performance compares to industry leading practices and the desired future state. For example, lenders provide deal financing with the expectation that M&A will increase the acquiring company's synergies and add value. This debt exposes Treasury on covenant management and debt repayment if the company is unable to follow through with a successful integration. This increases the need for Treasury to proactively manage deal risk. Managing debt well by setting up covenant schedules, identifying key providers, and diligently monitoring the integration process can provide an opportunity to showcase Treasury's strategic value to the business.

Plan for post-Day 1 organization optimization

It is important to remember that integration occurs at a fast pace that not all team members may be accustomed to. Treasury leadership should watch for team fatigue and work to maintain employee engagement and productivity. This can be aided by showing employees that they are valued, with frequent interactions and touchpoints to solicit feedback. Transparency, clear communication (e.g., weekly team meetings and monthly newsletters), and regular management outreach tends to boost morale and productivity. In addition, including valued team members in discussions about Treasury's future state is an effective way to gain buy-in and enhance employee loyalty.

Integrating two companies may lead to dis-synergies such as duplicative processes or over representation in certain regional areas, which can create the need to right-size the organization to fit the planned future state. These dis-synergies should be quickly identified and eliminated to gain immediate value from the integration process. Treasury can look at different operating models – such as taking on new strategic activities – that can support employee retention (Figure 5).

Figure 5: Organization optimization



Source: 2015 Deloitte M&A Trends Survey

Post-deal synergies

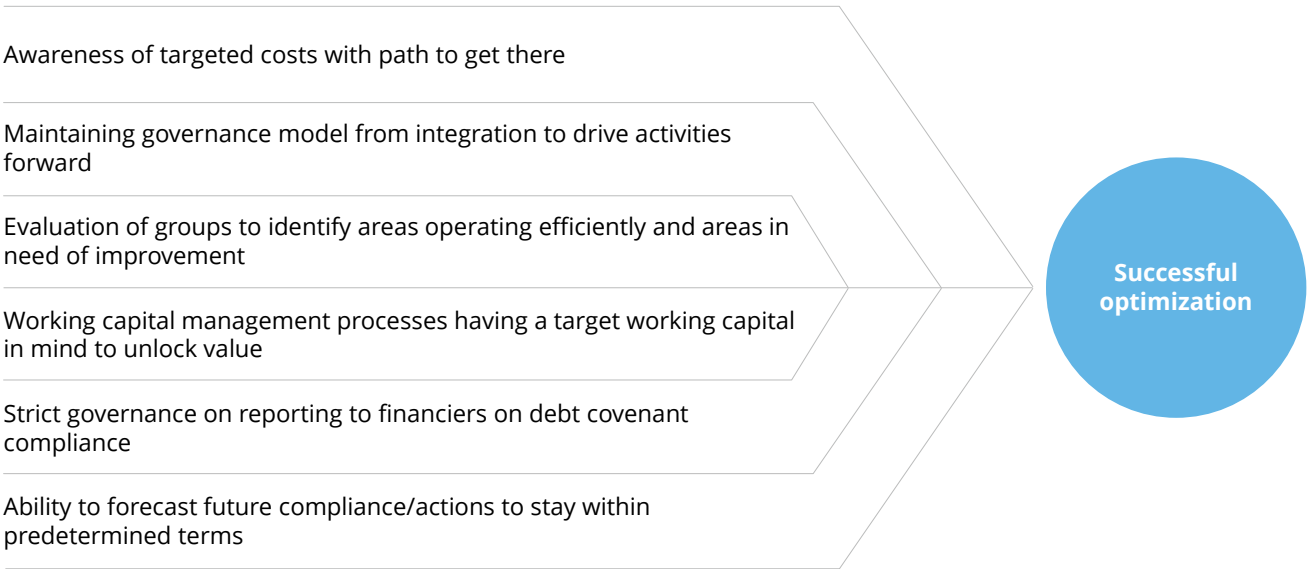
For Day 2 and beyond, the Treasury team should focus on stabilizing and optimizing the new company's infrastructure by completing tasks such as bank account rationalization and bank fee analysis, and managing debt. Post integration there is likely to be an overabundance of bank accounts – a well-executed analysis can lead to cost savings.

