M&A Information Risk Management: Towards Best Practices

"Someday, on the corporate balance sheet, there will be an entry which reads, "Information"; for in most cases, the information is more valuable than the hardware or software which processes it."
- Rear Admiral Grace Murray Hopper, US Navy (Ret)

As the economy goes digital (and global), competitive advantage is increasingly synonymous with information. More and more organizations are dependent on information systems to store their assets, be it a pharmaceutical company's novel drug formulations; a music company's original recordings of artists' latest albums; or a tech firm's code for new software applications.

Gaining competitive advantage through a merger or acquisition means that a company acquires the information assets of the target entity. How both acquirer's and target's information assets are integrated and shielded from various types of risk during the M&A can play a role in the success or failure of the new entity.

This paper discusses the challenges of managing information risk for several types of M&As and introduces a framework that can be used to address those challenges. The paper also offers a checklist of best information risk management practices for an M&A, based on the author's experience as a Certified M&A Advisor.

Choosing an Information Risk Management Approach

Companies pursue M&As to enhance their market position, drive growth, or to expand capabilities, products or services. Senior management typically focuses on four major areas during an M&A: brand protection, customer retention, cost reduction, and change management.

A robust information risk management (IRM) strategy supports the areas of management focus while creating value for the new entity. In this author's experience, managing information risk can be a challenge during an M&A, because it is typically a time of intense change and rapid execution.

Understanding the type of M&A the company is undertaking allows for more effective information risk management. M&As can be broadly categorized by the type of buyer (financial vs. strategic), the size of the deal, and the extent and speed of integration. These factors affect the overall integration strategy and call for different approaches to managing information risk (Figure 1).

The first M & A category are financial buyers who seek targets outside their market that will enable them to create value through transformation. These buyers will usually extend their existing products and services into a new geography or diversify by connecting with large conglomerates or private equity groups. Integrations are usually done slowly so as not to rock the boat for the target or distract people through rapid change.

For these financial buyers, the information risk management strategy should focus on compliance

How information assets are integrated and shielded from unnecessary risk during an M&A can play a role in the success or failure of the new company.

issues, laws and the regulatory frameworks that will impact the business. There is likely to be minimal formal integration and IRM teams must understand the resultant complexities in governance. The policies and procedures, although used to run distinctly different businesses, should be consistent across the two organizations. On the people side, IRM teams must recognize there are two different levels of risk awareness, skills and cultural knowledge. Since there is not full integration, there is little scope to bridge the gap between entities; this increases the complexities of governance. If not managed properly, this can adversely affect the strategic agility of the entities.

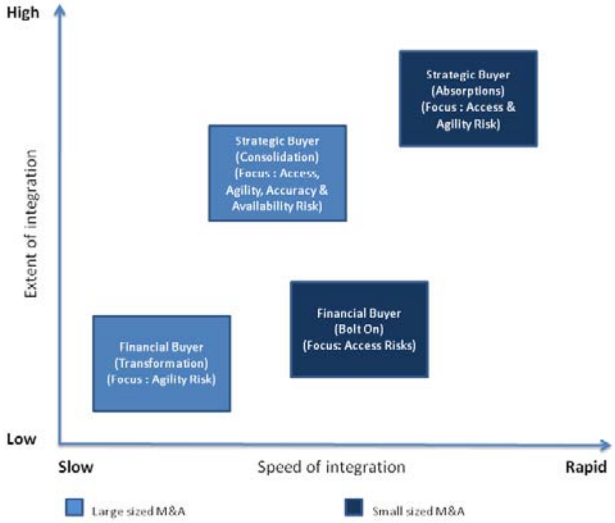
High
Extent of integration
Low
Strategic Buyer (Absorptions) (Focus : Access & Agility Risk)
Strategic Buyer (Consolidation) (Focus : Access, Agility, Accuracy & Availability Risk)
Financial Buyer (Bolt On) (Focus: Access Risks)
Financial Buyer (Transformation) (Focus : Agility Risk)
Slow
Speed of integration
Rapid
Large sized M&A
Small sized M&A

Figure 1

The second M&A category is the strategic buyer pursuing market leadership by consolidating two large entities to eliminate redundancies, improve operations, and leverage economies of scale. These M&As often warrant a full integration and are usually done at a modest pace. Pushing forward at a rapid pace could be risky, jeopardize the full value of the deal, and burn out resources from the sheer size of the effort.

For this strategic buyer, IRM teams should focus on classifying sensitive information to ensure the right people have the right level of information access, and the wrong people do not. The risks of any downtime and availability of information from systems migrations and integration of disparate systems should be well thought through; any downtime could affect customer retention and brand reputation. All obsolete and non-standard systems should be eliminated. Poor migrations and integrations often result in data accuracy and integrity issues, which have a huge impact on an organization's key business processes.

The third M&A category are those financial buyers who execute a series of "bolt-on" acquisitions to create a new platform for growth. These expansions could be geographic or involve vertical integration. The speed of integration is rapid, leveraging the skills and scale of the platform company. There is likely to be low extent of integration beyond eliminating redundancies and overlaps in corporate functions and the back office.

