



The Intelligent Organization

Delivery Ecosystem Guide: Large and Distributed Enterprises

Designing an Accountable Enterprise Ecosystem for Delivery, Trust, Scale, and Long-Term Capability.

Table of Contents

1. The Large and Distributed Reality	12. Sovereignty, Security, Privacy, and Resilience
2. The TIO Point of View	13. Commercial Models and Procurement Implications
3. What an AI Delivery Ecosystem Includes	14. Scenario-Based Provider Guidance
4. The Internal Enterprise Core	15. How to Select and Validate Providers
5. Data, Technology, and Factory Together	16. The First 90 Days
6. Delivery Archetypes	17. Final TIO Recommendation
7. Platform Anchors and Partner Ecosystems	Appendix A. Provider Candidate Matrix
8. Provider Landscape by Role	Appendix B. Reader Validation Worksheet
9. Forward-Deployed Factory Pods	Appendix C. Public Source Notes
10. Global Engineering Under Local Control	Closing Note
11. Public-Sector and Regulated-Environment Requirements	

How to Use This Guide

This guide is written for enterprise leaders, technology executives, data leaders, transformation leaders, risk and control functions, procurement leaders, and business-unit owners in large, distributed, regulated, or public-sector organizations. Use it to clarify the internal enterprise core, provider roles, platform anchors, sourcing models, and the evidence required before scale.

Use the early sections to understand the delivery ecosystem and clarify what must remain inside the organization. Use the middle sections to compare delivery models and provider roles. Use the final sections and appendices to validate candidates, shape the first 90 days, and make a decision based on evidence.

Bottom line

Large and distributed enterprises need more than AI tools, pilots, and platform roadmaps. They need an accountable delivery ecosystem that connects internal ownership, external capability, Data, Technology, Factory, governance, security, privacy, procurement, people, and evidence into one practical system for improving real work.

Research basis and reader responsibility

This Guide is based on publicly available information available at the time of writing. Sources may include company websites, public case studies, partner directories, product documentation, press releases, public-sector guidance, public risk frameworks, marketplace listings, public job descriptions, and other publicly accessible material. TSLA has not interviewed providers, performed confidential reference checks, reviewed private proposals, tested delivery teams, or verified non-public claims. Provider examples are research candidates. Inclusion does not imply endorsement.

01

The Large and Distributed Reality

Large and distributed enterprises have scale, reach, platforms, data, governance structures, formal budgets, and specialist teams. Those assets can create serious advantage when they work together. They can also slow the organization down when every function, business unit, region, system, vendor, and risk owner moves on a different rhythm.

AI and AI and automation make this tension more visible. Employees experiment. Vendors add AI features. Business units ask for copilots, chatbots, agents, workflow tools, analytics, and automation. Technology teams face integration, security, resilience, cost, data, and support questions. Risk, legal, privacy, records, accessibility, procurement, and people leaders need to protect trust while the organization learns.

A senior technology leader in a large public-sector or regulated organization will recognize the operating reality immediately: legacy systems, critical services, procurement rules, public scrutiny, privacy duties, cybersecurity exposure, records obligations, accessibility requirements, union and workforce considerations, constrained capacity, and demand for visible value.

Signal	What it usually means
AI activity is already widespread	The organization has tools, pilots, proofs of concept, vendor demos, employee use, and platform features, but value evidence may be uneven.
Functions move at different speeds	Business units, technology, data, privacy, legal, security, procurement, finance and people teams may not share one operating rhythm.
Platform choices shape the future	Microsoft, ServiceNow, Salesforce, SAP, Oracle, Databricks, Snowflake, AWS, Google Cloud and other anchors influence architecture and sourcing options.
Data issues block scale	Promising AI Use Cases expose ownership, quality, access, lineage, integration, retention, residency and reporting gaps.
Security and privacy arrive early	AI-enabled workflows can involve sensitive data, new interfaces, agents, model outputs, logs, integrations and third-party access.
Public accountability is visible	For public-sector and regulated organizations, sourcing decisions must withstand council, audit, media, resident, employee and regulator scrutiny.
Vendor maps become confusing	The organization may need prime integrators, platform partners, boutiques, security firms, global engineering, managed services and internal teams working together.

The practical challenge

The enterprise needs a delivery ecosystem that is strong enough to deliver, disciplined enough to govern, flexible enough to adapt, and transparent enough to defend.

02 The TIO Point of View

TIO starts with the whole organization and the work that must improve. The delivery ecosystem exists to build enterprise capability, not to collect vendors or chase impressive demonstrations.

The central sourcing question is simple: What capability do we need, where should it come from, and what must remain internal so the organization becomes stronger over time?

The TIO value statement for delivery ecosystems is this: every organization should become as independent, sovereign, and capable of serving its own needs as is possible and reasonable at each point in time.

That does not require the enterprise to do everything itself. Large organizations need external specialists, platform partners, global capacity, security experts, integrators, managed services, and advisors. The discipline is to assemble them in a way that preserves ownership, understanding, control, portability, public trust, and the ability to change direction.

