IT Acquisition Systems and Infrastructure Integration Framework

1. Discovery and Assessment Phase

Inventory all IT assets

- Deploy automated discovery tools to identify all infrastructure, software, and cloud services.
- Tag assets by ownership, criticality, and operational status.
- Validate software licenses for transferability and compliance.

Map business-critical systems

- Conduct structured interviews with business and technical stakeholders to map critical business processes to IT systems.
- Document integrations, data flow, uptime requirements, and dependency mapping.

Perform data integrity, risk, and compliance assessments

- Scan datasets and map storage locations for duplicates, inconsistencies, and regulatory risks.
- Alternatives: Outsource to data audit specialists or focus on high-risk domains first.

Conduct infrastructure dependency mapping

- Map network topology, firewall configurations, DNS dependencies, and inter-system APIs.
- Trace security policies, Identity and access management configurations, and certificates across the company's environments.

Interview key stakeholders

- Engage essential application owners and IT leads.
- Record walkthroughs and screen-capture documentation for long-term knowledge transfer.

- Use standardized documentation templates for systems, integrations, and business use cases.

2. Architecture Integration Strategy

Infrastructure Integration

Cloud Consolidation

- Evaluate the cloud spend, architecture, and usage patterns.
- Align with the company's cloud operating model (e.g., single cloud vs. multi-cloud strategy).
- Prioritize workloads for migration using the 6 R's model: Rehost, Refactor, Revise, Rebuild, Replace, Retire.
- Retain multi-cloud architecture if required by latency, regulatory, or strategic concerns.

Network Integration

- Establish secure site-to-site VPNs or SD-WAN overlays to connect legacy environments.
- Align IP schema and DNS naming conventions to prevent conflict.
- Merge firewall rules and Identity and Access Management configurations while applying zero-trust principles.
- Centralize policy management.

Device and Endpoint Standardization

- Identify all IT and OT endpoints and enforce policy compliance.
- Standardize baseline configurations (e.g., OS versions, tools, and encryption).
- Integrate devices with endpoint management and patching systems.

Applications Integration

ERP/MES/SCADA

- Align on preferred platforms and identify overlapping functionality.

- Use a coexistence model where required for phased transitions (especially MES/SCADA).

Data Integration

Data Harmonization

- Define and approve master data models for each core domain.
- Map, transform, and deduplicate records.
- Establish a data governance committee for oversight and stewardship.

Data Migration

- Use Extract, Transform, and Load (ETL) tools to ensure consistent migration.
- Perform iterative testing with full reconciliation before final cutover.
- Archive non-essential legacy data for historical access.

Decommission Plans

- Identify obsolete systems, confirm regulatory retention policies, and archive securely.
- Validate decommission readiness and sunset systems in a staged process.
- Host legacy systems in read-only mode for compliance access.

3. Security, Compliance, and Risk Management

Security Hardening

- Standardize Identity and access management.
- Extend SOC (Security Operations Center) monitoring coverage and update runbooks.

Compliance Audit

- Map data lifecycle and system compliance by domain.
- Remediate identified gaps and establish continuous compliance monitoring.

Licensing and IP Review

- Review contract terms for IP ownership, license transferability, and scope restrictions.
- Perform a software bill of materials (SBOM) audit.
- Engage vendors for renegotiation and validate continued usage rights.
- Replace non-transferable licenses.

4. Key Risks and Mitigations

Risk: Incomplete Documentation

- Deploy automated discovery tools and reconstruct system knowledge via SME interviews.

Risk: Obsolete or Unsupported Systems

- Score legacy systems by business criticality and vendor support.
- Virtualize or host legacy platforms while planning phased retirement.

Risk: IP/Licensing Gaps

- Audit for IP rights and validate all license contracts.
- Sandbox usage, renegotiate licenses, or replace with compliant alternatives.

Risk: Business Disruption

- Use phased cutover and fallback procedures; simulate live test scenarios.
- Contingency: Enable war rooms and 24/7 hypercare support.

Risk: Loss of System Knowledge

- Retain SMEs on post-acquisition contracts; record walk-throughs and key configs.
- Use documentation mining tools or vendor support to recover historical knowledge.

5. Tools and Templates to Use

Integration Playbook Template: Track system-by-system migration progress, dependencies, and milestones.

RACI Matrix: Clarify accountability and responsibility across all integration tasks.

Application Redundancy Tracker: Map system overlaps and assess rationalization opportunities.

Risk Register & Mitigation Log: Maintain visibility of risks, owners, severity, and mitigations.

Master System Cutover Plan: Coordinate go-lives with pre-cutover, validation, and rollback steps.