Treasury should set target working capital requirements for the combined company, both to achieve forecasted figures and to unlock excess working capital. In highly leveraged transactions, it's even more important, as the cost of capital for this unlocked working capital is much higher. Efforts should be made to look for opportunities to increase the accounts payable (AP) cycle wherever possible. Partnering with different finance leads and overall project management teams will help them stay abreast of company-wide cost-cutting plans and synergy savings. Also, maintaining awareness of the company's financial status will help produce accurate forecasts to prepare for covenant management. Areas where Treasury should be involved include:

- AR/AP management
- FP&A plans
- Changes to payroll and real estate operations
- Post-integration project management statuses on synergies

To reach desired levels of post-deal synergies and cost effectiveness, companies should focus on:

Figure 6: Post-deal synergies



Moving forward

Both during and after M&A integration, Treasury leaders should position their organization as a strategic partner to the CFO – a partner that can aid operational effectiveness and help drive inorganic growth. Showcasing Treasury's ability to manage debt, unlock cash, and drive cross-functional alignment during an integration can lay the groundwork to expand the function's footprint and support continued value creation.

End Notes

1. Jackson, Gavin, and Joe Rennison. "Bond Issuance to Finance M&A Deals Swells to Record High" Financial Times, 4 Aug. 2015
2. 2015 Deloitte Treasury Survey

Deloitte.

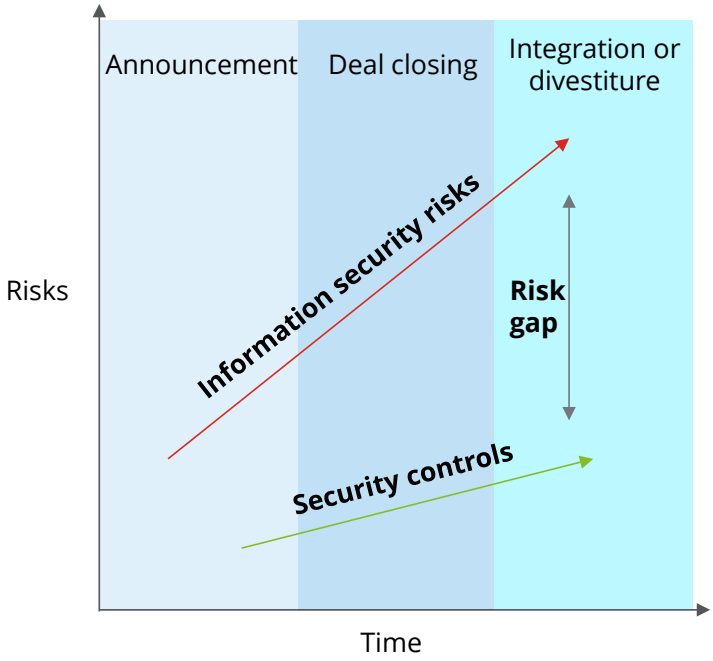
Don’t drop the ball

Identify and reduce cyber risks during M&A

By David Mapgoankar and Arun Perinkolam

As if M&A deal teams didn’t have enough balls to juggle during a transaction’s lifecycle, today’s complex and porous digital marketplace is tossing in one more – increased cyber risk. Every stage of M&A – strategy, screening, due diligence, transaction execution, and integration – is subject to heightened risk for cyber threats and attacks which, if not discovered and defused, could harm both the acquirer and target…and even scuttle the deal.