Principle	Meaning for a large or distributed enterprise
Capability first	Define the capability the enterprise needs before researching firms, platforms, or commercial models.
Client context first	The right provider depends on scale, complexity, risk, public accountability, current platforms, maturity and budget.
Evidence before reputation	Brand size, partner badges and conference visibility do not prove delivery fit for the client problem.
Outcomes before activity	Project completion has value only when work improves and evidence supports the next decision.
Sovereignty with trade-offs	Speed, quality, cost and specialist depth matter. Control, transparency, transfer and exit rights matter as well.
Right work, right place	Keep judgment, architecture direction, data control, product ownership, risk acceptance and Evidence Gates close to the enterprise. Source technical capacity where it can be delivered well and controlled properly.

03

What an AI Delivery Ecosystem Includes

An AI Delivery Ecosystem is the combination of internal teams, external providers, platforms, cloud services, data foundations, governance routines, security controls, workflow tools, operating support, and evidence practices used to improve real work with AI, automation, data and technology.

At this scale, the delivery ecosystem should be designed deliberately. A single vendor cannot usually cover every need with equal strength. A collection of unmanaged specialists creates fragmentation. The practical answer is usually an accountable internal core, clear provider roles, strong architecture and security controls, and Evidence Gates that force value and risk to be reviewed together.

Ecosystem part	Role
Internal enterprise core	Owns mandate, architecture direction, risk posture, data stewardship, public accountability, value decisions and operating acceptance.
Platform anchors	Provide major cloud, application, data, workflow, identity, security or AI capabilities that shape the delivery path.
Prime or orchestration partner	Coordinates delivery across workstreams, vendors, architecture, governance, testing, change and run handover when complexity requires a lead.
Specialist providers	Bring depth in data engineering, AI engineering, workflow platforms, cybersecurity, privacy, accessibility, records, managed services or global delivery.
Forward-deployed or embedded pods	Work closely with business units and users to deliver specific use cases, while documenting, transferring and supporting the solution.
Managed service partners	Operate, monitor, support and improve platforms, applications, infrastructure, security or data services after launch.
Independent assurance	Tests claims, controls, model risks, security, privacy, accessibility, value, procurement defensibility and readiness for scale.

04

The Internal Enterprise Core

External providers can provide substantial capability. The enterprise must retain the roles that make the work legitimate, coherent and sustainable. These roles should be named before provider selection begins.

Internal role	What it must own
Executive sponsor	Mandate, funding posture, enterprise trade-offs, escalation, public trust and final accountability.
CIO / CTO / technology executive	Technology direction, architecture governance, platform posture, cyber resilience, delivery feasibility and operational supportability.
Chief data or data leadership role	Data ownership, quality, access, classification, lineage, retention, analytics, reporting and data readiness.

Internal role	What it must own
Business owner / service owner	The workflow, users, customer or resident impact, operating measures, exceptions, adoption and business acceptance.
Product owner / Factory lead	AI Use Case backlog, Discovery, Design, delivery rhythm, Evidence Gates, decisions and reuse patterns.
Security and privacy leaders	Identity, access, logging, threat model, privacy impact, incident response, data handling, vendor risk and assurance.
Legal, procurement and records leaders	Contracting, public procurement, intellectual property, records, retention, auditability, public accountability and dispute protection.
People and change leaders	Manager cascade, workforce communication, adoption, skills, role impacts, labour considerations and trust.
Finance and value owner	Baseline, cost, benefit logic, budget, FinOps, evidence, benefit tracking and stop/scale decisions.

Governance rule

Leadership owns decision rights, risk posture, accountability and governance design. Data, Technology, Factory and People deploy those rules in their own work.

05

Data, Technology, and Factory Together

Most delivery failures occur at the seams. A data partner improves the data, a technology partner configures a platform, a business team redesigns work, a security team reviews risk, and a vendor demonstrates AI. The enterprise needs these efforts to operate as one delivery system.

Domain	Delivery question	What good looks like
Data	Can the organization trust, use, protect, move and learn from the data needed for this work?	Named data owners, clear definitions, access rules, quality thresholds, lineage, retention, reporting and data readiness evidence.
Technology	Can the technology foundation support the improved work safely, reliably and practically?	Architecture direction, platform ownership, integration patterns, identity, resilience, monitoring, security, support and vendor management.
Factory	Can the enterprise turn the opportunity into measured value?	Discovery, redesigned workflow, working release, adoption support, baseline, Evidence Gate and scale/stop decision.
People	Can people understand, adopt and adapt to the new way of working?	Clear change story, manager support, skills, role clarity, human review boundaries and trust routines.
Leadership	Can leaders make the choices and trade-offs required?	Mandate, priorities, decision rights, risk posture, funding, sponsor action and value review rhythm.

The delivery ecosystem should make these links visible. A provider that can build quickly but cannot work with data governance, security, architecture, change and value evidence will create risk at scale.

06

Delivery Archetypes

Large and distributed organizations can use several sourcing patterns. The right model depends on the problem, the risk, the platforms, the internal maturity and the required speed.

