

# Overcoming IT Challenges in Mergers and Acquisitions

## Introduction

Mergers and acquisitions (M&As) are the primary drivers of inorganic growth for consumer goods (CG) companies and are the widely preferred growth engine used by CG companies fortunate enough to have cash to spend. CG companies view M&As as a way to ensure that they have the right product at the right store on the right shelf at the right time.

The chief benefits of acquiring or merging with another CG company are to create or expand new lines of service or enter new geographical markets and enhance the product portfolio. In economic times where organic growth is hard to come by, these are powerful considerations. Acquiring a smaller player can offer a large CG company greater flexibility and quicker time to market -- a

key advantage now as the economic climate means every minute and every dollar count more than ever. Smaller companies often achieve higher returns on their brand management activities -- such an acquisition can quickly accrue to the larger organization's bottom line.

For most companies, deciding a merger or an acquisition is the easy part. The real challenges come after the acquisition as the new entity struggles to accommodate needed changes in

people, processes, technology systems, and compliance. This white paper focuses on the information technology challenges faced in an organization after M&A.

M&A poses massive challenges for any IT infrastructure, especially in cases where organizations of similar size merge. There, it would not be uncommon that the merged organization would have two entirely disparate systems, different images, different hardware, protocols, and Websites. In order to get the expected benefits from the merger, however, the new organization would have to rationalize its technical architecture, standardizing systems and applications platforms. In cases where a large company acquires a smaller entity, the IT architecture choices are often simpler, with the newly acquired parts of the company generally migrating to the larger firm's platforms.

This paper primarily focuses on the challenges faced by the organizations in consolidating and Integrating IT effectively so that it becomes a strong business driver. This paper also suggests a strategic approach that should be adopted by organizations to meet the objectives of the M&A.

## Challenges in M&A

The challenges that arise after an M&A generally fall into three areas: cultural, technical, and those related to compliance.

**M&A poses massive challenges for any IT infrastructure, especially in cases where organizations of similar size merge.**



- **Cultural challenges:** An M&A brings two distinct cultures face to face. This is akin to a union of two totally different people. Unlike in a relationship where one hopes the onus is on making it work, a corporate M&A always has an element of animosity, especially among the individuals at the target company, who tend to believe they have been taken over and upon whom the biggest adjustments usually fall. Conversely, employees at the acquiring company may feel like they no longer fit in. They may be disinclined to expend the necessary effort to build bridges in the new organization. They may be unready or unwilling to retool, realign, and relearn how to do their jobs. A lot of acclimatization and adjustment is expected on both sides.
- **Technical challenges:** M&A also bring to the fore the state of the companies' technical infrastructure. At the point of confrontation begins the exercise of planning a revamp or transfer of technologies, processes, and systems needed to establish a common regime upon which the new organization will operate.
- **Compliance-related:** When organizations merge there is a corresponding meshing of their compliance with applicable regulations. More often than not, organizations have achieved different levels of compliance, and the merged organization needs a strategy to bring the laggard up to par (or both up to par, if that is the case). In some instances, the M&A may bring the need to comply with new regulations, and that will require additional understanding, planning, and execution.

While this white paper concentrates on the steps necessary to overcome the technical challenges related to M&A, the other types of challenges are not to be underestimated.

## Making M&A Successful

When organizations combine or restructure as a result of a merger or acquisition, they need to:

- Inform customers of both entities on the need and impact of the merger
- Create a "100-day plan" outlining the priorities for the immediate activities and communications of the new entity
- Implement change management processes and thorough communication to all employees
- Streamline processes

- Integrate systems and implement new policies and procedures that leverage best practices

The key to a successful M&A is the effective and efficient integration of two organizations into a single business unit, capable of executing the vision of management. Integration of people, processes, policies, technology, products, customers, and solutions toward this vision is most important. The key aspects of a successful integration are shown in Figure 1 (see page 3).

It is most critical to document the desired "To Be" state at the earliest and ensure a core team is formed that will work toward that state.

