

## How Should Companies that Acquire Firms Deal Involve Risk Management Teams as Part of M&A (Merger and Acquisition) Deals

Pranith Shetty

Information Security and Risk Lead, Cisco, New Jersey, United States of America

### ABSTRACT

Firms irrespective of the sector they are in or serving (Financial Services, Technology, Manufacturing etc.) look into Merger and Acquisition (M&A) prospects, there are varied reasons to it but most of the times it's to stay competitive and have an edge over competitors. As part of the M&A, there are different steps involved between the firms involved in the deal. In addition to those steps evaluating security posture and getting context on risks is very important to avoid future business impact. There have been a many papers and articles around the importance of involving cybersecurity risks in M&A discussions, as part of this research, its advised to understand the basic security posture of the firms, vendors , BC/DR, Physical security and policies etc. but there are some areas that are overlooked, however, the key problem is the absence of an overarching Risk management team in these deals, that helps keep tabs on all the risks in the register, tracking, monitoring etc. Presence of Risk management teams ensure risks identified through the process don't slip through the cracks, especially the Moderate and low rated ones since everyone is busy solving the Critical and Highs, crucial terms like the Risk appetite and tolerance of the acquiring firms can be brought into the conversations.

Risk teams are more often than not, playing catch-up, as a result, they can't function to their full potential for risk reporting that in ideal conditions, helps the senior leadership understand the story.

This article aims to shed some light on the M&A process and how involving the Risk management teams early onto these deals, can not only favor these M&A deals for the firms involved in the long run but also ensure there is no business impact down the road.

### \*Corresponding author

Pranith Shetty, Information Security and Risk Lead, Cisco, New Jersey, United States of America.

**Received:** November 11, 2023; **Accepted:** November 18, 2023; **Published:** November 25, 2023

**Keywords:** Mergers & Acquisitions, Risk Management, M&A, Information Security

### Introduction

Before diving into Security risks and how risk management has a part to play before, during and post Mergers & Acquisitions commonly called or known a M&A,

Its best to try and understand the basic definitions involved in this topic are

- M&A refers to the consolidation of companies or their major business assets through financial transactions between companies, without getting into too much detail, there are various types of Mergers & Acquisitions, Merger is when board of director of two companies approve the combination and seek shareholders approval, Acquisition is when the acquiring company obtains majority stake in the acquired firm, which does not change its name or structure.
- Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of
  1. The adverse impacts that would arise if the circumstance or event occurs and
  2. The likelihood of occurrence.

- Risk Management is the process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes

1. The conduct of a risk assessment
2. The implementation of a risk mitigation strategy and
3. Employment of techniques and procedures for the continuous monitoring of the security state of the information system.

### Rationale for this Study

There are several researches that have been performed and articles/ blogs written around the role of cybersecurity and information security in M& A, meaning how important it is to think about and be proactive when it comes to aforementioned risks in both domains, however, there is little to no research on the need to involve risk managers in those M&A due diligence sessions especially around Information security, Data privacy and other matters. There is no well-known articles that talk about how risk managers can play a crucial role if involved in early stages, this sets the background and context needed for future discussions around governance, policies and procedures, risk assessments, control environments etc.

This article here while giving a glimpse of standard M&A steps, also dives into the information security side of things the important benefits of involving the risk management team in the three phases during M&A that is the Pre-Merger, During Merger and Post Merger, how it helps set the stage with respect to the risk management lifecycle starting from Identification to risk reporting to Senior leadership, the Risk team don't have to exclusively wait for the risk assessments or conduct them for more information around M&A and all the control gaps and / or critical processes.

### Literature Review

As per Binary streams, a consulting team in M&A, most deals fail because of not assessing the complete security of firms involved including compliance regulations.

As per articles written by Cybersecurity leaders from IBM in Independent research blog named Security Intelligence, Cybersecurity leaders should be involved in M&A discussions, bring in someone like CISO helps and the risk management teams have reporting line to CISOs who would pull them in right away.