Archetype	Use when	Main watch-out
Internal core plus specialists	The organization has strong product, architecture and governance capacity, but needs targeted depth.	Specialists can fragment delivery when internal coordination is weak.
Prime integrator or orchestrator	The program crosses many systems, functions, regions, vendors or controls.	Prime accountability can become dependency if knowledge transfer and transparency are weak.
Platform-centric ecosystem	The work is anchored in Microsoft, ServiceNow, Salesforce, SAP, Oracle, Databricks, Snowflake, AWS or Google Cloud.	The platform roadmap can overtake the business problem if Discovery is shallow.
Federated Factory model	Business units need local speed under shared standards, Evidence Gates and reusable patterns.	Local teams can drift without a common operating model and reusable architecture.
Forward-deployed Factory pods	A priority use case needs close collaboration between business users, AI/data engineers and product owners.	Embedded teams can leave behind technical debt if support and transfer are weak.
Managed service model	The organization needs ongoing operation, monitoring, cybersecurity, cloud, data or platform support.	Managed services can hide cost, lock-in or weak improvement unless service measures are clear.
Global engineering under local control	The organization needs scale, speed or specialist development capacity after architecture and acceptance criteria are clear.	Control, security, data access, code ownership and knowledge transfer must be explicit.
Independent assurance	Public accountability, safety, cyber, privacy, model risk, accessibility or critical services require external challenge.	Late assurance creates rework. Bring it into design and Evidence Gates.

07

Platform Anchors and Partner Ecosystems

Platform anchors matter because they shape architecture, procurement, data flow, user experience, operating support, security and long-term cost. In large enterprises, the platform decision and the provider decision are often connected, but they are not the same decision.

Platform anchor	Typical role in the ecosystem	Reader validation focus
Microsoft	Microsoft 365, Azure, Entra, Defender, Power Platform, Dynamics, Fabric, Copilot and partner ecosystem.	Tenant design, identity, records, privacy, data boundaries, agent governance, licensing, support and change management.
AWS	Cloud infrastructure, AI services, data, marketplace, partner network and modernization patterns.	Cloud architecture, data residency, security controls, cost management, managed service model and procurement path.
Google Cloud	Cloud, Gemini, data analytics, security, AI and partner ecosystem.	Public-sector fit, integration with existing stack, data handling, identity, security and partner validation.
ServiceNow	AI platform for service management, workflow automation, enterprise service and case management.	Process redesign, configuration standards, integration, licensing, citizen or employee service impact and support.
Salesforce	CRM, service, marketing, data cloud, AI and industry solutions.	Data model, integration, workflow, public-sector use, licensing, records and platform governance.
SAP and Oracle	Enterprise resource planning, finance, HR, supply chain, asset and database foundations with AI features.	Process ownership, data definitions, modernization scope, change impact, cost and integration dependencies.
Databricks and Snowflake	Data and AI foundations, analytics, governance, data products, AI applications and partner ecosystems.	Data ownership, lineage, access, residency, integration, cost controls, operating support and skills transfer.
Palantir and related operational AI platforms	Operational data integration, workflows, AI use cases and embedded delivery patterns.	Procurement fit, data governance, explainability, platform dependence, transfer, public accountability and exit rights.

Platform discipline

Choose platforms through enterprise direction, architecture, security, data readiness, user need and evidence. Avoid letting a vendor demo become the strategy.

08

Provider Landscape by Role

The large and distributed provider landscape is broad. A single ranked list would be misleading. Provider categories matter more than provider names at the start.

Provider role	Examples to investigate	Best use
Enterprise prime and systems integration	CGI, IBM Consulting; Kyndryl, Deloitte, Accenture, Capgemini, NTT DATA, Cognizant	Large-scale orchestration, systems integration, public-sector modernization, managed services and platform programs.
Canadian technology integrators and MSPs	CDW Canada, Compugen, Long View Systems, Softchoice, a World Wide Technology company, TELUS Business, Bell Business Markets	Canadian proximity, workplace, cloud, security, procurement, managed services and platform support.
Business-facing product and AI delivery firms	Slalom, Thoughtworks, TELUS Digital, EPAM, AltaML, AOT Technologies, Adastra	Embedded delivery, product, AI, data, modernization and business-aligned use case work.
Platform specialist ecosystem	Microsoft, AWS, Google Cloud, ServiceNow, Salesforce, SAP, Oracle, Databricks, Snowflake	When the delivery path is anchored in a major cloud, workflow, application or data platform.
Global engineering partners	EPAM, Globant, Endava, SoftServe, N-iX, ELEKS, Intellias, CI&T, BairesDev, Nagarro	Engineering capacity, modernization, integrations, testing, data engineering and product build under local control.
Cybersecurity and assurance specialists	Mandiant, CrowdStrike Services, Palo Alto Unit 42, Fortinet, eSentire, ISA Cybersecurity, Kroll, NCC Group	AI/cloud security, incident response, threat modeling, red teaming, privacy support and independent testing.
Advisory and assurance firms	Deloitte, EY, PwC, KPMG, McKinsey, BCG, Gartner and specialist boutiques	Governance, operating model, risk, assurance, portfolio design, sourcing strategy and board-level perspective.

These examples are public-evidence candidates. The reader should validate current fit, delivery team, pricing, geographic model, subcontracting, references and contractual terms before acting.