## Safeguarding Information Security

Securing information before the merger is a key success factor but information security post-merger is more important and integrating this is a daunting task. If this is not done effectively, it will have serious effects on an organization's security posture, even making the combined organizations less secure than when they were separate organizations.

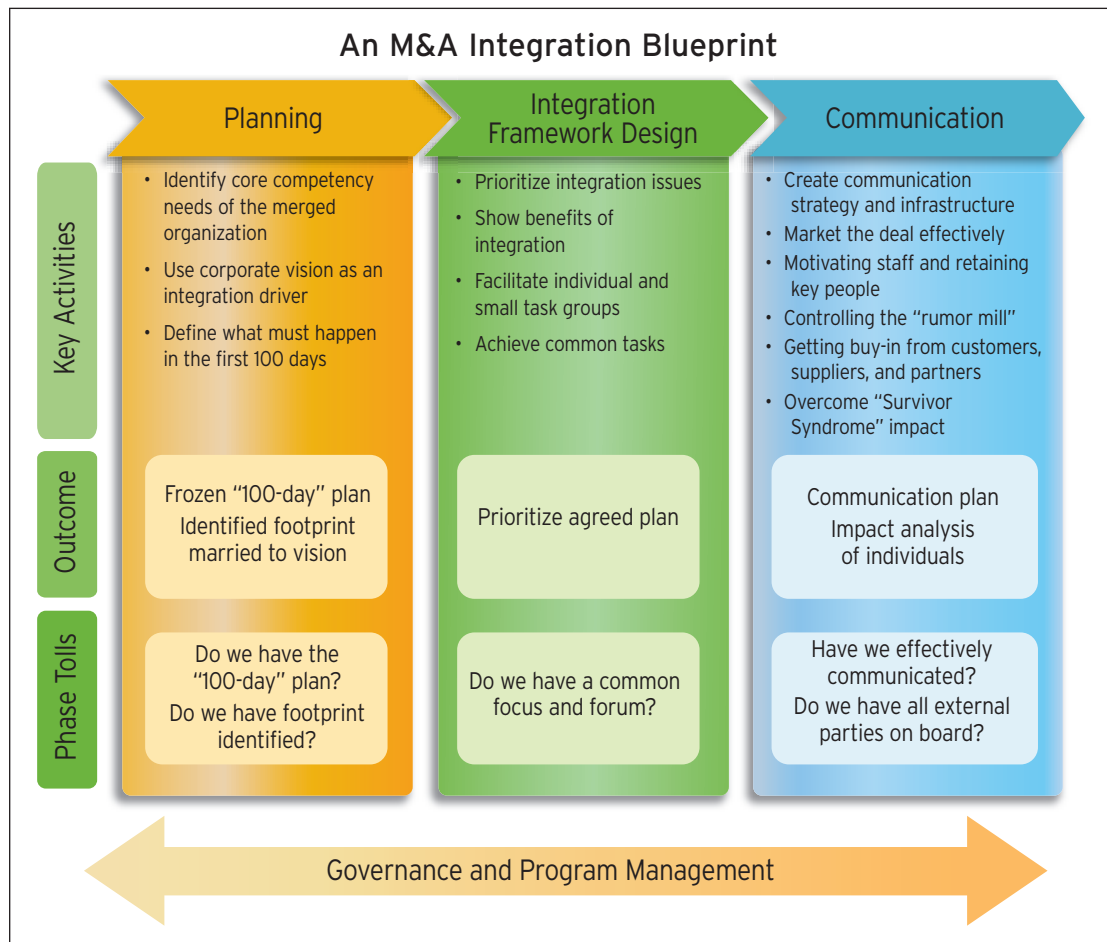
A loosely coupled architecture strategy carries the risk of exposing the organizations' vulnerabilities and could eat into profitability by increased incidents of phishing, malicious activity.

