International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|

DOI: 10.15662/IJSRAT.2026.0903002

Cybersecurity Integration Framework for Mergers and Acquisitions

Vilas Shewale

Independent Researcher, USA

Publication History: Received: 15.04.2026; Revised: 07.05.2026; Accepted: 10.05. 2026; Published: 15.05.2026

ABSTRACT: The practice of merger and acquisition transactions predictably produces a unique period of cybersecurity exposure lasting the 45-90 days immediately following the transaction's close. Throughout this interval, the acquired business unit must operate on the basis of the cyber deficiencies inherited, inconsistencies within the privilege controls assigned to its users and insufficient access to or understanding of the cybersecurity processes employed by the acquirer. Despite considerable literature about cybersecurity in mergers, most treat this as either a due diligence activity solved during the pre-deal period or an effort to create full and consistent similarity over 12-24 months, which leaves little published research covering effective strategies for those 45-90 days.

The cybersecurity integration framework proposed here aims directly at that 45-90 day period. The framework includes parallel efforts along four lines of activity; **directory and policy**, **endpoint management**, **privilege controls** and **visibility and compliance;** bound by a reusable **runbook template**. The framework utilizes a **four-phase gated decision model** with well-documented criteria for both entering and exiting each phase, plus a hybrid pattern for merging user and resource identity management that addresses situations involving both on premises Active Directory and cloud identities, common today in acquired entities. The pattern proposed is a general-purpose and vendor-neutral concept intended to serve across multiple industries and the paper is intended to bridge between high-level concepts about merger integration and the step-by-step vendor guides to specific products that often are the sole reference documentation available to practitioners.

KEYWORDS: Mergers and Acquisitions; Cybersecurity Integration; Privileged Access Management; LAPS; Endpoint Privilege Management; Identity Integration

I. INTRODUCTION

What information security does the world's literature cover on mergers and acquisitions? We learn that when firm X buys firm Y, X will not get only Y's products, markets and employees. X also takes on Y's servers, all running some unknown software from some unknown origin that has never patched yet, many times not set to proper configuration files, Y's admins (also having some other passwords in the same company), the entire application tree Y relies on that few people documented when Y went live last year. Every lack of security controls and misconfigurations over Y's years of life in IT systems that many were unable to document and patch due to time. This post-transaction close period when all these companies are tied together, by some stretch of the definition, is the time when we are most vulnerable. Y runs under Y's prior security setup. Meanwhile, attackers (ranging from states all over the globe to ransomware criminals) also know how to prey on companies fresh off having undergone mergers, precisely during this vulnerability window [1] [2].

Management studies of M&A integration beginning from Johnson and Goetz [3] to Rikhardsson and Yetton [4] showed how effective IT integration matters most for performance after a merger, treating security mainly as a secondary attribute. Vendor guides focus on specific tool deployment such as installing Microsoft's Local Administrator Password Solution (LAPS) or Endpoint Privilege Management (EPM) or migrating credentials from Active Directory to identity solutions, yet lack a comprehensive framework for dealing with what should be done in situations like the acquisition of firm 14, 18, 23-each requiring adherence to common security guidelines than taking an inordinate amount of time (years).

The output is a vacuum left in our methods. Businesses that deal with these sorts of transactions daily must secure the newly acquired property's safety rapidly. However, we only find guidance which recommends generic advice (try to match security) or provider manuals (add a new EPM agent on machines) but lacks the connecting approach which

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|
DOI: 10.15662/IJSRAT.2026.0903002

gives guidelines on repeatable, tech neutral implementation, where advice on security matches the acquired business size, locations and technology stack

.

The framework that this paper suggests is described. We cover the cybersecurity risks that are involved in acquisitions (M&A), along with available literature in Section 2. Section 3 covers the integration method's architecture: four workstreams. We provide details on a phase gate system in Section 4. We then turn to one of the common factors in today's M&As: hybrid identity. Section 5 touches on these themes, followed by a concluding Section 6, covering constraints and findings.

II. THE M&A CYBERSECURITY EXPOSURE WINDOW

The principle of this paper rests on the observation that acquired assets exhibit a measurable and predictable security risk pattern in the period following transaction close. Figure 1 illustrates the exposure window.