Figure 1: Cyber risks in the M&A lifecycle



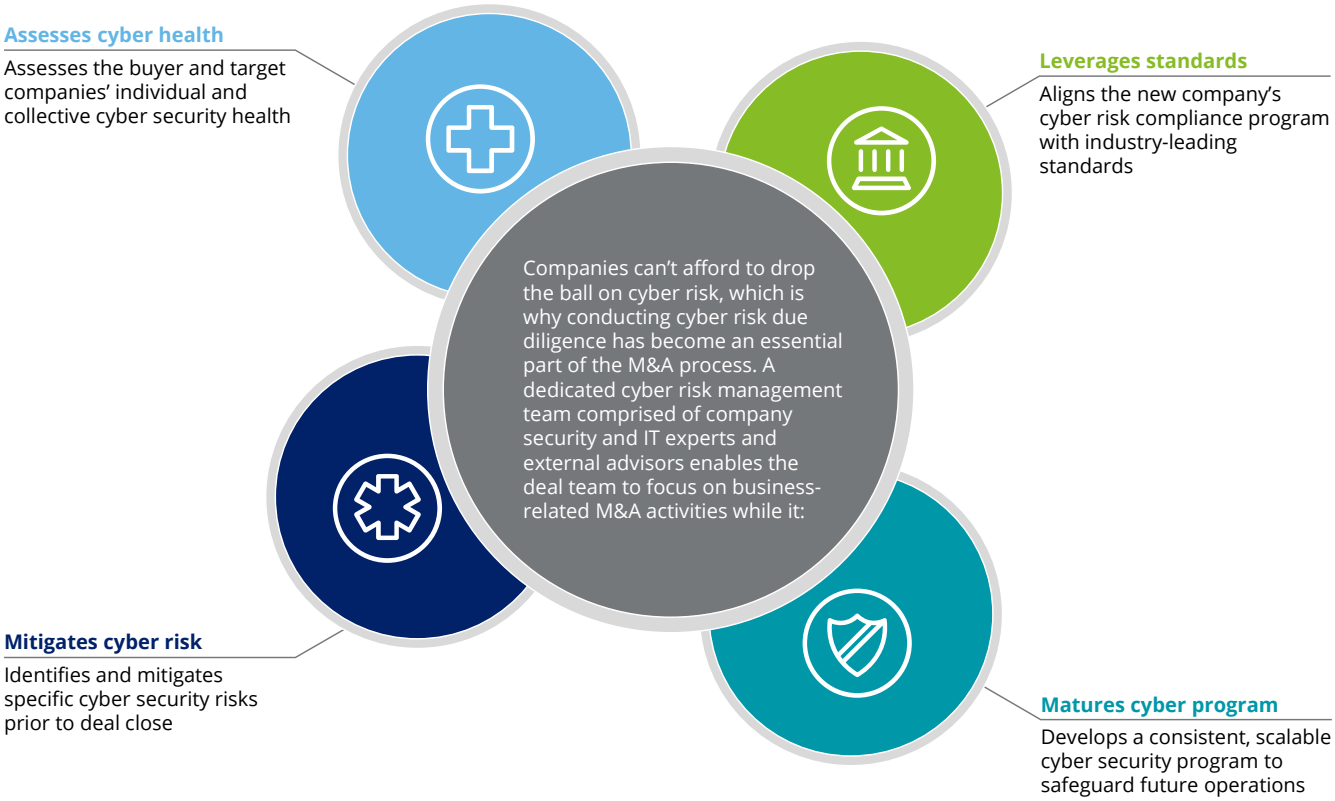
Source: Deloitte & Touche LLP, 2016

Cyber risks vary from one M&A lifecycle stage to the next, and may be generated both internally and externally. Common risks include:

- Targeting from a cyber threat actor leading to damaged reputation with Wall Street and potential stock devaluation;
- Failure to understand and mitigate deep cyber shortcomings (including legal and regulatory risks) in the target company;
- Reaching a deal price that does not accurately reflect the cyber health and robustness of the seller’s networks and systems that will form the basis for a new division of the acquiring company;
- Unknowingly exposing the acquirer’s enterprise network to threat of cyber attack when integrating potentially antiquated and unpatched systems and IT assets of the target company

Engaging the cyber risk management team prior to initiating the M&A process can provide strategic value at each stage in the deal lifecycle.

Figure 2: Cyber risk due diligence



M&A strategy

Prior to launching an M&A transaction, the cyber risk management team should develop a corporate risk assessment strategy and playbook to guide cyber risk-related due diligence consistently for each potential M&A target, with defined requirements and expectations for cyber risk controls. This playbook can help reduce the level of ad hoc and deal-specific project planning and increase the speed and reliability of the company's overall cyber due diligence process. Once this pre-planning is complete, acquisition targets can be sought out and compared to the existing strategy.

Playbooks are typically comprised of two major components: the cyber risk due diligence approach and the associated tools and templates. The due diligence approach identifies organization-specific drivers to align the cyber risk due diligence with broader corporate strategy. To enable the most effective results, the approach should lay out high-level timelines and milestones and identify a core team of subject matter experts for each deal. The timelines and milestones should be flexible enough to recognize variable deal complexity (e.g., a complete merger of overlapping business functions between two highly-regulated companies is likely be more complex and multidimensional than a straightforward purchase of IP assets in a non-regulated industry).

The tools and templates section of the playbook should identify and include documentation and reference materials for executing the approach, including a cyber assessment framework, checklists to enable and track information requests, sample questions, and project management templates.