09

Forward-Deployed Factory Pods

Forward-deployed delivery is useful when the problem cannot be solved from a distance. The team works close to the business unit, workflow, users, data, systems and decision owners. The pattern can be powerful for AI Use Cases because design, data, build, testing, adoption and measurement must happen together.

For large and distributed enterprises, the better pattern is usually a Forward-Deployed Factory Pod: a small, cross-functional team that combines product ownership, workflow design, AI or automation engineering, data/integration capability, technology architecture, security review, user adoption and measurement.

Pod role	What it contributes
Business product owner	Owns the service problem, user needs, workflow and acceptance criteria.
Factory lead	Runs Discovery, Design, delivery rhythm, baseline, Evidence Gate and scale decision.
AI / automation engineer	Builds or configures the AI, agent, automation or application component.
Data / integration specialist	Connects data, systems, lineage, quality, access and reporting.
Technology architect	Tests fit with enterprise architecture, security, platform and support standards.
Security / privacy reviewer	Reviews data flow, threat model, privacy, logs, access, retention and vendor exposure.
Change and adoption lead	Helps users, managers and service owners adopt the improved workflow.
Value owner	Tracks baseline, value evidence, cost, adoption, risk and Evidence Gate decisions.

Transfer test

A forward-deployed team has done its job only when the organization can understand, operate, support, change, pause, recover, recompute or retire the solution.

10

Global Engineering Under Local Control

Global engineering can be valuable for large organizations that need speed, specialist depth and build capacity. Eastern Europe, Latin America, India, the Philippines and other delivery markets can provide strong engineering, data, QA, integration and platform skills. The delivery geography should serve the capability model, not replace it.

The safest pattern keeps business design, architecture direction, data control, security, privacy, product ownership, procurement, public accountability and acceptance close to the enterprise. Technical work can be sourced globally when the work is well specified, securely managed, and supported by clear ownership and documentation.

Delivery location pattern	Potential strength	Control requirement
Canada / local proximity	Business context, public-sector familiarity, workshops, governance, security, change, stakeholder alignment and accountability.	Validate depth, cost, specific team quality and ability to deliver beyond advisory.
Nearshore Americas	Time-zone alignment, agile collaboration, software engineering, QA, product and data delivery.	Protect data access, code ownership, architecture, security, IP and acceptance criteria.
Eastern Europe	Strong engineering depth, product development, data engineering, AI engineering, cloud and QA.	Manage time-zone overlap, geopolitical exposure, data access and knowledge transfer.
India and Philippines	Large-scale technology services, managed services, application support, testing, data work and platform delivery.	Control communication, handover, security, service quality, turnover and escalation.

Delivery location pattern	Potential strength	Control requirement
Hybrid global pod	Combination of local leadership, nearshore development, offshore support and specialist resources.	Clarify who owns architecture, security, product decisions, documentation and operations.

Requirement	Evolve the Current Operation	Establish the New Operation Beside It
Partner role	Work within the existing operation, progressively improve work, data, systems, controls, skills, and operating ownership.	Build a complete bounded target operation with a clear interface to the current one, then support proof, work routing, authority transfer, stabilization, and legacy outcome.
Control focus	Protect current-state integrity, service continuity, portable improvements, and client ownership.	Define old/new synchronization, authoritative truth, transaction commit, reconciliation, recovery, support, transfer, and retirement or deliberate coexistence.
Enterprise Autonomy test	Provider evidence question	
Mandate and control	Does the client retain priorities, architecture direction, decision rights, value decisions, Evidence Gates, and residual-risk accountability?	
Knowledge and data	Can the provider use the required Enterprise Knowledge and State without uncontrolled copies, unclear provenance, or provider-held dependency?	
Identity and authority	Can people, agents, models, tools, services, and devices be separately identified, limited, monitored, and revoked?	
Action and transaction	Are consequential changes validated and committed through controlled authoritative services?	
Trust and recovery	Can the client observe, stop, investigate, reconcile, recover, and continue service?	
Portability and exit	Can the client replace a model, platform, or provider without losing the operating capability?	
Capability transfer	Will the client understand and operate what has been built, or will essential knowledge remain outside?	

11

Public-Sector and Regulated-Environment Requirements

Public-sector delivery carries obligations that go beyond ordinary vendor fit. A provider that looks impressive in a private-sector demo may still be unsuitable for a public-sector or regulated environment if it cannot support procurement defensibility, privacy, accessibility, records, security, explainability, service continuity and public accountability.

Requirement	Practical test
Public accountability	Could the sourcing decision be explained to council, an auditor, the media, employees or residents without embarrassment?

Requirement	Practical test
Privacy and data residency	Can the provider explain where data is stored, processed, accessed, logged, retained, deleted and protected?
Security and resilience	Can the provider work within identity, logging, monitoring, incident response, vulnerability management and continuity expectations?
Procurement defensibility	Can the sourcing path be fair, transparent, value-based, compliant and easy to audit?
Accessibility and inclusion	Can the solution meet accessibility, language, equity, inclusion and service-user needs?
Records and transparency	Can the solution preserve records, explanations, audit trails, decision logs and disclosure obligations?
Architecture and integration	Can the provider work with legacy systems, current platforms, identity, records, data stores and integration patterns?
Evidence of value	Can the provider work with baselines, adoption measures, Evidence Gates and value tracking?