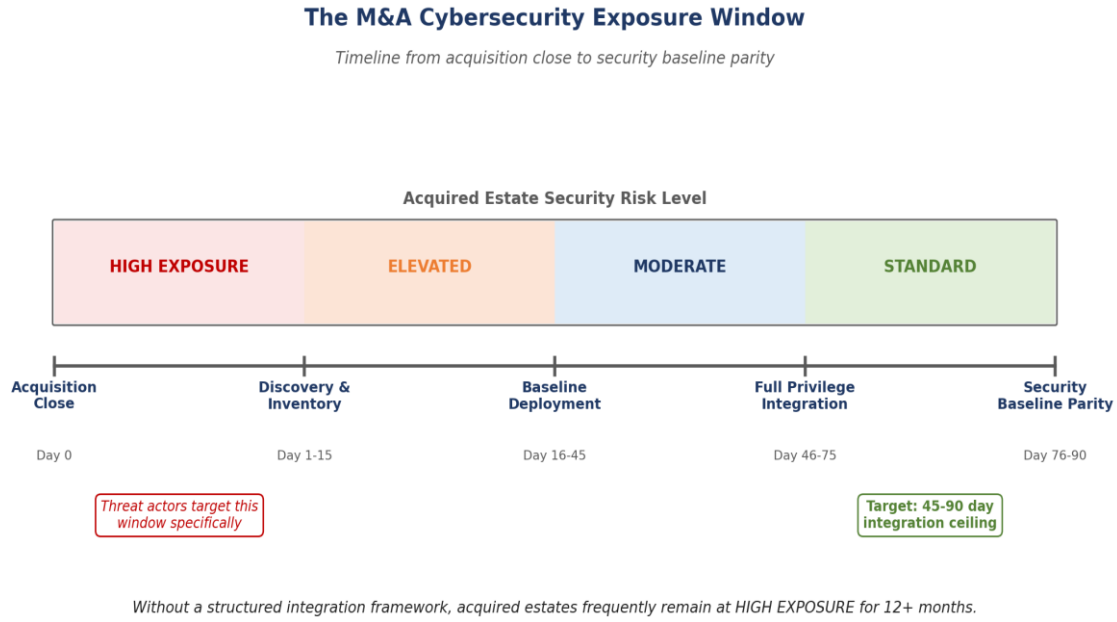

Figure 1. The M&A Cybersecurity Exposure Window. Acquired estates carry inherited security debt that is most acute in the days immediately following close and reduces only as integration activities progress.

First, the target was secured according to the practices, risks and needs of its previous owners, a completely different context to that of its new owners. It was properly hardened against the threats to the original organization, but these security practices were inappropriate for the target company post close, where a stringent set of NERC CIP, TSA Security Directives, SOX or NIST SP 800-53 standards may now be mandated for the combined company[5] [6] [7]. This differs to standards it may have previously been subject to. Second, integration itself introduces an extended surface: security domains that trust each other based on new relationship structures, the misuse of shared credentials used during integration, elevated access required by an integration team over a prolonged period or connections made during migration. Third, actors targeting an acquired entity take advantage of the publicity of a takeover to exploit opportunities during the disruption, because these public reports signify the security vulnerabilities caused by the stress of the takeover [8].

Three structural conditions combine to generate an exposure window, starting on the day the deal closes and extending to when the target company is fully integrated and up to speed to match the current security standard of the combined company at which point the organization is at materially greater exposure. The longer or shorter this is open, depends on the method of integration used. While unstructured integration typically extends the exposure window for up to 24

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|
DOI: 10.15662/IJSRAT.2026.0903002

months, well-run integrations shorten the security exposure by closing the window within 45 days in most acquisitions and sometimes extending longer only for major takeovers that are complex in scale.

2.1 Why Existing Literature Does Not Address the Window

There are three areas in the published literature that fail to meet this need:

Management literature, especially the M&A integration subgenre, is missing pieces. Johnson and Goetz (2003) [3] found it takes five times longer to conform financial services M&As to an enterprise's security posture than their nonfinancial counterparts and Rikhardsson and Yetton (2001) [4] reported that the key determinant of post-merger performance is the extent to which IT has been successfully integrated (the subject of our next section). While valuable, these insights merely describe the problem than offering concrete methods to bridge this management literature gap.