**A loosely coupled architecture strategy carries the risk of exposing the organizations' vulnerabilities and could eat into profitability by increased incidents of phishing, malicious activity.**

M&A activity encourages threats from within, as nervous insiders may fear how a consolidation might affect their job security. As a result, some may start hoarding valuable information from the network. All this contributes to the challenge facing a security team as it figures out the "100-day goal" of the M&A and how to best protect the organization. Information security consolidation is the best approach and involves:

- Aligning information security policies
- Implementing a strict information security regime
- Investing in information security sensors

The merged organizations should establish and empower a body or authority to ultimately decide the security policies. The security authority should keep compliance requirements



and obligations in view even if they go against the wish of the masses. Employees who are not accustomed to strict information security policies may be resistant at first -- that is to be expected.

**The merged organizations should establish and empower a body or authority to ultimately decide the security policies.**

The key is to move ahead with policies that are complete and well thought out.

Once policies are aligned, perform a gap analysis, assessing the status of the merged organization, generating a roadmap that states which procedural and

technological changes will be needed for the merged organization to comply.

After information security policies are integrated, a full-blown awareness program should follow. Even before the policy is completed, merged organizations should consider rolling out a short, focused awareness initiative on different types of security risks, including targeted phishing.

Desk-to-desk fliers, table tents in the cafeteria, and an email campaign can all be used effectively to warn employees that they should not trust every link and that they should always verify the apparent source of email addresses. It's also important to tell workers that they should never run an executable email attachment, even if it is included in a ZIP file. These are standard security best practices for any organization -- whether involved in an M&A or not. Once the new organization is in place, it is a good time to reinforce these practices.

If the consolidation of policies will result in dramatic changes to the way the merged organization conducts business, try to implement the policies in a phased fashion where possible. This will allow time for employees to adopt the new requirements and will offer the opportunity to review compliance progress and ensure that the integration process remains on track.

For example, if a staff member wants to impose content filtering where unfettered outbound access was previously the norm, it may be best to consider phasing it in by launching an initial phase that blocks only the most egregious sites, followed by a notification phase where users are warned that the content they are accessing would be blocked under the new policy. This gives users the opportunity to test the waters and identify areas where the new policy might interfere with business requirements.

Once the policy is in place, start the necessary assessment work as early as possible. Assessments are an effective way to find the loopholes in the system, concentrate on the opportunity for improvements (OFIs) that will emerge from the assessment reports. Each assessment will automatically help develop awareness and thereby help align information security policies.

Some of the critical security-related decisions that will eventually emerge include:

- **Whether to enable or disable USB devices.** Disabling USB devices on laptops is advised to lower the possibility of an internal data security breach or other insider threat. Before choosing this route, however, it is important to consider the political and functional ramifications of such a move.
- **How to handle malware and spyware.** Invest in robust anti-malware and anti-spyware that regularly reinvents itself and provides regular patches.
- **How to monitor firewalls and IDS tools.** Once the M&A is complete, members of the security team should watch for large amounts of data being transferred outbound across the Internet. Depending on employees' "normal" Internet usage patterns, organizations may want to set up a scan for any FTP or HTTP transfer of a file greater than a certain amount, such as 100 MB or 1 GB. Any violation could be a sign of a major data exfiltration. Monitor Web proxy logs as well to determine if attack tools are being downloaded and used inside either organization.

So, in the end, to avoid information security threats during an M&A, organizations should have two main goals:

- A long-term alignment of policies, procedures and technology, and;

- An augmented policy supported by a series of quick-hit technical defenses.

Successful execution of this two-pronged strategy can help merging organizations significantly lower their exposure.

## Consolidation of Technical Architectures

To reduce the cost and complexity of the IT environment, the merged organization has to eliminate redundant hardware and software, consolidate services, and enforce corporate IT standards.

Organizations should spend considerable time documenting the network architecture showing Internet and business partner connections for the merged organizations. They need to ensure the merged organization is capable of monitoring their "DMZs" (the "demilitarized zones" within their information networks separate from the production environment) and vital internal networks, specifically with intrusion detection system (IDS) sensors.

The merged organization should invest in consolidation and standardization of relevant client and server technologies that could eliminate datacenters and deploy a three-tiered load-balanced Web farm, reducing the number of servers by more than half.