Public-sector and regulated-environment lens

A public-sector or regulated-environment AI delivery ecosystem must protect service, trust, accountability and continuity while improving the work. Speed matters. Defensibility matters too.

12

Sovereignty, Security, Privacy, and Resilience

Sovereignty is practical control. The enterprise needs enough understanding and rights to make decisions, operate, monitor, pause, change, recover, recompetete, replace or exit a solution. This applies to data, technology, operations, talent and business ownership.

Sovereignty dimension	Question leaders should ask
Business sovereignty	Do we retain mandate, priorities, process ownership, value decisions and Evidence Gates?
Data sovereignty	Can we control where data is stored, processed, accessed, transferred, retained and deleted?
Technology sovereignty	Do we own or control accounts, environments, credentials, configuration, code, architecture knowledge and transition rights?
Operational sovereignty	Can we operate, monitor, support, pause, recover and change the solution?
Capability sovereignty	Are we becoming more capable, or more dependent on one provider?
Talent sovereignty	Can we access global expertise without allowing critical knowledge to live only outside the organization?

Security and privacy should be designed into the work. For generative AI and agentic systems, validation should cover prompt injection, insecure output handling, sensitive information disclosure, supply chain exposure, excessive agency, model use, logs, training data, human review, and incident response.

13

Commercial Models and Procurement Implications

Commercial structure shapes behavior. Large and distributed enterprises should match commercial model to uncertainty, control needs, funding rules, procurement path and operational risk.

Commercial model	Best use	Watch-out
Advisory / assessment	Strategy, readiness, operating model, sourcing design, risk and roadmap.	Can become shelfware if it does not lead to decisions and funded work.
Project delivery	Defined scope, clear outputs, controlled timeline, known acceptance criteria.	Weak fit for uncertain discovery or evolving AI Use Cases unless stage gates are clear.
Product / pod model	Iterative use case development, workflow redesign and agile delivery.	Requires strong product ownership and backlog discipline.
Managed service	Ongoing platform, security, data, cloud, application or workflow operations.	Can hide cost and dependency unless service levels, exit and improvement measures are explicit.

Commercial model	Best use	Watch-out
Staff augmentation	Temporary capacity under strong internal direction.	Creates weak accountability when the organization lacks product and architecture leadership.
Build-operate-transfer	Capability establishment with an explicit path to handover.	Transfer can become performative unless documentation, training, ownership and support are measured.
Outcome-linked	Narrow situations where value is measurable, attributable and contractually clear.	Difficult in public sector and complex systems. Can distort behavior if measures are weak.
Enterprise agreement / platform consumption	Large platform or cloud consumption with partner ecosystem support.	Needs FinOps, usage controls, security, data governance and procurement transparency.

Planning budgets vary widely. A focused discovery and readiness phase may be measured in hundreds of thousands of dollars. A production AI Use Case tied to integration, security, adoption and support can move into the low millions. Platform, data foundation and enterprise modernization programs can move far higher. Treat these as planning signals only. Validate through the procurement process.

14

Scenario-Based Provider Guidance

The provider landscape should be read by scenario. Different problems require different delivery models. The table below identifies candidate sets for reader validation. It is a starting point for sourcing design, not a ranking.

Scenario	When it fits	Candidate examples	Validation focus
Enterprise AI and technology prime	Use when coordination risk, procurement complexity, public accountability, and cross-functional integration require one accountable lead.	CGI, IBM Consulting; Kyndryl, Deloitte, Accenture, Capgemini, NTT DATA, Slalom	Validate actual team, public-sector references, subcontracting, data handling, transfer, managed service model, and exit rights.
Canadian public-sector proximity	Use when Canadian presence, public-sector familiarity, procurement channels, service continuity, and proximity matter.	CGI, CDW Canada, Compugen, Long View Systems, Softchoice, a World Wide Technology company, TELUS Digital, Bell Business Markets, TELUS Business	Validate AI and data delivery depth separately from licensing, resale, and managed infrastructure capability.
Microsoft-heavy enterprise or public-sector stack	Use when the environment is built around Microsoft 365, Azure, Entra, Defender, Power Platform, Dynamics, Fabric, or Copilot.	Microsoft, Avanade, Softchoice, a World Wide Technology company, Long View Systems, CDW Canada, Compugen, CGI, Accenture, Deloitte	Validate tenant design, records, privacy, access, agent governance, Copilot readiness, and ongoing support.
Workflow and service transformation	Use when the business problem is case management, internal service, citizen or customer service, IT service, HR service, field work, intake, or workflow automation.	ServiceNow, Salesforce, Microsoft, Accenture, Deloitte, CGI, IBM, Capgemini, Slalom	Start with work redesign and value measures. Workflow platforms can scale poor handoffs when Discovery and Design are weak.