A second category of related work comes from cybersecurity vendors. Palo Alto Networks (2021) [9], CrowdStrike and leading vendors of identity management solutions offer guidance for M&A security due diligence. This advice falls into two extremes: high-level principles like "assess the acquired environment, " or low-level product-oriented instructions such as " deploy our solution. " This kind of guidance omits the necessary architecture that connects disparate software and workflows in the two entities to integrate across multiple compliance frameworks (HIPAA, GDPR, PCI DSS, SOX) in an orderly, repeatable fashion.

The third category includes books for cybersecurity practitioners on building strategy and architecture (Schwartz, 2020, Johnson and Johnson, 2018) [10] [11]. These books touch upon fundamental topics such as Zero Trust principles, management of privileged identities, architecture for managing identities and the security elements for M&A integration. While these topics are all critical, these texts tend to cover M&A integration as either an isolated chapter within the larger context or simply as a topic not falling within their remit. How to translate these principles and other security building blocks into a well-defined, achievable 90 days playbook that can be applied in complex, heterogenous acquired environments is lacking from published sources.

III. FOUR-WORKSTREAM INTEGRATION ARCHITECTURE

The proposed integration framework organizes activity into four parallel workstreams, each addressing a distinct security dimension, all governed by a shared master runbook template that is customized per acquisition. Figure 2 illustrates the architecture.

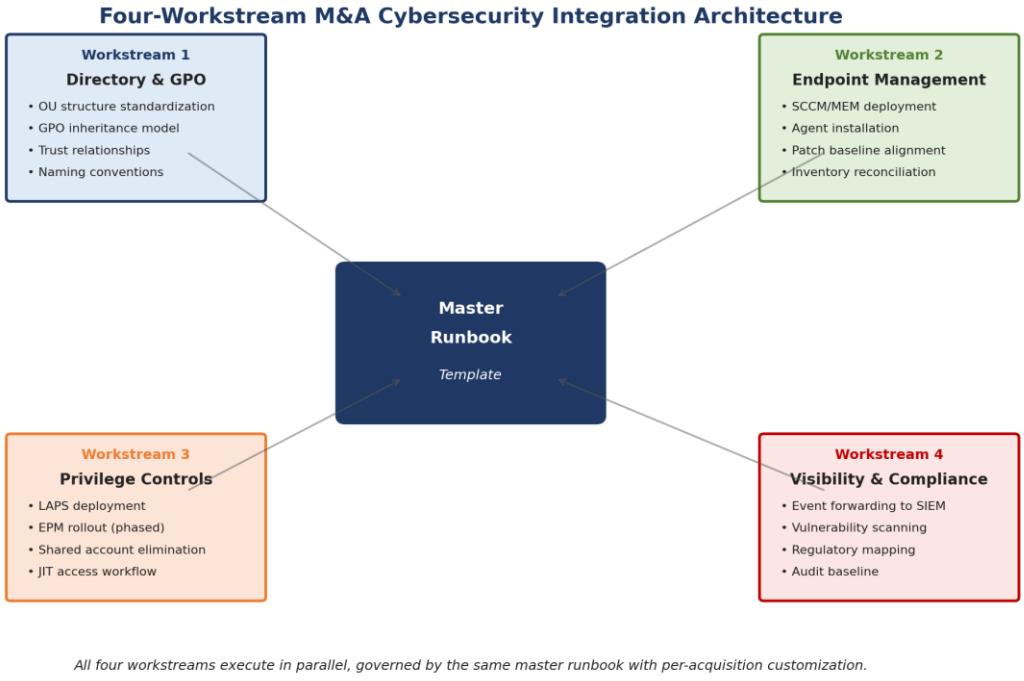

Figure2. Four Workstream M&A Cybersecurity Integration Architecture

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|
DOI: 10.15662/IJSRAT.2026.0903002

All workstreams execute in parallel, governed by a master runbook template with per-acquisition customization.
The problem is this: all M&A transactions require a massive number of tasks and regulatory requirements to be completed. There is simply too much to do to treat this as a single project sequenced in stages. On the other hand, these tasks often have dependencies so they cannot be treated as independent, separate, sequential work streams without creating confusion, rework and potentially huge gaps. The four work streams resolve this: it divides the massive number of tasks into four parallel work streams and defines explicit points of coordination and dependencies. We handle dependencies that cross workstreams with what is called a Master Runbook.

