The Role of DSPM in Mergers and Acquisitions

Normalyze®

Eliminating Data Chaos, Security and Compliance Risks through the Transition and Integration

Mergers and acquisitions can be a goldmine of opportunity—or a minefield of risk. The stakes couldn't be higher: Data mismanagement during an M&A process can lead to costly surprises, failed integrations, or even disastrous compliance breaches.

Studies show that upwards of **70% of M&A transactions fail to deliver intended value***, with poor data handling and integration cited as key contributors. Organizations often underestimate the volume and complexity of sensitive data in the acquired company, leaving them scrambling to classify, secure, or eliminate unnecessary data. This oversight can lead to ballooning costs from storing "just in case" data, increased attack surfaces, or regulatory fines due to unknown exposure.

Without the right tools, navigating this terrain is like driving blindfolded through a storm. Key challenges include:

- Insufficient visibility into valuable and sensitive data, making classification and prioritization nearly impossible
- Data access risks from legacy permissions, resulting in overprovisioned users or unauthorized exposure
- Compliance failures, with data spread across multiple platforms in inconsistent formats
- Communication gaps, leaving teams misaligned and vulnerable during a critical period

Normalyze DSPM helps businesses confidently tackle these challenges, providing the clarity and control needed to transform chaos into seamless, secure transitions—at every stage of the M&A journey.

Pre-acquisition

During the pre-acquisition phase, the acquiring company must perform thorough due diligence to evaluate and document assets, risks, and compliance. This process includes identifying valuable and sensitive data that must be secured, evaluating user access and its associated risks, and analyzing the target organization's compliance posture.

Effectively communicating these quantified risks to the acquired company in short timeframes fosters transparency, aligns priorities, and lays the groundwork for addressing security gaps and protecting critical data assets.

How Normalyze helps:

Data Discovery
The Normalyze One-Pass Scanner™ discovers and classifies valuable and sensitive data across hybrid environments, including SaaS, PaaS, public or multi-cloud, on-premises, and hybrid infrastructures, as well as LLMs and the data they are accessing.

Data Classification
With the most accurate classification of data in the market, Normalyze employs a hybrid approach of regular expressions, natural language processing and large language models that optimizes performance and minimizes resource usage.

Access Governance
Analysis of IAM roles, permissions, access logs, and database grants identifies and visualizes who has access to valuable and sensitive data, highlighting unused permissions so security teams can identify overprovisioned and high-risk users.

Risk Assessment
Detection of misconfigurations and vulnerabilities with over 800 checks, mapping attack paths to valuable and sensitive data in near real-time for quick identification of risks.

Compliance
Normalyze identifies regulatory compliance risks and pinpoints missing controls to identify exposure and misalignment with legal requirements and inconsistencies in the acquired organization.

Efficient Operations
With a fully managed platform, Normalyze scans data at scale (~1TB per hour) with minimal setup or manual intervention for fast and accurate operations and with in-place scanning for maximum safety.

Post-acquisition | Pre-integration

During the pre-acquisition phase, the acquiring company must perform thorough due diligence to evaluate and document assets, risks, and compliance. This process includes identifying valuable and sensitive data that must be secured, evaluating user access and its associated risks, and analyzing the target organization's compliance posture.

Effectively communicating these quantified risks to the acquired company in short timeframes fosters transparency, aligns priorities, and lays the groundwork for addressing security gaps and protecting critical data assets.

How Normalyze helps:

- **Risk Prioritization**
  The DataValuator™ estimates breach costs for each data store, enabling teams to prioritize security efforts on high-risk, high-impact assets based on access and exposure insights.
- **Abandoned Data**
  Normalyze identifies abandoned or stale data stores, including backups and snapshots, that should ideally be eliminated or offloaded to an archive, reducing attack surface and data storage costs.
- **Access Governance**
  The Data Risk Navigator™ and Data Access Graph™ help teams audit access privileges, communicate issues, and enforce least-privilege access while enabling timely and accurate provisioning of access to users who need it
- **LLM Security**
  Normalyze identifies and secures valuable and sensitive data in Large Language Models (LLMs) and cloud-based AI deployments, ensuring AI-generated content and custom models in platforms like ChatGPT, Microsoft Copilot, AWS Bedrock, and Azure OpenAI do not expose critical information.
- **SaaS Security**
  Teams can eliminate risky links in SaaS apps with the ability to remove public access links, organization-wide shares, and domain-wide access for Google Workspace and Microsoft 365.

Post-integration

In the post-integration phase, the focus is on aligning organizational standards, managing access privileges, and maintaining compliance. Security frameworks must be unified, legacy permissions addressed, and least-privilege access enforced to minimize risks. Critical data protection, ongoing monitoring, and regular assessments ensure compliance, while continuous reporting and proactive access management mitigate vulnerabilities and operational risks

How Normalyze helps:

- **Continuous Risk Management**
  Real-time detection of users and datastores, unauthorized access, misconfigurations, and privilege escalations enables faster responses and unified visibility across hybrid environments to prevent security incidents.
- **Remediation**
  AI-guided remediation steps for each of the risks identified make it easy for appropriate teams to take action quickly.
- **Workflow Integrations**
  Out-of-the-box integrations with third-party ticketing, notification and automation platforms help security operators collaborate with DevOps and platform engineering teams to remediate risks in a timely manner.
- **Continuous Compliance**
  Normalyze continuously monitors and assesses compliance posture against over 500 benchmarks and generates audit-ready reports with detailed views by account, resource, and compliance framework

See Normalyze in action. Request a demo or take advantage of our Data Risk Assessment to understand how our platform can make a significant difference in managing and securing your organization's most valuable data assets. **Visit www.normalyze.ai to get started**.

* source: https://fortune.com/2024/11/13/we-analyzed-40000-mergers-acquisitions-ma-deals-over-40-years-why-70-75-percent-fail-leadership-finance/