Screening and due diligence

Once a potential acquisition target has been identified, the next phases typically involve target screening and in-depth due diligence. Target screening identifies potential acquisition candidates, or potential acquirers for a company wishing to sell itself entirely or in part. Due diligence provides the opportunity for the acquirer to conduct discovery on the acquisition target, including analyzing or financial stability and health, review of cyber risk and infrastructure, or interaction with acquisition target leadership to gauge interest in an M&A transaction.

A number of tools and methodologies are available to support target screening. Activities often include conducting high-level research to create a target company's threat profile, identifying instances of historical cyber risks (e.g., published examples of breaches), and providing industry-level insights. The resulting report should be helpful in driving and/or scoping follow-on due diligence efforts.

Once a target has been selected and passed through the initial screening, due diligence is fully initiated, and the cyber risk management team should coordinate the due diligence activities related to cyber risk. At a foundational level, cyber risk assessment activities typically employ a custom-designed framework that leverages industry leading practices, globally recognized standards, and unique requirements that reflect the acquiring company's deal drivers. The framework should facilitate a holistic review of a target's cyber risk, including an in-depth analysis of its IT governance, operations, information security, business continuity, physical security, and overall risk posture.

The assessment generally consists of three core methods that may be used in parallel: offline document and system review (typically handled via a virtual data room), onsite workshops, and cyber risk profiling. One or more of these methods may not be appropriate or necessary in all contexts, however, as every deal has its own nuances and complexities. The offline document and system review includes analyzing documentation, resources, and artifacts (e.g., system architecture documents, information assets) to develop an understanding of the acquisition target's environment and identify preliminary findings and remediation opportunities. In addition to the document review, the cyber risk management team may determine it appropriate to conduct vulnerability assessments and penetration testing on the target's IT systems. While this testing typically focuses on perimeter weaknesses, the scope and scale can be readily adjusted to fit the situation.

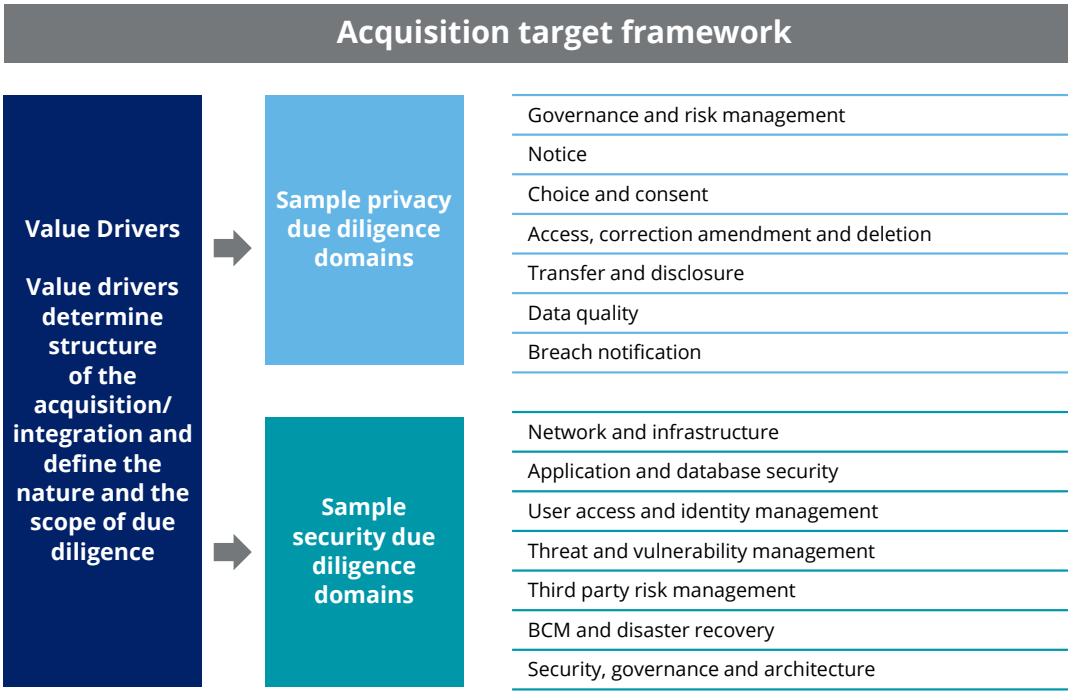
The second core method is the onsite workshops, which typically take place at the acquisition target's corporate facilities, including data centers, where appropriate. The cyber risk management team meets directly with leadership, management, and subject matter experts to identify and discuss risks, findings, and remediation opportunities. In some cases, the acquiring company will send additional representatives. When this occurs, the risk management team will typically operate as a central project management office (PMO) to coordinate schedules, align content to reduce overlap, and lead workshop activities.