3.1 Workstream 1: Directory and Policy

This first workstream and thus all subsequent security workstream outcomes, relies heavily on creating and managing the foundational elements in Active Directory: 1) create a new OU structure in the acquirer's existing AD that duplicates the organization structure in the acquired company, 2) carry out the GPO inheritance structure to extend acquirer baseline security policies to the new OUs while minimizing disruption to the daily operations of acquired company users and 3) if the company will maintain the acquired entity's current domain, extend to the acquired entity's domain AD domain trust, 4) standardize computer names and the names used for user and security group objects and standardizing all policy names and descriptions, these last steps will enable full automation down the line.

A common pattern seen is organizations will use standardizing OU naming conventions starting with their first acquisitions and then reuse these standards across every acquisition since that time. If there is an inconsistency with the OU naming conventions between acquirer and target entities, the integration workload will continue to stack with each new acquisition, if, however, there is consistency, there can be a template effect, so that every succeeding acquisition becomes quicker than the last since the AD environment can be anticipated.

3.2 Workstream 2: Endpoint Management

Workstream 2 makes sure the end points belonging to the acquisition become properly incorporated into the endpoints controlled by the purchaser. This process includes deploying the relevant Microsoft Endpoint Manager (Intune) or System Center Configuration Manager site roles (Management Points), the Microsoft Endpoint Manager management agent on all devices owned by the acquisition, integrating a consolidated inventory count that accurately details the hardware, software assets owned by the acquired firm to the assets that are managed by the purchase organization's existing Asset Management Database, setting up the patching standards and baseline configuration of each device to that used within the larger business of the acquirer and creating the necessary application installation packaging to ensure that applications can be deployed or software can be updated accordingly to the former business of the acquired company on devices belonging to it.

This is the phase in which the largest of the surprise "gotcha's" typically appear. More than once has this workstream discovered many unmanaged or partially managed endpoints like digital signage kiosks, point-of-sale (POS) systems, field data devices or even workstation environments managed by other organizations that need to be brought under management or noted. Asset management's reconciliation of discovered devices against the known inventoried assets of the two organizations can be a time-consuming element of the whole integration process.

3.3 Workstream 3: Privilege Controls

Workstream 3 involves much of the heavier security work. Its objectives include deploying Microsoft LAPS (or the more modern Windows LAPS [12]) across the estate being acquired to end-to-end use of shared local admin credentials, phasing endpoint privilege management by starting with discovery, progressing to multiple pilot waves and finally bringing enforcement globally. Additional tasks include eradicating shared service accounts with local admin rights and setting up just-in-time access flows for the legitimate administrative work that does require these rights.
The phase approach is critically important. Attempting to enforce EPM before sufficient app discovery almost never works because acquired businesses often have critical applications that cannot handle privilege elevation restrictions [13]. The discovered first pattern - EPM monitoring-only deployments with an allowed list built over 30 days and including several small pilots before enforcement - are the pattern that success relies on for greenfield EPM deployments and is equally applicable to acquired situations.

3.4 Workstream 4: Visibility and Compliance

Workstream 4 provides visibility to acquired endpoints within the acquirer's security operations center (SOC) and accounts for the acquired assets under the same regulatory requirements. The following are typical activities carried out in this workstream:

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|
DOI: 10.15662/IJSRAT.2026.0903002

- Configure Windows Event Forwarding to feed events collected from acquired endpoints to the acquirer's Security Information and Event Management (SIEM)
- Integrate acquired entities into the acquirer's vulnerability scanning tool and schedule.
- Perform an assessment to map the acquired entity's compliance posture to the acquirer's regulatory obligations, identifying and documenting gaps.
- Establish the baseline that will be used to report ongoing compliance activities.