Organizations should regain control of Web sites that were previously hosted externally and consolidate their intranet/extranet with simplified domain structure and site-naming standards to replace previous networks. There should also be a process of routing Web traffic to the new URLs.

## Email and Workflow

As in any organization, email systems are the way the post M&A entity will communicate, share data, and collaborate. Along with email, organizations have created workflows for such processes as purchasing, requisition handling, expense reporting, and other financial processes. A careful analysis of the existing systems should be performed. Based on the

**To reduce the cost and complexity of the IT environment, the merger organization has to eliminate redundant hardware and software, consolidate services, and enforce corporate IT standards.**

vision for the merged organization one system which “captures the best of both worlds” can be carved out. This requires a large cultural change management effort, and training is essential.

Another option is for IT senior management to elect one of the systems as the “winner” and migrate the other one over to it. A third, and much less common, choice is to choose a brand new email/workflow platform that is new to both entities.

### LAN and Wi-Fi

It is important to analyze the working culture of the two organizations. If one relies heavily on wireless computing but the other does not, there may be a significant difference in their vulnerability profiles. Rather than removing wireless from the culture, invest in checking the security settings of the existing wireless infrastructure. If it lacks encryption or has weak authentication, consider boosting the security with improved technology.

### Disaster Recovery and Business Continuity Services

An organization's proprietary data as well as its IT infrastructure are among its most valuable assets. As such, it is important to ensure that these assets are protected and to plan for any potential disruption in their availability and/or reliability.

**Creating a unified compliance team, consisting of compliance staff from both organizations, is an effective way to ease the process.**

The effectiveness of a disaster recovery solution is most often determined by the research, planning, and design of the solution performed during the early stages of the project. Each organization varies in size, business plan, and unique goals requiring custom disaster

recovery plans to ensure constant business continuity.

Disaster recovery is an important concept that should be understood by all organizations, large and small alike. The potential loss of important assets such as data, hardware, and software is too great a risk to ignore. With the added cost of downtime and loss of assets, the results can be staggering.

### Network Audit and Penetration Testing

While generally hidden from day-to-day view, your network infrastructure plays a fundamental role in ensuring your business runs reliably and securely. We strongly advise that you perform a thorough network audit to identify loopholes or recommended improvements in your IT infrastructure.

A network audit allows you to plan for future improvements and helps ensure that you continue to invest smartly in your network infrastructure.

### Handling Compliance Issues

When organizations merge, the respective levels of compliance also become one. More often than not, organizations are at different levels of compliance. The merged organization needs to have a future-state vision to work toward. This needs to be addressed in the “100-day plan” as it may affect customer service and accreditation.

The two key factors determining the difficulty of meshing compliance efforts are the industries of the partners and the specifics of the particular compliance provisions they must meet. Creating a unified compliance team, consisting of compliance staff from both organizations, is an effective way to ease the process.

An organization's compliance mandates are often driven by the industry or specific vertical in which it operates. Financial organizations are required to meet the provisions of the Sarbanes-Oxley Act (SOX) and Gramm-Leach-Bliley Act (GLBA). For CG companies that operate in Europe it is also very important that the merged organization be REACH (Registration, Evaluation, Authorization and Restriction of Chemicals) compliant.

In regard to each of the commonly applicable regulations mentioned above, the most critical issues to consider are:

- Access management
- Information security policies
- Protection of customer data
- Monitoring and testing

SOX Section 404 is the provision affecting IT security. This section calls for controls on IT systems that access sensitive customer and financial data. The statute is vague as to how to implement those controls, but it basically looks for documentation covering access management, encryption, firewalls and malware protection. In addition, a solid information security policy outlining implementation of these items must be in place.

From an M&A perspective, SOX auditors and regulators will look for reports on access management controls. Before the auditors arrive, though, there are some key questions organizations should ask to ensure both organizations are on a level playing field:

- What types of access management systems do the two organizations use?
- Are they both on Active Directory, or is one using LDAP while the other uses something else?
- What is the current state of audits of accounts at both organizations?