Scenario	When it fits	Candidate examples	Validation focus
Data and AI foundation	Use when priority use cases expose weak data ownership, quality, access, flow, reporting, analytics, and AI readiness.	Microsoft, AWS, Google Cloud, Databricks, Snowflake, IBM, CGI, Accenture, Adastra, Slalom	Validate data residency, ownership, lineage, governance, operating model, cost controls, and integration with existing platforms.
ERP and enterprise application modernization	Use when AI and automation depend on SAP, Oracle, Microsoft Dynamics, Salesforce, finance, HR, asset, supply chain, permitting, or other core systems.	SAP, Oracle, Microsoft, Salesforce, Deloitte, Accenture, IBM, NTT DATA, Capgemini, Cognizant	Treat the work as enterprise transformation. Keep process ownership, controls, data definitions, and acceptance criteria internal.
Embedded AI Use Case delivery	Use when selected priority use cases need rapid design and build with close business involvement.	Slalom, Thoughtworks, EPAM, TELUS Digital, Databricks, Palantir, Accenture, CGI	Validate transfer, documentation, support, technical debt, security review, human review, and what happens after the pod leaves.
Global engineering capacity	Use for application modernization, data engineering, integration, testing, platform build, and product engineering once business design and architecture are clear.	EPAM, Globant, Endava, SoftServe, N-iX, ELEKS, Intellias, CI&T, BairesDev, Nagarro	Keep architecture, data access, code ownership, security, acceptance, product ownership, and vendor management close to the client.
Cybersecurity and independent assurance	Use when AI, cloud, integration, agents, automation, identity, privacy, or critical service risk need specialist review.	Mandiant / Google Cloud, CrowdStrike Services, Palo Alto Unit 42, Fortinet, eSentire, ISA Cybersecurity, Kroll, NCC Group, Deloitte, EY, PwC, KPMG	Involve assurance early enough to improve design. Late-stage review often becomes expensive rework.

15

How to Select and Validate Providers

The selection process should test role fit before firm preference. Decide whether the need is advisory, prime integration, platform implementation, AI engineering, data foundation, workflow redesign, managed service, global engineering or independent assurance. Then validate providers against the role.

Validation area	Evidence to request
Current facts	Current ownership, legal entity, Canadian presence, delivery locations, subcontractors, public-sector references and insurance.
Team quality	Named proposed team, resumes, certifications, comparable work, delivery leadership and escalation path.
Data handling	Data flow, residency, access, logging, retention, deletion, model use, training use and third-party exposure.
Security	Threat model, identity, access, secrets, vulnerability management, penetration testing, incident response and audit evidence.
Architecture	Current-state assumptions, target pattern, integrations, APIs, code ownership, configuration, environments and operational handover.
Public-sector fit	Procurement experience, accessibility, privacy, records, transparency, resident impact and public accountability.
Commercial fit	Pricing, change control, service levels, exit rights, intellectual property, warranties, liability and transition terms.
Value evidence	Baseline, adoption measures, benefits logic, Evidence Gates, stop/scale criteria and reporting cadence.
Transfer	Documentation, runbooks, training, support, internal capability build and exit plan.

Warning signs

Be careful when a provider leads with a demo before understanding the work, treats partner badges as proof, cannot explain data flow, avoids transfer, hides subcontracting, resists documentation, or asks for platform commitment before Discovery and Design are complete.

16 The First 90 Days

The first 90 days should build decision quality before the enterprise commits to large delivery. The goal is to identify a small number of high-value opportunities, design the sourcing model, validate public evidence, and prepare the first delivery wave.

Timing	Leadership question	Practical outputs
Days 0 to 15	What mandate, risk posture and accountability will govern this work?	Executive mandate, sponsor map, decision rights, initial CTO Test and public-evidence standard.
Days 15 to 30	Where is the work already under strain and which AI Use Cases matter?	Opportunity scan, current-state workflow map, system/data constraints, candidate backlog.
Days 30 to 45	Which use cases deserve Discovery and which should wait?	Value hypotheses, readiness screen, risk screen, data and technology dependency map.
Days 45 to 60	What delivery ecosystem model fits the work?	Sourcing model, internal core roles, provider role map, platform assumptions, validation plan.
Days 60 to 75	Which candidates should enter public-evidence validation?	Scenario shortlist, evidence log, provider questions, procurement path and security/privacy review triggers.
Days 75 to 90	What will we launch, and how will we prove whether it worked?	First delivery wave charter, Evidence Gate, baseline, adoption plan, value measures and next-quarter decision calendar.

17

Final TIO Recommendation

Large and distributed enterprises should treat AI delivery as ecosystem design. The work is too important and too exposed to be left to isolated pilots, single-platform enthusiasm, local experimentation or vendor-led strategy.

Start with the mandate. Name the internal enterprise core. Choose a small first portfolio. Separate platform decisions from provider decisions. Use scenario-based sourcing. Keep public accountability, security, privacy, records, accessibility and resilience in the design from the beginning. Require evidence before scale.

The strongest delivery ecosystem will help the enterprise improve real work while becoming more capable over time. That is the point. The organization should not simply buy capacity. It should build the ability to choose, govern, deliver, measure, learn and adapt in the age of AI and AI and automation.

The simple move

Build the ecosystem around capability, not vendor preference. Keep ownership close. Source expertise deliberately. Validate public claims. Use Evidence Gates. Scale only what proves value and trust.

