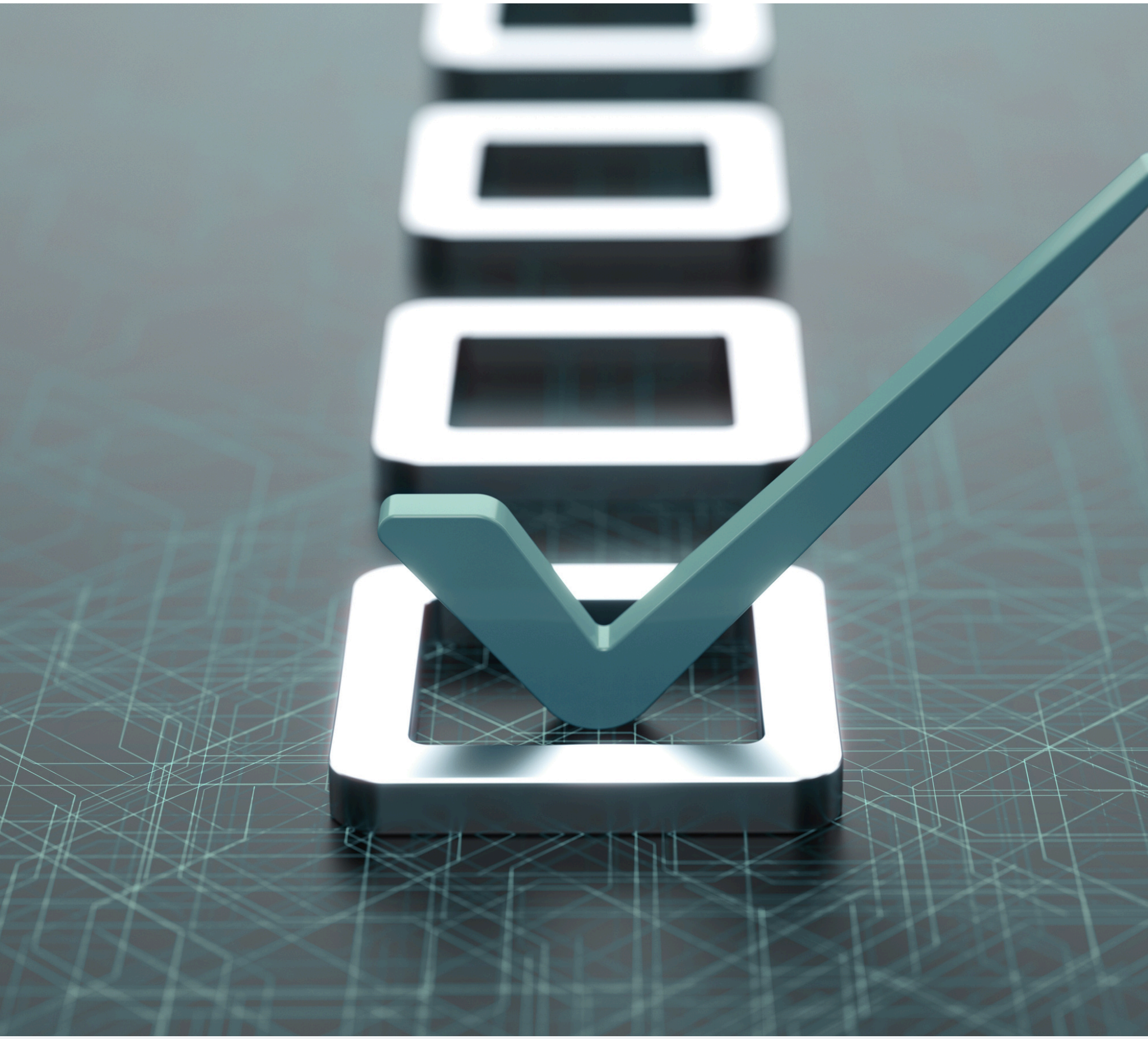
ERPFOCUS

MICROSOFT DYNAMICS 365
INTEGRATION READINESS CHECKLIST

FORMULATED BY INDEPENDENT INDUSTRY EXPERTS



Index

INTRODUCTION

For ERP teams assessing integration potential across new software projects

Use this checklist before integrating third-party, legacy, or newly acquired systems with Microsoft Dynamics 365 (CRM, Finance, Operations, or Business Central). It will help your team evaluate technical feasibility, identify risks early, and plan integrations with confidence.

1. SYSTEM OVERVIEW

Establish a basic profile of the system you're looking to integrate. Understanding its ownership, deployment model, and current usage will set the stage for deeper technical assessment.

- □ What is the name of the system or application?
- □ What is its primary function? (e.g. CRM, finance, marketing)
- □ Is it cloud-based, on-premises, or hybrid?
- □ Who owns/administers the system internally?
- □ Are there current integrations already in place?

2. INTEGRATION CAPABILITIES

Review the technical readiness of the system for integration. Native connectors, API access, and export/import functionality are critical enablers.

□ Does the system have open APIs? (REST, SOAP, etc.)

□ Are Microsoft-certified connectors available (e.g. Power Automate)?

□ Can the system import/export data in structured formats (CSV, XML, JSON)?

□ Are middleware or Integration Platform as a Service (iPaaS) tools (e.g. Zapier, MuleSoft) already in use?

□ Is developer documentation available?

3. DATA & PROCESS ALIGNMENT

Clarify the types of data that need to move between systems and how often. Map this against business processes to identify friction points early.

- □ What data needs to flow between systems? (e.g. contacts, invoices, orders)
- □ Which direction should the data flow? (one-way, two-way sync)
- □ How frequently should data be exchanged? (real-time, batch, scheduled)
- □ Are the data models compatible (fields, formats, IDs)?
- □ Is a data mapping exercise required?

4. SECURITY & COMPLIANCE

Ensure the integration meets internal and external compliance requirements. This is especially important when dealing with PII, financial data, or industry-regulated environments.

- □ Are there data protection requirements (GDPR, HIPAA, etc.)?
- □ Are authentication standards compatible? (OAuth, API keys, SSO)
- □ Are access controls in place for the integration layer?
- □ Will PII or financial data be transferred?
- □ Is data residency an issue across systems?

5. TESTING & VALIDATION

Before full deployment, validate the integration in a sandbox environment with sample data. Document everything and prepare a fallback strategy.

- □ Is a test/sandbox environment available for both systems?
- □ Are sample data sets available for testing workflows?
- □ Who is responsible for validating data integrity?
- □ What are the rollback or failure protocols?
- □ Are test cases being documented?

6. IMPLEMENTATION & OWNERSHIP

Assign responsibility for the integration. This ensures clear communication and accountability throughout the project lifecycle.

□ Who owns the integration project internally?

□ Have technical and business stakeholders been identified?

□ Is there a clear change management plan for users?

□ Are helpdesk or support teams trained on the integration?

□ Is ongoing maintenance and monitoring accounted for?

7. FINAL DECISION CRITERIA

Conclude the assessment with a go/no-go review based on technical fit, effort required, and organizational alignment.

- □ Does the integration meet business requirements?
- □ Are risks and limitations clearly documented?
- □ Is the estimated effort and cost acceptable?
- □ Is integration the right choice, or would consolidation be better?
- □ Has the integration been approved by all necessary stakeholders?