GLBA has similar provisions to SOX, but it's more focused on protecting customer data rather than access management. GLBA calls for:

- Encryption of confidential data
- Use of strong passwords for accessing systems, limiting employee access to customer data, and physical security for customer records

As with SOX, in an M&A situation, the security teams should compare each organization's:

- Encryption methods
- Customer data-handling procedures and overall adherence to their respective information security policies

- Policies and procedures, which will need to be adjusted to common standards for both organizations. Also, as with SOX, all of this needs to be documented for regulators

Even though all of the regulations are targeted at the same basic items -- access controls, protection of customer/consumer data, and monitoring network security -- be sure to observe the specific requirements of each. The regulations' similar mandates don't mean that compliance with one will translate into compliance for another.

In an effort to make the entire process easier, newly merged organizations must create a compliance point person for the melded entity. That person should come from one of the two merger partners and be able to work directly with compliance people from both to achieve compliance harmony.

## Conclusion

Any merger or acquisition presents risks and challenges in the areas of culture, technical infrastructure, and regulatory compliance. We have a proven track record of helping CG companies overcome these challenges and achieve the expected returns. We can help with every aspect of M&A, from strategy to change management programs to rationalizing the new organization's technical infrastructure and processes. We also help CG organizations operate their post-M&A technical infrastructure via our expansive global presence and reach. Whether offshore, nearshore, or onshore, we will help you ensure that the total cost of running this new entity is less than the sum of the two entities put together.

## About the Author

*Ramji Mani has 20 years of experience in Supply Chain Management (SCM), Supply Chain Execution, Advanced Planning Systems (APS), Supplier Relationship Management (SRM), Trade Promotion Management (TPM) in the Consumer Goods/Retail and Manufacturing industry. Mani has a track record of leadership and program management of global system implementations and business process reengineering for Fortune 500 companies. As the practice director for the consumer goods vertical within Cognizant Business Consulting, Mani leads all consulting engagements in TPM/CRS/SCM/WMS/Logistics for large customers in Europe, the United States, and the Asia/Pacific region. He can be reached at [Ramji.Mani@cognizant.com](mailto:Ramji.Mani@cognizant.com).*

## About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting and business process outsourcing services. Cognizant's single-minded passion is to dedicate our global technology and innovation know-how, our industry expertise and worldwide resources to working together with clients to make their businesses stronger. With over 50 global delivery centers and more than 64,000 employees as of June 30, 2009, we combine a unique onsite/offsite delivery model infused by a distinct culture of customer satisfaction. A member of the NASDAQ-100 Index and S&P 500 Index, Cognizant is a Forbes Global 2000 company and a member of the Fortune 1000 and is ranked among the top information technology companies in BusinessWeek's, Hot Growth and Top 50 Performers listings.

## Start Today

For more information on how to drive your business results with Cognizant, contact us at [inquiry@cognizant.com](mailto:inquiry@cognizant.com) or visit our website at [www.cognizant.com](http://www.cognizant.com).



**Cognizant**

Passion for building stronger businesses

### World Headquarters

500 Frank W. Burr Blvd.  
Teaneck, NJ 07666 USA  
Phone: +1 201 801 0233  
Fax: +1 201 801 0243  
Toll Free: +1 888 937 3277  
Email: [inquiry@cognizant.com](mailto:inquiry@cognizant.com)

### European Headquarters

Haymarket House  
28-29 Haymarket  
London SW1Y 4SP UK  
Phone: +44 (0) 20 7321 4888  
Fax: +44 (0) 20 7321 4890  
Email: [infouk@cognizant.com](mailto:infouk@cognizant.com)

### India Operations Headquarters

#5/535, Old Mahabalipuram Road  
Okkiyam Pettai, Thoraiipakkam  
Chennai, 600 096 India  
Phone: +91 (0) 44 4209 6000  
Fax: +91 (0) 44 4209 6060  
Email: [inquiryindia@cognizant.com](mailto:inquiryindia@cognizant.com)