The final assessment method – cyber risk profiling – includes two avenues: cyber reconnaissance and compromise diagnostics. With the acquisition of the target company's assets, the acquiring company also receives certain aspects of the target's threat profile. Cyber reconnaissance and threat profiling can assist in identifying techniques, tactics, and procedures that threat actors employ against companies experiencing large-scale, organizational change. Cyber reconnaissance provides a company undergoing a transformation a point-in-time assessment of its exposure to cyber threats by assessing the company's assets across relevant intelligence sources. Reconnaissance typically includes conducting threat assessments that leverage ethical hacking and penetration testing techniques, and that use open, closed, and proprietary sources and underground criminal forums. The resulting cyber threat profile provides insight into the criticalities that threat actors may target and how.

Based on knowledge gleaned from the reconnaissance and threat profile, the acquiring company may wish to perform a gap analysis and cyber diagnostic to determine if the target is already compromised. Advanced attackers specifically evade the cyber risk tools and technologies companies traditionally leverage. With this in mind, a diagnostic can review the target's environment to identify active or dormant threats present on its computer systems and networks. The review assesses endpoints and network traffic transiting between the target organization's networks and the Internet. It deploys agent-based endpoint technology to all desktops, laptops and servers to search and review for potential Indicators of Compromise to identify anomalies, malware, vulnerabilities, or other conditions that would pose a threat to the organization.

Once the risk management team has completed assessment activities, it may compile a cyber risk mitigation plan that includes a detailed review of each risk with prioritized tactical steps for remediation. The plan also identifies suggested owners for remediation activities, forecasts costs, and may even recommend a preliminary end-state IT infrastructure to support cyber risk-related integration activities.

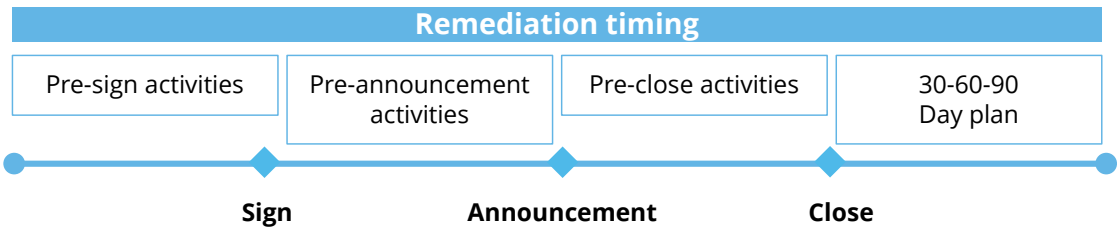
Figure 3: Acquisition target framework



In some cases, this remediation plan may require mitigation activities prior to Day 1, but usually after the deal is signed. These mitigation activities are tailored to address the highest severity risks, especially those that may lead to issues. When identifying these activities, the risk management team should account for additional activity and interest from threat actors that can occur once the acquisition is publicly announced.

Finally, the remediation plan may also be used as leverage in the deal-making process itself. The costs associated with remediation of significant cyber risks may be used as a lever to reduce the overall acquisition costs. For example, if the acquisition target requires the development and implementation of a network demilitarized zone (DMZ) to be stable on Day 1, some or all of the costs of that project may be subtracted from the overall valuation of that company. This process requires careful coordination between company leadership and cyber risk management subject matter experts in order to convey the appropriate messaging to the acquisition target, syndicates and attorneys involved.

Figure 4: Remediation timing



Transaction execution

The cyber risk management team's involvement in an M&A transaction does not end after target screening and due diligence. The acquirer's prime objective in this phase is to facilitate an uneventful, issue-free Day 1. During this phase, the deal team may ask for assistance with cyber risk remediation activities and advise on integration plans for network architecture, and support technology (e.g., e-mail servers, human resources systems). Tasks may include reviewing the asset inventory developed during the due diligence phase to outline recommendations for logical and physical access provisioning, and identifying, developing, and implementing controls and processes to support Day 1 activities. Other relevant activities include reviewing critical system redundancies, planning for back-up and storage requirements, creating incident response procedures, and ramping-up cyber threat monitoring and vulnerability management capabilities.