This workstream is often de-prioritized, as the acquirer's security team does not typically see the work produced by this workstream (in the same way they can see credentials and endpoints produced by the other workstreams). De-prioritizing is a bad practice. If security teams are not running workstream 4, then the SOC team has no visibility into what is happening on acquired systems and cannot prove that the integration has completed. A simple test to determine if integration is complete is if a security event that takes place on an acquired system triggers the same SIEM alerting as would have taken place if the event happened on a non-acquired system.

IV. PHASE-GATE DECISION MODEL

Workstream 4 architecture establishes what work happens. The phased decision model determines when each piece of work happens and what conditions must be satisfied before progressing to following phases. Figure 3 illustrates the four phase model.

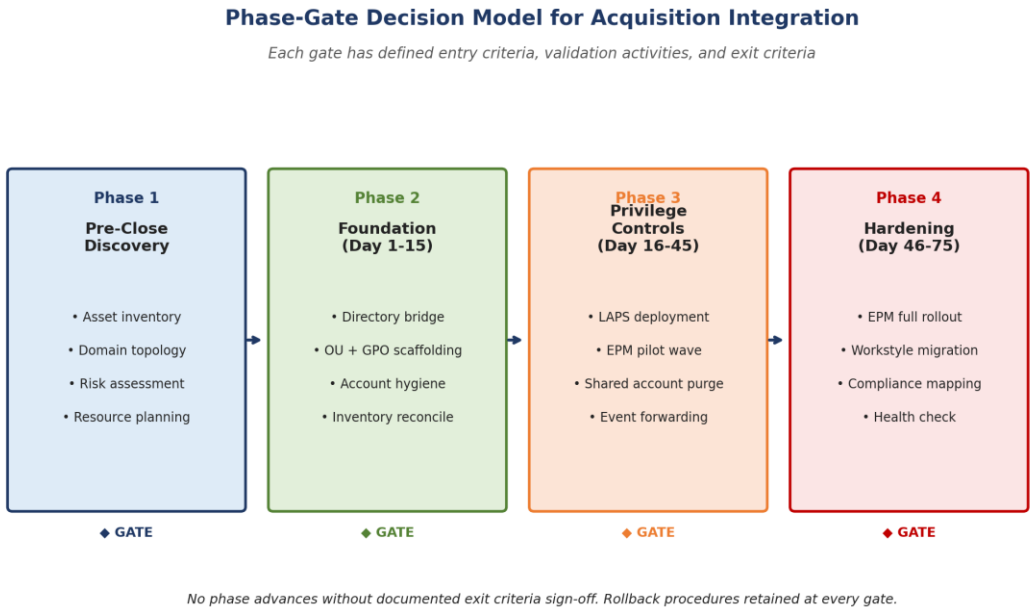

Figure 3. Phase-Gate Decision Model for Acquisition Integration

Each gate has defined entry criteria, validation activities, and exit criteria before the next phase begins.

The stage gate model is a management process that is been used to impose discipline over chaos. The organization requires 4 sequential steps, with defined criteria-the entry gate (what should be true before starting the stage) and the gate closure criteria (what should be true before starting the next stage), a list of validation activities performed in the stage, Gate review performed by the program manager of the integrated product and by the information security (IS) head of the purchasing organization. Neither stage passes without a recorded sign-off.

4.1 Phase 1: Pre-Close Discovery

Phase 1 starts when NDA terms are favorable for sensitive due diligence between the two parties and ends upon the transaction's closing date. Its primary goal is to be aware enough of the acquired firm's tech assets and integrations to execute the Phase 2 foundation tasks efficiently during post close integration. Entry criteria for Phase 1 include an

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|
DOI: 10.15662/IJSRAT.2026.0903002

executed NDA and other confidentiality rules in effect that will allow the sharing of technical details about the acquired entity. Phase activities include the creation (or reception from the acquiring organization) of an asset inventory (by population type), development of the acquired organization's domain topology map, outlining regulatory demands impacting the acquired firm's assets and workforce planning for the post-close integration team. Criteria to successfully exit Phase 1 are a documented inventory (by population type) of all acquired endpoints managed by the integration team and an acquirer CISO approved domain integration plan.

