

M&A IT DAY -1 READINESS CHECKLIST



This is a practical guide to ensure your merger or acquisition doesn't fail on Day-1

Who this is for

This checklist is designed for **CEOs, COOs, CFOs, CIOs, CISOs**, Integration Leaders, Programme Directors, and IT/Operations teams preparing for **Day-1** (legal close / operational go-live).

What 'Day-1 Ready' means (in plain English)

On Day-1, your organisation must be able to:

- **operate safely and legally**
- **communicate and transact**
- **protect customer and company data**
- **pay people and suppliers**
- **support customers without disruption**
- **avoid preventable outages, security incidents, and reputational damage**

How to use this checklist

- Treat each item as **Green / Amber / Red**.
- Assign an **owner** and a **date**.
- Record **dependencies** and **risks**.
- If you're Red on multiple 'Critical' items, you're not Day-1 ready — you're **Day-1 exposed**.

Scoring tip: If you want a simple readiness score:

Green = 2, Amber = 1, Red = 0.

Critical items should be weighted double.

M&A IT DAY -1 READINESS CHECKLIST



1) Day-1 Decision Pack (Executive Readiness)

Goal: Everyone knows what will and won't change on Day-1 and the risks are visible.

- **Day-1 scope is defined** (what changes, what stays the same)
- **Day-1 success criteria** agreed (business outcomes + technical outcomes)
- **'No-go' criteria** agreed (what triggers delay / rollback)
- **Day-1 governance** in place (SteerCo cadence, escalation paths)
- **Named Day-1 Command Centre** (who is on-call, when, where)
- **Decision log** maintained (what was approved, by whom, and why)
- **Single integrated plan** with dependencies (business + IT + vendors)
- **Risk register** includes Day-1 risks + mitigations + owners
- **Operational readiness sign-off** is defined and scheduled

Owner: _____ **Status (G/A/R):** ___ **Due:** ___ / ___ / ___

2) Identity, Access & Security Controls (Critical)

Goal: People can access what they need and attackers can't.

- **Identity model confirmed** (separate identities vs. unified, Day-1 vs Day-2)
- **Access provisioning process in place for key roles** (IT, Finance, HR, Service Desk)
- **Privileged access controlled** (admin accounts, MFA enforced, break-glass accounts)
- **MFA enabled** for critical systems and remote access
- **Endpoint protections aligned** (EDR/AV coverage confirmed across both entities)
- **Security monitoring coverage confirmed for Day-1** (SOC/MDR handoffs clear)
- **Known vulnerabilities assessed** for acquired environment
- **Incident response** roles, contacts and playbooks aligned
- **Third-party access reviewed and restricted** (vendors, outsourced IT, partners)

Owner: _____ **Status (G/A/R):** ___ **Due:** ___ / ___ / ___

M&A IT DAY -1 READINESS CHECKLIST



3) Connectivity & Collaboration (Critical)

Goal: People can work, communicate, and support customers.

- **Network connectivity plan** agreed (interconnect, VPN, segmentation, zero trust)
- **DNS, email routing, and domain impacts** understood and tested
- **Teams/Email/Calendars** Day-1 operating model agreed (coexistence vs migration)
- **Device onboarding** process ready (laptops/mobiles, MDM policies, compliance)
- **Remote access** validated (capacity, MFA, policies, support hours)
- **Service Desk ready** (tools, scripts, knowledge base, triage categories)
- **Contact centre/customer channels** protected (IVR, CRM, customer comms)

Owner: _____ **Status (G/A/R):** ___ **Due:** ___ / ___ / ___

4) Business-Critical Applications & Transactions (Critical)

Goal: Money moves, orders flow, and customers are served.

- **Top 10 business-critical applications** identified and ranked
- **Day-1 app ownership** confirmed (support, escalation, vendor contacts)
- **Licensing rights** confirmed (transferability, compliance risk, true-up exposure)
- **Payment systems** validated (payroll, AP/AR, treasury, billing)
- **Customer-facing systems** validated (availability, support, SLAs)
- **Data feeds and integrations** mapped for Day-1 dependencies
- **Change freeze window** agreed for Day-1 (what is allowed, who approves)
- **Rollback approach** defined for any Day-1 change

Owner: _____ **Status (G/A/R):** ___ **Due:** ___ / ___ / ___

M&A IT DAY -1 READINESS CHECKLIST



5) Data, Privacy & Regulatory Exposure (Critical)

Goal: You don't inherit hidden legal, privacy, or regulatory liabilities.

- **Data classification** understood (customer data, sensitive data, regulated data)
- **Privacy impact** assessed (cross-border transfers, consent constraints, retention rules)
- **Regulatory obligations** understood (industry requirements, audit duties, reporting timelines)
- **Data access** restricted on Day-1 (least privilege)
- **Records and retention** policies defined for transitional period
- **Breach notification obligations** understood and operationalised
- **DLP / logging / monitoring** appropriate for the combined environment

Owner: _____ **Status (G/A/R):** ___ **Due:** ___ / ___ / ___

6) Infrastructure & Operational Resilience

Goal: You can withstand failures, outages, and supplier issues on the worst possible day.