Here, the IRM teams should focus on compliance with specific regulations. Access risk and residual access risk must be evaluated and acted on quickly. There also needs to be a tight level of integration at the governance level, similar to that needed for the "transformational" financial buyer.

The strategic buyer who is absorbing a competitor – usually of a smaller size – are the final M & A category. This buyer seeks to capture operational synergies by eliminating excess capacity and enhancing efficiencies. This often includes merging sales functions, scrapping product lines or services, or closing offices.

M&As can be categorized by the type of buyer, the deal size, and the extent and speed of the integration. These affect the overall integration approach and mean there are different kinds of information risk to be managed.

While this is a full integration at rapid speed, extra care must be taken not to alter the risk profile of the target so much that it diminishes in value and takes on too much agility risk. In addition, access risks play a very important role in this kind of a merger, having the same level of impact as consolidation with full integration. The use of non-standard or obsolete systems stand a negligible chance and hence much time and effort is not spent on this area during absorptions thereby reducing accuracy risks. Frequently the methods used by the acquirer for managing availability risks are adopted by the new entity.

THE '4 A' FRAMEWORK: UNDERSTANDING RISK PROFILES

M&As create environments more complex than steady state operations, and thus should be viewed differently when managing information risk. It is also important to have a common IRM framework during an M&A, so that the integration and IRM teams can ensure changes are visible and controlled.

To manage, mitigate and monitor risk in this highly complex environment, it helps if the framework is robust enough to be customized by the type of M&A. The framework should allow for integration between the tactical tasks that help manage risk and the strategic imperatives of the transaction. Such an information risk framework also aids in building a common language of alignment between business design and the Information environment.

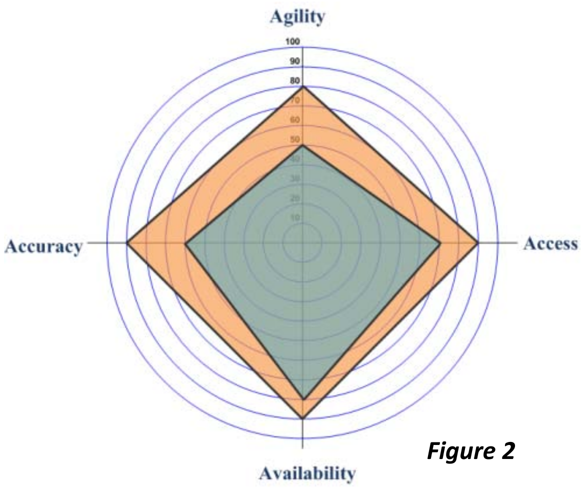

Figure 2

The 4 A Framework[1] is a model that allows IRM teams to look at all aspects of risk. Using this framework for M&As allows IRM teams to customize to the transaction, maintain transparency and connect risk management to strategic goals. Entities undergoing M&A can evaluate the risk profile of the acquirer and the target company, and that of the combined entity based on these parameters:

- Availability – keeping existing processes running and recovering from interruptions, while avoiding negative incidents such as outages and security leaks
- Access – ensuring that the right people have access to appropriate information and that the wrong people do not
- Accuracy – providing accurate, timely and complete information to all relevant stakeholders
- Agility – supporting changes in the business with acceptable cost and speed.

With the 4A Framework, the IRM team can manage top-down, rather than get bogged down in operational details right away. This can simplify execution.

It's important to note that the 4As are not independent of each other. For example, over-engineering access can reduce agility, while over-engineering agility can increase availability or accuracy risks. Ultimately, balancing the 4As in alignment with business objectives leads to better integration and risk management.

[1] *Applying the 4A Framework to M&A scenarios is an adaptation from a framework originally developed in George Westerman's paper "Understanding the Enterprise's IT Risk Profile". © 2007 MIT Sloan Center for Information System Research and Gartner, Inc.*

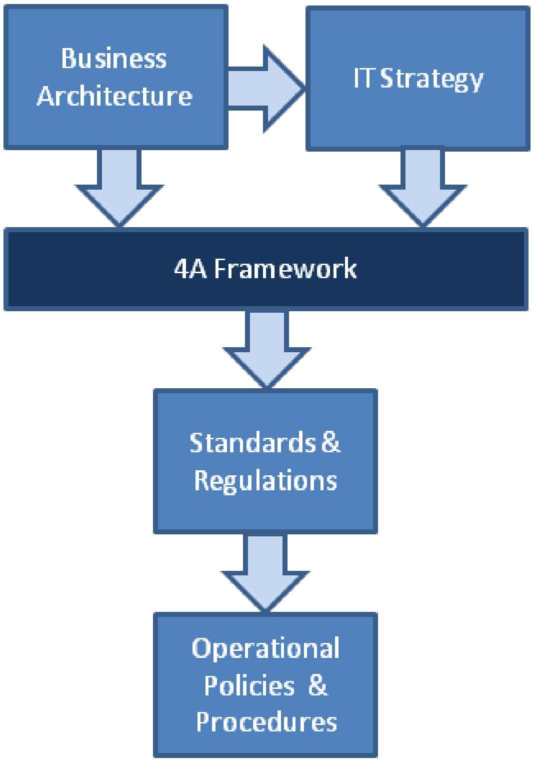

Figure 3

Integrating Risk Profiles

Seasoned M&A professionals usually tend to select either the acquirer's or the target's IRM approach because similar choices usually work for other functional areas.