4.2 Phase 2: Foundation (Days 1 to 15)

This phase occurs right after transaction closes and spans the first 15 days. The main goal is to set up the directory services bridge and a solid, accurate inventory benchmark that will be critical for all future phases. Phase entry is only granted when the transaction closes and the integration team is granted the necessary access credentials into the acquired company's environment. Key phase tasks include setting up an Active Directory (AD) trust or a domain extension of AD, making an organizational unit (OU) and group policy object (GPO) framework underneath the acquirer's domain, executing a thorough account hygiene process (finding all shared accounts, abandoned accounts and all accounts that pose security risks due to their privileges) and finishing the inventory verification process against the baseline created during Phase 1. When phase entry criteria are all met, which entails that the acquired business is accessible via the acquirer's directory services, the OU/GPO structure is ready to go, and the inventory adjustment found in relation to Phase 1 has been documented and resolved.

4.3 Phase 3: Privilege Controls (Days 16 to 45)

Phase 3 deploys the privilege controls closing the important phase of exposure. This phase begins upon meeting Phase 2 exit criteria. LAPS is deployed to the entirety of the acquired endpoint estate. EPM agent is installed across endpoints with policy active in monitor mode. The initial pilot runs for EPM policy Enforcement are kicked off targeting specific user sets. Shared administrative accounts, discovered in Phase 2, are deleted. Windows event forwarding is configured from acquired endpoints into a SIEM within the acquirer. The exit criteria for Phase 3 include reaching over 95% LAPS coverage of acquired endpoints, successfully installing EPM agents in monitor mode to every in-scope endpoint, establishing confirmed end-to-end event forwarding into the acquirer's SIEM and eliminating the last remaining shared local administrative credentials.

4.4 Phase 4: Hardening (Days 46 to 75)

The fourth and final phase of acquisition, at its core, takes everything that the acquired company previously had at their baseline security and pushes it all to the acquirer's baseline security. Entering Phase 4 requires successful fulfillment of all Phase 3 exit criteria. Tasks involve implementing EPM for all users within the acquired entity in waves, leveraging the discovery first pattern, transitioning users from broad, generic policy structures to those in the acquirer's workstyle library, thoroughly mapping the acquirer's regulatory requirements versus the acquired company's actual compliance posture and identifying and rectifying all the security gaps in the newly integrated estate and finally conducting a baseline assessment (internal or via a third party) of the new, fully integrated company. Exit criteria at the end of Phase 4 include ensuring all privileges on the acquired system match the acquirer's defined standards, addressing all discovered compliance gaps through remediation or acceptance of risks and ensuring the newly merged environment passes a security health check.

The target duration for this phase, 75 days, yields the overarching integration target range of 75 to 90 days for standard acquisitions.

However, if the acquisition involved more complex security environments, such as different ID environments (detailed in Section 5 below), an additional 15 to 30 days might need to be added to Phase 4, bringing the overall acquisition range to 90 to 120 days. If the integration timeline exceeds 120 days before baseline parity is achieved, this acquisition should be noted as a deviation and there should be an examination to identify systemic obstacles that this general approach might not be capable of resolving.

V. HYBRID IDENTITY INTEGRATION PATTERN

The framework as presented through Section 4 assumes a primarily on premises Active Directory environment. Modern acquisitions increasingly involve target organizations whose identity infrastructure has shifted partly or entirely to cloud identity like Microsoft Entra ID, primarily, though similar considerations apply to Okta and other cloud identity providers. The hybrid identity pattern described in Figure 4 addresses this case.

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|
DOI: 10.15662/IJSRAT.2026.0903002