- **Hosting footprint** understood (on-prem, cloud, colocation, managed services)
- **Backups** verified (coverage, restore testing evidence, RPO/RTO understood)
- **Disaster recovery** status known (plans, last test date, gaps)
- **Monitoring** covers all critical systems and alerting is actionable
- **Capacity risks** assessed (VPN load, email load, VDI load, call centre load)
- **Support hours** aligned for Day-1 and immediate post-close period
- **Major incident process** defined (war room, comms, exec updates cadence)

Owner: _____ **Status (G/A/R):** ___ **Due:** ___ / ___ / ___

M&A IT DAY -1 READINESS CHECKLIST



7) Vendor, Outsourcer & Contract Reality Check

Goal: You can actually run the environment legally and practically after close.

- **Key vendor contracts** identified (critical apps, hosting, telecoms, security tools)
- **Assignment/novation requirements** understood and initiated
- **Termination risks** identified (change-of-control clauses)
- **Service credits / SLA obligations** understood
- **Vendor runbooks** obtained (support procedures, escalation contacts, maintenance windows)
- **Tooling overlaps** identified (duplicate costs, incompatible stacks)

Owner: _____ **Status (G/A/R):** ___ **Due:** ___ /___/___

8) People, Communications & Change Adoption

Goal: Staff know what's changing, how to get help, and how to keep the business running.

- **Day-1 internal comms plan** ready (what changes, what stays, where to get help)
- **FAQ and support scripts** prepared for frontline teams
- **Training** planned for high-impact groups (Service Desk, Finance Ops, HR, Sales Ops)
- **Key person dependency risks** identified and mitigated
- **Role and responsibility changes** documented (RACI for Day-1 operations)

Owner: _____ **Status (G/A/R):** ___ **Due:** ___ /___/___

9) Cutover, Validation & Command Centre (Critical)

Goal: Day-1 is controlled, observable, and recoverable.

- **Day-1 cutover plan** is written, reviewed, and version-controlled
- **Validation checklist** exists (what must work by time X)
- **Hypercare window** defined (minimum 2–4 weeks recommended)
- **Command Centre roster** confirmed (IT, security, vendors, business ops)
- **Escalation paths** documented (technical + business + executive)
- **Status reporting cadence** agreed (internal + executive updates)
- **Rollback steps** documented and rehearsed where possible

Owner: _____ **Status (G/A/R):** ___ **Due:** ___ /___/___

M&A IT DAY -1 READINESS CHECKLIST



Day-1 Readiness Snapshot (1 page)

Use this section as your executive dashboard.

Critical Readiness (must be Green/Amber only)

- Identity & Access: **G / A / R**
- Security Monitoring & IR: **G / A / R**
- Connectivity & Collaboration: **G / A / R**
- Business-Critical Apps: **G / A / R**
- Data & Privacy: **G / A / R**
- Cutover & Command Centre: **G / A / R**

Top 5 Day-1 Risks

1. _____ (Owner: _____)
2. _____ (Owner: _____)
3. _____ (Owner: _____)
4. _____ (Owner: _____)
5. _____ (Owner: _____)

Go / No-Go recommendation (tick one)

- **GO** (managed risk)
- **GO with conditions** (conditions: _____)
- **NO-GO** (reasons: _____)

M&A IT DAY -1 READINESS CHECKLIST



Common failure patterns (what this checklist helps prevent)

- 'We closed then discovered access, licensing or security gaps'
- 'No one owned the cutover end-to-end'
- 'The Service Desk got flooded and couldn't triage'
- 'Critical integrations weren't mapped'
- 'Security monitoring didn't cover the new environment'
- 'Day-1 became Day-30 because hypercare wasn't planned'

About Bushey IT Change

Bushey IT Change helps organisations execute **Mergers and Acquisitions** with confidence by ensuring IT is ready, resilient, and controlled from Day-1.

We specialise in high-risk **integration, separation, and migration programmes** where failure is visible, costly, and reputational.

Our M&A approach combines disciplined governance, deep technical understanding, and proven delivery runbooks to protect business continuity, security, and customer experience at the moment it matters most.

From pre-close readiness and Day-1 cutover through to stabilisation and value realisation, we work alongside you to turn deal intent into operational reality, without disruption, surprises, or loss of control.

Want help turning this checklist into a Day-1 plan?

Book a 20-minute readiness call: <https://busheyitchange.com/contact-us/>

Email: contactus@busheyitchange.com | Phone: **1800 959 925**

Disclaimer

This checklist is general guidance. It does not constitute legal, regulatory, or financial advice. Always align to your organisation's obligations, contracts, and risk appetite.