A

Provider Candidate Matrix

The matrix below is based on public evidence and should be treated as a research starting point. It is not a ranking. It is not an endorsement. Readers must validate facts and fit directly.

Provider	Public-evidence role	Confidence	Possible fit
CGI	Canadian and global prime, systems integration, managed services, AI, data, public-sector delivery	High public evidence	Prime delivery, Canadian public-sector proximity, managed services, data and AI, enterprise modernization
IBM Consulting; Kyndryl	AI, hybrid cloud, data, enterprise modernization, managed infrastructure and operations	High public evidence	Complex enterprise programs, regulated environments, hybrid operations, AI governance and infrastructure
Deloitte	Advisory, technology transformation, cyber, data, AI, enterprise platforms, public sector	High public evidence	Strategy-to-delivery support, governance, assurance, platforms, large transformation
Accenture	AI, data, platforms, cloud, managed services, workforce and enterprise transformation	High public evidence	Large-scale delivery, global resources, platform programs, managed services, industrialized AI
Capgemini	Technology transformation, cloud, data, AI, systems integration, managed services	Medium public evidence	Large programs, global delivery, platform integration, data and AI transformation
NTT DATA	Systems integration, cloud, data, AI, application modernization, managed services	Medium public evidence	Large enterprise programs, managed technology services, modernization
Slalom	Business and technology consulting, cloud, data, AI, product and embedded delivery	High public evidence	Embedded teams, business-facing AI, data, cloud and workflow work
Thoughtworks	Digital engineering, product, data, platform and engineering culture	High public evidence	Product-led delivery, modernization, engineering enablement, agile delivery
EPAM	Global engineering, AI, data, platform and product engineering	High public evidence	Global engineering under local control, modernization, AI and data engineering
TELUS Digital	Digital product, AI data, automation, customer experience and managed digital delivery	Medium public evidence	Embedded delivery, data for AI, digital operations, experience and automation
CDW Canada	Technology products, cloud, security, professional and managed services	High public evidence	Canadian channel, platform implementation, managed services, public-sector procurement support

Provider	Public-evidence role	Confidence	Possible fit
Compugen	Canadian IT solutions, managed services, cloud, workplace, security and professional services	Medium public evidence	Canadian technology foundation, workplace, device, cloud, managed services
Long View Systems	Canadian IT, cloud, workplace, cybersecurity and managed services	High public evidence	Technology operations, Microsoft-oriented foundation, cloud and managed services
Softchoice, a World Wide Technology company	Technology solutions, cloud, software, lifecycle and enterprise IT advisory	High public evidence	Platform sourcing, licensing, cloud, security, enterprise technology support
Microsoft	Platform anchor: M365, Azure, Copilot, Power Platform, Dynamics, Fabric, Entra, Defender	High public evidence	Platform and partner ecosystem, AI productivity, cloud, identity, data, security
AWS	Platform anchor: cloud, data, AI, marketplace and partner ecosystem	High public evidence	Cloud, AI, modernization, data platforms, marketplace and partner ecosystem
Google Cloud	Platform anchor: cloud, Gemini, data, AI, analytics, security and partner ecosystem	High public evidence	AI, data, analytics, cloud modernization, security and partner ecosystem
ServiceNow	Platform anchor: AI platform for service management, workflow and enterprise service operations	High public evidence	Workflow, service management, case management, automation and partner ecosystem
Salesforce	CRM, service, marketing, data cloud, AI and partner ecosystem	High public evidence	Citizen, customer, case, service and CRM-centered transformation
SAP	ERP and enterprise application platform with AI and partner ecosystem	High public evidence	ERP modernization, finance, supply chain, HR, procurement, asset and enterprise process work
Oracle	Cloud, applications, database, AI infrastructure and enterprise AI	High public evidence	ERP, database, cloud, AI infrastructure and enterprise applications
Databricks	Data and AI platform with partner ecosystem and lakehouse architecture	High public evidence	Data, AI, lakehouse, governed analytics, AI applications and data engineering
Snowflake	Data cloud, AI services, governed data, analytics and marketplace	High public evidence	Data sharing, analytics, governance, AI services and enterprise data products
Palantir	Operational AI and data platform, forward-deployed model, government and enterprise positioning	Medium public evidence	Operational AI, complex data integration, mission workflows, public-sector scenarios
Adastra	Data, AI, cloud and analytics specialist with Canadian and global footprint	High public evidence	Data foundation, governance, analytics, cloud and AI platform work
AltaML	Canadian applied AI and vertical AI specialist	High public evidence	Applied AI discovery, opportunity validation, industry use cases and AI delivery
AOT Technologies	Open technology, workflow, digital services and regulated-sector delivery	Medium public evidence	Open standards, workflow, public-sector-adjacent and regulated delivery

Provider	Public-evidence role	Confidence	Possible fit
Mandiant / Google Cloud	Cybersecurity consulting, incident response, threat intelligence and cloud security	High public evidence	Security assurance, AI/cloud security, incident response and resilience
CrowdStrike Services	Cybersecurity services, incident response, threat hunting and managed security	High public evidence	Incident response, endpoint and identity threat assurance, AI service exposure review
Palo Alto Unit 42	Cybersecurity consulting, incident response, threat intelligence and cloud security	High public evidence	Security assurance, incident response, cloud and AI-related security testing
eSentire	Canadian-founded managed detection and response and cybersecurity services	Medium public evidence	Managed detection, response and security operations support
Kroll / NCC Group	Security testing, incident response, digital risk and assurance	Medium public evidence	Independent security testing, privacy, cyber review and assurance