As per Dan in an article, Security needs to be involved way early in Mergers and Acquisitions, as part of Shift left security design or Security upfront approach to avoid business risks.

As per Richard in a Forbes article, there are data privacy and regulatory issues in M&A, only an equipped Risk management team can navigate all these risks and help management teams understand the business impact

### Strategy & Benefits

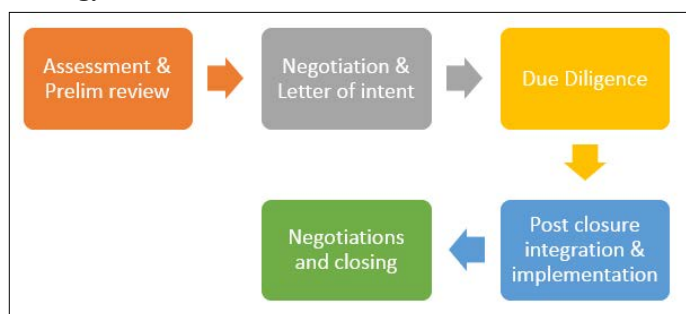


Figure 1: M&A Steps

In a standard M&A transaction, be it an acquisition of shares in the target company or an acquisition of the business of a target entity, tends to follow more or less the process visually described above. The said process is not final, and may differ depending on the complexity of the transaction at hand, type of businesses involved, verbal agreements beforehand and many more intricate details. In a more straightforward M&A transaction, some of the stages outlined below might be shortened or outright skipped.

- **Assessment and Preliminary Review:** It is a standard practice for an M&A transaction process to begin by an Information memorandum, this usually contains good enough detail about the company to be acquired or merged with, without divulging any sensitive information about data, assets etc. There would also be an NDA (Non-Disclosure agreement) that is intended to secure the confidentiality of information surrounding this potential deal.
- **Negotiation & Letter of Intent:** This step comes into play before Due Diligence when there is only one potential buyer, here various matters are considered around licensing, fiscal implications etc., if there are many buyers, Due diligence

exercise takes precedence.

- **Due Diligence:** This is an important step where all factors of the acquiring company are looked into, ensuring there are no risks that could potentially impact the sale.
- **Negotiations and Closing:** As the name suggest this is literally negotiations over the final price of the agreement and the SPA (Purchase agreements) are drafted.
- **Post-Closure Integration and Implementation:** After closing the deal

Now that we have understood the basics involved behind an M&A deal, it's time to discuss the Security and related considerations to be involved in this process.

Involving the risk management team early will help in the following security domains across the three phases, as listed below.

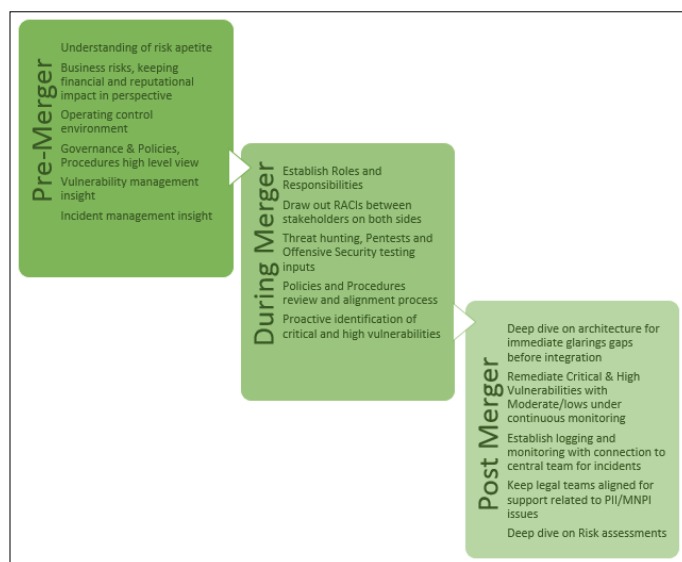


Figure 2: Benefits of Involving Risk Management Team across Three Phases

As we can see in the visual above, Risk management team when gets involved early on can ensure governance of programs like Vulnerability management, incident management they can tie these pillars to the Risk register for identification of risks, Risk rating, ownership, remediation and reporting. They will be able to guide risk owners through the risk management lifecycle over the course of M&A and beyond. Risk teams are well versed with the Infosec policies and procedures, operating control environment. These teams bring in a collaborative approach bringing in the security architects, program managers, accountable engineering teams to ensure there are no risks falling through the cracks, Information is communicated seamlessly to leadership through risk reports thus ensuring transparency as well.