Traditional information risk management professionals, on the other hand, tend to lean towards standards or regulatory frameworks during an M&A. While this does work for steady state operations, it often leads to issues during the transaction, because the risk profile of the new entity differs from steady state.

IRM teams also should avoid using either company's risk profile for the new organization. The best practice approach, the acquirer imposing approach, or a standard approach might work for other areas of integration, but not for information risk management.

An organization's business architecture revolves around five broad areas: customer segments, scope of products or services, geographic coverage, strategic differentiation, and profit pools. During an M&A, organizations tend to alter one or more of these areas. This impacts the IT strategy needed to support the new structure. As a result, the new entity is likely to have a different risk profile than either the acquirer or target. The information risk profile for the new entity should align with the new business architecture as well as the new IT strategy, thereby creating and protecting value for the new entity.

An example would be if the acquirer's focus has been historically skewed towards access and availability risks because of the nature of their business, while target's agility risk management was a competitive advantage for them. By imposing the acquirer's profile on the target, there will not only be erosion of competitive advantage and loss of value, but also perhaps new exposures for the new entity.

Best Practices for Managing Information Risk During an M&A

Based on the author's experience, these tactics are best practices for M&As from an information risk management perspective:

1. Get the information risk management teams involved right at the due diligence phase.

> *IRM teams should avoid using the acquirer's risk profile or the target's for the new organization. The best practice approach, the acquirer imposing approach, or a standard approach might work for other areas of integration, but not for information risk management.*

2. Form the governance committee upfront and get agreement on the merger imperatives.

3. Understand the risk profile of both organizations and agree on the risk profile of the new entity.

4. Ensure the risk profile, IT strategy and business architecture of the new entity are aligned.

5. Align information risk management with the overall risk management work stream supporting the business rather than have it as a work stream within IT.

6. Understand the strategic intent of the transaction and get a solid handle on the speed and extent of integration.

7. Some mergers are heavily focused on capturing synergies through cost reduction; make sure this does not come at the expense of increasing risk beyond the appropriate threshold.

8. Understand and classify all sensitive information early in the transaction. Know where information resides and ensure adequate controls are in place to protect it during the integration and in transit to the new control structure.

9. Critical skills and knowledge reside with people and both acquirer and target need to retain good people to make integration successful. Loss of key people during the M&A could increase project risk and increase costs while impacting efficiencies in other areas.

10. Understand the regulatory environment. Regulations such as SOX, HIPAA, Basel II, GLBA etc., may come into play. Though some regulatory guidelines might overlap, addressing one does not mean compliance with others.

11. Understand and document all cross border issues with respect to legal possession of systems, applications, transactions, data rights and regulations that might come into play.

12. Use of non-standard technologies can result in loss of agility and affect speed to market, procurement, invoicing, or other critical business processes, thus eroding competitive advantage.

13. Pay attention to all information migrations; most accuracy and integrity risks arise due to poor migration executions.

14. Give immediate access to information on Day Zero. People will need it to do their jobs. Improper integration or poor consolidation of access control systems could lead to access risks, potentially violating SOD rules.

15. Look for hidden liabilities in licensing that can increase costs.

Information risk management teams should be involved right at the start – at the due diligence phase.

About the Author

Nitin Kumar

CM&AA, CMAP, CGEIT, CGRCP, CMC

Nitin Kumar is a Certified M&A Advisor, a Chartered M&A Professional, Certified in the Governance of Enterprise IT, a Certified GRC Professional and a Certified Management Consultant.

He has extensive experience with high growth environments, turnarounds and start-ups, has held executive positions with global multi-billion dollar organizations and has served Fortune 500 clients in advisory and interim executive roles.

Nitin has spent many years in diverse M&A environments as well as consulting on information risk management in the US, Europe, Asia & Africa.

He currently serves as CEO for Aujas Information Risk Services and is based out of New York.

Nitin can be reached at nitin.kumar@aujas.com or 917.338.6773.

About Aujas

Aujas is a global information risk management company providing management consulting and technology life-cycle services. Aujas consultants work with the client management team to align information risk with business initiatives, so that security becomes a competitive advantage rather than a financial burden.

The company's holistic approach focuses on fundamental business issues and how they interrelate with risk mitigation strategy, governance, compliance and other key strategic information issues.

The U.S. headquarters for Aujas is located at 2500 Plaza 5, Harborside Financial Center, Jersey City, NJ 07311.

AUJAS
MANAGING INFORMATION RISK

Disclaimer: This paper is general in nature and is based on the experiences of the author. Aujas or the author does not claim to render professional advice or services through this paper. This publication is not a substitute for such professional advice and must not be used for any decisions affecting your business. Before making any decision or taking any actions that may affect your business, you should consult a qualified professional advisor. Aujas or the author shall not be responsible for any loss sustained by any person who relies on this paper.