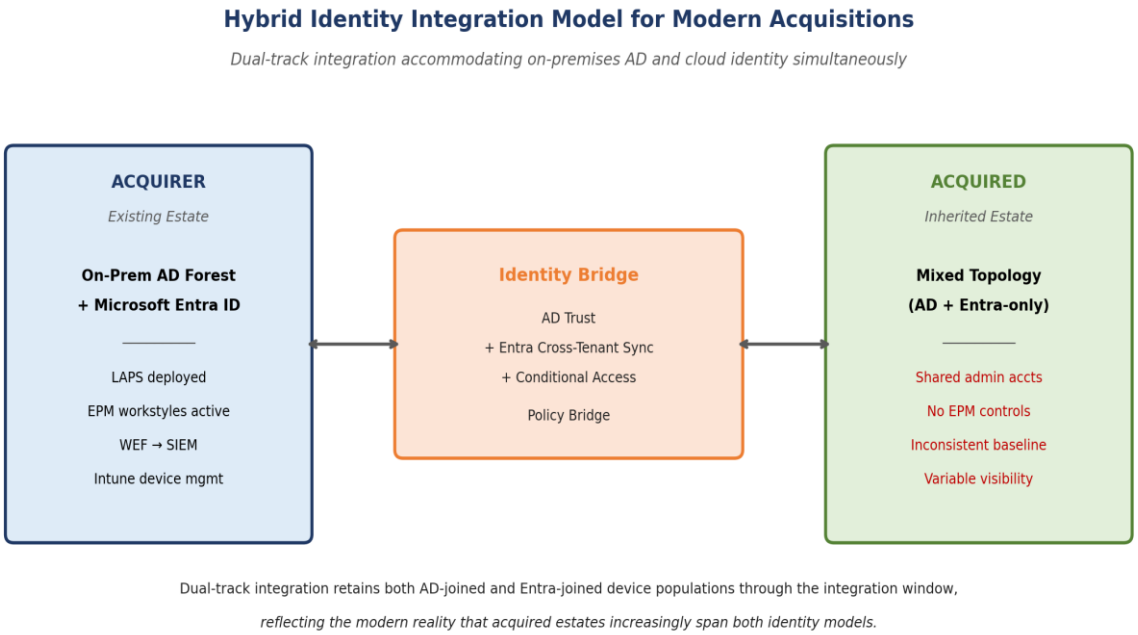

Figure4. Hybrid Identity Integration Model for Modern Acquisitions

Dual-track integration retains both AD-joined and Entra-joined device populations through the integration window.
There are really two parts to this problem. First, you may own devices that join AD, Entra or both. So a single integration needs to support two different ways of managing devices. Second, the tools you already use for privilege management work in pure AD environments. For example, LAPS or GPO-based EPM policy. These do not extend to Entra joined devices. On these, you need to deploy through Intune. So, you need either let one drive and force people onto another setup or design an integration that can accommodate both at the same time.

Here at the center is the identity bridge itself. You will use Active Directory trust for any existing AD joined population and have Entra Cross Tenant Synchronization (or equivalent) for the Entra joined one. Then use Microsoft Conditional Access policies spanning both, to force the same risk based security decision to be made on any endpoint regardless of what type of identity it is using. And you want the same policy bridge configuration, so your security controls are enforced consistently. This hybrid approach is what is required today. All the orgs we get have started to work more like cloud native orgs. So, this hybrid model is encouraging than discouraging.

VI. DISCUSSION, LIMITATIONS, AND CONCLUSION

In essence, this paper introduces a middle ground method or a practical how-to document, between the broad principles in "M&A Integration" from Ernst & Young and the granular instructions from individual technology providers. Assuming the company performs acquisitions often, its main utility for large organizations would be offering a reproducible template that allows them to transition from the several weeks or months of vulnerability they commonly experience through typical, haphazard integrations to the intended 45 to 90 days that this four step process should provide through each phase gate.

Some aspects prevent the framework from being effective for everybody. It assumes the organization buying another company mainly relies on an Active Directory to manage users. Companies with different kinds of identity services, either cloud native identity solutions or entirely non Windows workstations, will have to work out the four main processes. Similarly, the methodology suggests that the company performing the acquisition must have the resources to run all four processes at once. Organizations smaller in size could possibly run them one after the other, in sequence, than side by side, but they will need to recognize that this means the full integration timeline will be longer. Also, each of the phase timelines assumes that the organization being bought is readily accessible to technology and will cooperate. This is obviously not the situation for hostile acquisitions or mergers where regulators hold up access to

|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|
DOI: 10.15662/IJSRAT.2026.0903002

information or the purchase of a company that is in financial trouble, as this would extend the amount of time necessary to complete the steps involved. The plan does not cover the often critical issues related to bringing together employees and cultures, which typically proceed at different rates and are overseen differently than the information security process that the methodology intends to organize.