Integration

An issue-free integration starts long before an M&A deal closes. Both companies participate in the integration process, where the two entities are merged according to the terms of the deal and the overall M&A strategy of the acquirer. The cyber risk assessment results may prompt the newly combined company's IT and cyber security staff to address a number of findings, improvement opportunities, and integration activities. To drive this effort, remediation and integration activities are typically summarized in a prioritized "30-60-90 plan," with target milestones laid out at 30-days post-close, 60-days post-close, 90-days post-close, and beyond.

Within the first 30-days post-close, the IT and security teams should address critical or high risk remediation activities, especially in cases where onsite remediation cannot occur prior to Day 1. Activities usually include developing strong perimeter security, addressing substantial gaps in business continuity, and closing critical or high-risk vulnerabilities. Additionally, the end-state cyber risk infrastructure should be developed and revised, with foundational technologies and devices implemented as needed.

Once the 30-day milestones have been addressed, the 60-day and 90-day activities should include re-testing and re-assessing solutions implemented as part of the earlier plan, and performing additional remediation for medium- and low-risk findings and vulnerabilities. Issues vary greatly from company to company and typically are prioritized based on factors unique to that environment. Finally, the cyber risk management team should play a key role in safeguarding the new company's IT systems, applications, and online presence. Common responsibilities include:

Identity and access management

M&A typically spawns reorganization and restructuring, which require heightened identity and access supervision. Ongoing identity and access management (IAM) services facilitate administration throughout the user lifecycle, from on-boarding to off-boarding enterprise users (e.g., employees, contractors, vendors, customers). Along with identify management comes the need to administer and monitor access privileges and roles. Access management is critical to organizations that may be shifting large amounts of enterprise resources. Services include access control and configuration support, and maintaining user profiles, entitlements, and application access rules. Familiarity with the leading IAM technology vendors, such as Oracle, IBM, CA, SailPoint, EMC/RSA, CyberArk, Lieberman, is also key to effectively implementing an IAM solution.

Enterprise application integrity

A company merger can present a challenge to managing and protecting critical assets due, in part, to evolving threats that accompany the integration of business environments. A portion of this challenge is related to enterprise resource planning (ERP). When expanding and extending beyond traditional corporate IT borders, it is critical to address ERP system security, privacy, control, and compliance requirements. Enterprise application integrity (EAI) services help promote data security across the application ecosystem and within related business processes.

Managed Threat and SIEM

Organizations must remain ever-vigilant to cyber security threats. This means having overarching visibility and pre-emptive threat insights to detect known and unknown adversarial activity. To be able to accomplish this, the cyber risk team should work with internal and external resources to develop managed threat services (MTS) solutions that enhance in-house capabilities and increase the value of Security Information & Event Management (SIEM).

Threat intelligence analytics

A company's ability to manage cyber threats and have a trusted SIEM operation depends heavily upon its ability to operationalize an organization's cyber threat intelligence program. During and after M&A activity, mitigating business risk should be a priority that requires timely, insightful, and predictive analysis tailored to the company's changing environment. Effective, actionable threat intelligence analytics provides the context and prioritization necessary to support recommendations for risk mitigation.

Don't drop the (cyber) ball

Conducting cyber risk due diligence has become an essential part of the M&A process. A dedicated cyber risk management team can provide strategic value at each stage in the deal lifecycle by assessing, identifying, and reducing potential cyber security risks prior to and after deal close.

Authors

Chi Yun Lee
Senior Manager
Deloitte & Touche LLP
chiylee@deloitte.com

David Mapgoankar
Principal
Deloitte & Touche LLP
dmapgoankar@deloitte.com

Arun Perinkolam
Principal
Deloitte & Touche LLP
aperinkolam@deloitte.com

Gaurav Sharma
Senior Manager
Deloitte & Touche LLP
gauravsharma36@deloitte.com

Carina Ruiz Singh
Partner
Deloitte & Touche LLP
caruiz@deloitte.com

M&A
Institute

About the Deloitte M&A Institute
The Deloitte M&A Institute is a community of clients and practitioners focused on increasing the value derived from M&A activities, powered by Deloitte's M&A Services capabilities. The Institute serves as a platform to build connections, showcase thought leadership, and accelerate experience and learning for those involved.

Deloitte.