Mitigating Insider Threats During Mergers and Acquisitions

Mergers and acquisitions (M&A) create conditions that increase the likelihood of insider threats, data exposure, and compliance risks.

This checklist provides practical steps to help organizations reduce insider risk and maintain operational stability throughout the M&A lifecycle. Use it to align stakeholders, guide planning, and strengthen oversight by ensuring visibility into user activity, access patterns, and data handling during periods of significant change.

Due Diligence

Gain an early, accurate understanding of where insider risks may emerge before integration begins.

- ☐ Identify and classify sensitive data held by both organizations.
- ☐ Examine historical activity for indications of misuse, unauthorized access, or irregular behavior patterns.
- ☐ Review past incidents involving insider threats, policy violations, or system abuse.
- ☐ Confirm data residency requirements and assess regulatory obligations for each entity.
- ☐ Assess contractor and vendor access levels. Identify privileged external identities for closer review.
- ☐ Compare logging practices, access controls, and monitoring coverage across both organizations.
- ☐ Document the security controls, processes, and systems in place to support day-one readiness.

Population Segmentation

Create focused user groups to support focused monitoring during the transition.

- ☐ Treat newly acquired users as higher risk until their normal activity patterns are better understood.
- ☐ Create watch lists for new employees, executive users, contractors, and privileged entities.
- ☐ Apply least-privilege principles as roles and responsibilities evolve.
- ☐ Validate that permissions match job functions and adjust any access inherited through previous roles.
- ☐ Monitor authentication frequency, administrative activity, and access to sensitive systems.
- ☐ Watch for sudden changes in behavior among high-risk populations.
- ☐ Label user groups to maintain consistent monitoring as the combined environment evolves.
- ☐ Include automated processes, scripts, and AI agents in monitored populations.

Technology Deployment

Introduce monitoring and visibility measures early to maintain continuity and avoid gaps.

- ☐ Prioritize onboarding of essential log and activity data sources.
- ☐ Validate existing integrations, authentication systems, and cloud connections before merging environments.
- ☐ Confirm that logs are complete, consistently formatted, and captured by both organizations.
- ☐ Tune collection and parsing practices in phases to prevent data loss during transitions.
- ☐ Conduct pre-integration threat hunting to identify any existing compromise.
- ☐ Enable detections and alerts related to M&A-specific risks, such as unusual data access or privilege escalation.
- ☐ Monitor for shifts in user behavior once systems begin to converge.
- ☐ Confirm that automated processes and AI-driven systems generate auditable activity records and that these events are captured consistently in each environment.

Data Loss Prevention (DLP)

Protect critical information while teams migrate accounts, applications, and systems.

- ☐ Activate controls for data transfers, removable media, printing, and cloud uploads.
- ☐ Encrypt data at rest and in transit, including during backups and file transfers.
- ☐ Monitor authentication attempts, file movement, and access to sensitive repositories.
- ☐ Validate that both organizations maintain consistent retention and deletion practices.
- ☐ Identify sensitive data stored in unapproved locations and remediate quickly.

Governance and Communication

Maintain alignment and accountability across both organizations during the transition.

- ☐ Develop a shared RACI model covering all security responsibilities.
- ☐ Establish secure communication channels for cross-functional coordination.
- ☐ Update policies to reflect unified expectations for access, data handling, and response procedures.
- ☐ Provide leadership with regular updates on risk posture and integration progress.
- ☐ Form a cross-functional response group to oversee monitoring, analysis, and escalations during the transition.
- ☐ Deliver targeted training on insider risk, privilege misuse, and social engineering for newly merged teams.
- ☐ Update policies to reflect expectations for the use, monitoring, and oversight of automated processes and AI tools.

Executing a Secure Integration at Speed

Protect stability while changes accelerate.

- ☐ Prioritize early ingestion of the most important data sources for visibility during onboarding.
- ☐ Define user segments and response criteria for activity related to the transition.
- ☐ Build or update response playbooks for insider risk scenarios, including account restrictions and evidence preservation.
- ☐ Run tabletop exercises that include both organizations to validate readiness.
- ☐ Track spikes in activity, changes in access patterns, and new system usage immediately after integration begins.
- ☐ Document all changes and maintain an audit trail to support transparency and oversight.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

Learn more at www.exabeam.com →

Without limitation, the Exabeam and LogRhythm names and logos, related product, service, and feature names, and related slogans are service marks, trademarks, or registered marks of Exabeam (or its affiliates) in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.

2026 Exabeam, LLC. All rights reserved.