Beyond the constraints, this framework offers a concrete solution to a persistent gap in existing approaches to M&A cybersecurity integration. When organizations close deals, their newly acquired IT systems present a "cybersecurity exposure window" a recognized danger that can pose significant risks. Yet, a scarcity of publicly shared and replicable methodology for closing this gap means each acquiring organization must independently craft its integration plan from scratch for every deal it undertakes. This paper aims to provide assistance at the level at which such companies actually operate. They deal with a disparate array of acquired systems, a mix of varying compliance mandates and a broad range of cybersecurity vendors, all while operating under the reality that acquisition processes cannot be halted just so integration teams can meticulously develop entirely new procedures.

To further enhance this area of research, significant benefits would arise from joint studies involving different organizations that evaluate integration timelines under varied frameworks. This paper presents a structure that reflects proven and effective practices from real-world scenarios. However, the cybersecurity research field could greatly expand its knowledge base through comparative investigations of multiple acquiring entities that use diverse integration methods. Specific avenues for further study could involve precisely quantifying the level of risk exposed during the cybersecurity exposure window relative to the integration duration, automating with artificial intelligence the difficult tasks of discovery and inventory reconciliation, which currently consume much of Phase 1 and Phase 2 efforts and testing the broad applicability of the framework beyond the usual study subjects. Industries such as healthcare, banking and organizations operating critical infrastructure, which frequently engage in acquisitions, are prime candidates for this exploration.

Mergers and acquisitions will persist as a fundamental component of how large corporations grow, expand their market share and acquire new capabilities. The cybersecurity integration hurdle following every acquisition will remain an ongoing challenge. The referenced framework presented herein is intended as a contribution to the practical methodologies situated between management theory and product documentation. It acknowledges the immediate need that acquiring companies have for this bridging methodology, as they are unable to await the formal standards development to align with the demanding realities of integrating diverse acquired systems on a massive scale under tight time constraints.

REFERENCES

1. Verizon. 2024 Data Breach Investigations Report. Verizon Business, 2024. https://www.verizon.com/business/resources/reports/dbir/
2. IBM Security. X-Force Threat Intelligence Index 2024. IBM, 2024. https://www.ibm.com/reports/threat-intelligence
3. Johnson, M.E. and Goetz, E. Information Technology Integration in Financial Services Mergers. Tuck School of Business at Dartmouth, 2003.
4. Rikhardsson, P. and Yetton, P. The Effectiveness of IT Integration in Mergers and Acquisitions. Journal of Strategic Information Systems, 13(4), 305-321, 2004.
5. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53, Revision 5. National Institute of Standards and Technology, 2020. https://doi.org/10.6028/NIST.SP.800-53r5
6. North American Electric Reliability Corporation. CIP-007-6: Cyber Security — Systems Security Management. NERC, 2016. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
7. Transportation Security Administration. Security Directive Pipeline-2021-02D (SD-02D): Enhancing Pipeline Cybersecurity. TSA, 2022.
8. CISA. The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. Cybersecurity and Infrastructure Security Agency, May 2023. https://www.cisa.gov/news-events/news/attack-colonial-pipeline
9. Palo Alto Networks Unit 42. Security Considerations for Mergers and Acquisitions. Unit 42 Threat Intelligence, 2022. https://unit42.paloaltonetworks.com/mergers-acquisitions-cybersecurity/
10. Shewale, Vilas. Cybersecurity in the Modern World: Protecting Data, Privacy, and Systems. Amazon Kindle, 2025. https://www.amazon.com/dp/B0DVM23TM1

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|

DOI: 10.15662/IJSRAT.2026.0903002

11. Shewale, Vilas. Zero Trust from the Trenches. Amazon Kindle, 2026. https://www.amazon.com/dp/B0DPVTMXC9
12. Microsoft Corporation. Windows LAPS Overview. Microsoft Learn, 2023. https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview
13. Gartner. Market Guide for Privileged Access Management. Gartner Research, 2023.
14. Plachkinova, M. and Knapp, J. Least Privilege across People, Process, and Technology: Endpoint Security Framework. Journal of Computer Information Systems, 63(5), 1153-1083, 2023. https://doi.org/10.1080/08874417.2022.2128937
15. NIST. Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology, August 2020. https://doi.org/10.6028/NIST.SP.800-207