B

Reader Validation Worksheet

Step	Question to answer
1. Define the problem	What workflow, service, decision, process, user need or operating constraint are we trying to improve?
2. Confirm ownership	Who owns the business outcome, data, technology, security, privacy, procurement, adoption and value decision?
3. Classify the delivery need	Do we need advisory, architecture, platform work, data work, AI engineering, workflow redesign, managed service, global engineering or assurance?
4. Choose the sourcing model	Internal core plus specialists, prime integrator, platform-centric, embedded pod, managed service, global engineering, or hybrid?
5. Validate public evidence	Which public claims are supported by official sources, public case examples, partner directories or observable delivery evidence?
6. Request direct evidence	What references, team resumes, architecture, security, pricing, delivery plan, transfer plan and contract terms must the provider supply?
7. Test security and privacy	Where will data go, who can access it, what is logged, what is retained, what is deleted, and how will incidents be handled?
8. Test public-sector fit	Can the provider support accessibility, records, procurement, transparency, audit, public accountability and service continuity?
9. Confirm transfer and exit	What will we own, understand, operate, monitor, change, recover, recompute or replace after delivery?
10. Set the Evidence Gate	What baseline, adoption, value, risk, cost and trust evidence will decide whether to continue, scale, redesign or stop?

C

Public Source Notes

These sources informed the research frame and source streams for this Guide. They do not validate provider suitability for any specific client. Readers should review current source pages directly before acting.

Source stream	How it was used	Public URL
NIST AI Risk Management Framework	Voluntary framework for incorporating trustworthiness into AI design, development, use and evaluation. NIST notes that AI RMF 1.0 is under revision and released a Generative AI Profile in 2024.	https://www.nist.gov/itl/ai-risk-management-framework
NIST AI 600-1 Generative AI Profile	Profile for identifying risks posed by generative AI and suggested actions for generative AI risk management.	https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf
Government of Canada Algorithmic Impact Assessment	Mandatory risk assessment tool supporting the Treasury Board Directive on Automated Decision-Making. It uses risk and mitigation questions to determine impact level.	https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html
OWASP GenAI Security Project and Top 10 for LLM Applications	Open-source security guidance for LLM and generative AI risks, including prompt injection, insecure output handling, supply chain issues and sensitive information disclosure.	https://owasp.org/www-project-top-10-for-large-language-model-applications/
Microsoft AI Cloud Partner Program	Official partner ecosystem and partner-finder source for Microsoft AI, cloud, business applications, security and marketplace relationships.	https://partner.microsoft.com/en-us/partnership
AWS Partner Network	Official partner ecosystem for AWS software, consulting, managed services, marketplace and partner success stories.	https://aws.amazon.com/partners/
Google Cloud Partner Network	Official partner ecosystem with tiers, competencies, solution areas and partner finder.	https://cloud.google.com/partners
ServiceNow Partner Program	Official partner program for reseller, service provider, consulting and implementation, and build partners for the ServiceNow AI Platform.	https://www.servicenow.com/partners.html
Databricks Partners	Official partner ecosystem and partner-finder source for data and AI delivery.	https://www.databricks.com/partners
Snowflake AI	Official product page for AI and governed data capabilities in the Snowflake Data Cloud.	https://www.snowflake.com/en/product/ai/
Oracle AI	Official source for Oracle AI services, generative AI, cloud applications and OCI AI infrastructure.	https://www.oracle.com/artificial-intelligence/

Source stream	How it was used	Public URL
CGI Canada AI	Official CGI Canada page on AI services, data governance, Canadian AI practice and public-sector relevance.	https://www.cgi.com/canada/en-ca/artificial-intelligence
IBM Consulting AI	Official IBM Consulting page for AI services and consulting.	https://www.ibm.com/consulting/artificial-intelligence
Accenture AI and Data	Official Accenture AI and data services page.	https://www.accenture.com/us-en/services/ai-data
TELUS Digital Data for AI Training	Official TELUS Digital page for data for AI training and related AI delivery positioning.	https://www.telusdigital.com/solutions/data-for-ai-training
Kyndryl AI Services	Official Kyndryl page for AI and data services, including AI-native infrastructure and agentic AI.	https://www.kyndryl.com/ca/en/artificial-intelligence
World Wide Technology and Softchoice	Official WWT announcement confirming completion of the Softchoice acquisition and the combined software, cloud, cybersecurity, and AI portfolio.	https://www.wwt.com/press-release/world-wide-technology-announces-completion-of-softchoice-acquisition-expanding-software-cloud-cybersecurity-and-ai-capabilities

END**Closing Note**

This Guide should help a large or distributed enterprise ask better sourcing questions. The right answer will depend on the organization, its existing stack, its public obligations, its maturity, its risk posture, its budget and the work it chooses to improve first.