# M&A Migration Decision Checklist – A Strategic Playbook for IT Leaders

## 1. Map Workloads To Risk, Not Just To Tools

• Group workloads into high-risk (regulated or sensitive), high-visibility (email, Teams, SharePoint), and utility (low-risk archives) for the current environment.

• For each group, note the identity, security, and integration dependencies so it is clear what a delay or failure would actually mean for people and processes.

## 2. Interrogate "Native First" With Hard Constraints

• Check licensing, tenant eligibility, and configuration requirements before treating native paths as guaranteed options across all entities.

• Lay native limitations – batch and queue sizes, throttling behavior, unsupported workloads – next to actual migration windows to see whether the numbers add up.

## 3. Expose The Automation And Validation Debt

• List where mapping, policy recreation, and testing still depend on spreadsheets and manual steps, and treat those explicitly as risk items, not invisible effort.

• Agree with stakeholders on what "good enough" validation means per workload, so teams are not silently expected to deliver perfection without the time or tools.

## 4. Assemble A Deliberate Multi-Tool Migration Stack

• Combine native features with targeted third-party tools wherever there are clear gaps: identity and directory sync, Teams and collaboration, Power Platform, and compliance workloads.

• Make sure the stack includes orchestration, monitoring, and rollback options so that a single failure does not put an entire weekend, or the TSA plan, at risk.

## 5. Walk Into Steering Committees With A Decision Checklist

Instead of debating individual features, frame recommendations around a small, shared set of questions:

**• Does the chosen stack cover all in-scope workloads and policies for this deal, or are there stated exceptions everyone understands?**

**• Can it realistically deliver the needed throughput within the available migration windows and before TSA exit?**

**• Will the organization's security and compliance posture be at least as strong after migration as before, and how will that be demonstrated?**

**• Where is automation robust, and where does manual work under pressure still introduce risk that needs to be acknowledged?**

**• Which metrics – throughput, throttling incidents, failure rates, user impact – will be reviewed regularly, and what thresholds trigger early escalation?**