All of these steps take a lot of time sometimes it might take years for the acquiring organization to completely assimilate into the acquired firm so that both operations look seamless from the outside to customers, Risk management teams when involved early get complete context into the Risk posture and can help the firms get there.

### Discussion and Extended Use Cases

These strategies have been based out of the organization structure of primarily technology firms that constantly are on the lookout for other firms to stay competitive and have an edge, in a certain line of business, however, these do apply to companies in manufacturing

and other sectors including finance. Risk management teams are existent in all lines of business so whenever companies or firms in various sectors are going through or planning to get into Mergers and Acquisitions, involving the Risk teams early might favor the overall assimilation of the two or more organizations involved in the deal. This approach has been practiced in technology firms through first drawing RACIs with the Risk management team and then collaborating with the central security teams that bring the new products/companies onboard. As said earlier, this strategy can be employed in financial firms, manufacturing sector, no roadblocks anticipated with this approach, it will enable information communication and transparency of the risk posture [1-9].

### Conclusion

Every firm at some point in time gets involved in M&A deals be it financial firms acquiring smaller business for customers, or smaller firms trying to get into the fold of conglomerates to stay profitable, or maybe its firms of equal strength getting to gather in a partnership for their own varied reasons of successes. Involving the Risk management team strategy needs to be part of every M&A since it not only helps the acquiring firm be proactive in terms of risk management lifecycle but at the same time ensures risks are not orphaned. It also sets expectations on both firms and avoids not only any last-minute repercussions but also future overall business impact. It ensures certain teams are not playing catchup, since Risk teams ensure collaboration across the board as part of the governance approach, risk reporting from these teams eventually helps the Senior leadership and management understand the overall risk posture and control gaps.

### References

1. Hayes A (2023) Mergers and Acquisitions (M&A). Investopedia. Available: <https://www.investopedia.com/terms/m/mergersandacquisitions.asp>.
2. NIST (2023) Risk-Glossary. CSRC. Available: <https://csrc.nist.gov/glossary/term/risk>.
3. NIST (2022) risk management - Glossary. CSRC. Available: [https://csrc.nist.gov/glossary/term/risk\\_management](https://csrc.nist.gov/glossary/term/risk_management).
4. PwC (2022) Mergers & Acquisitions - The 5 stages of an M&A transaction. Available: <https://www.pwc.com/mt/en/publications/tax-legal/mergers-and-acquisitions-5-stages-of-MA-transaction.htm>
5. Definition of Mergers and Acquisitions (M&A) - Gartner Finance Glossary, Gartner. Available: <https://www.gartner.com/en/finance/glossary/mergers-and-acquisitions-m-a->
6. Anita Hartman (2021) 667.pdf on Egnyte, Egnyte. Available: <https://sansorg.egnyte.com/dl/nBOWmEKj44>.
7. 4 common security issues mergers and acquisitions face. Binary Stream Software Inc. Available: <https://binarystream.com/blog/4-common-security-issues-mergers-and-acquisitions-face/>
8. Nick Coleman, Julio Gomes (2020) Taking the Risk Out of Mergers and Acquisitions. Security Intelligence. <https://securityintelligence.com/posts/mergers-and-acquisitions-without-cybersecurity-risk/>
9. Dan Swinhoe (2019) Why security needs to be involved early during mergers and acquisitions, CSO Online. Available: <https://www.csoonline.com/article/567249/why-security-needs-to-be-involved-early-during-mergers-and-acquisitions.html>.

**Copyright:** ©2023 Pranith Shetty. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.