



Everest Group PEAK Matrix[®] for IT Security Service Provider 2022 – Europe

Focus on Wipro
September 2022



Background of the research

The demand for IT security services in Europe is growing in terms of technological capabilities and localized presence of cybersecurity talent. Enterprises are grappling with cybersecurity challenges arising from the new-age security threats. Coupled with the rising trend of tying executive evaluation with cyber risk management, cybersecurity has started to become a boardroom mandate rather than just being a CISO-led effort. European enterprises are looking for service providers that can offer geographically nuanced security services, especially in areas such as data security & privacy, verticalized SOCs, converged IT/OT security services, and regulatory assessment services, to make sure that enterprises are not just adhering to ever evolving EU regulations but also the localized data privacy laws.

IT security service providers too have started to tap into these demand themes and are building capabilities to deliver the geographically contextualized services. Additionally, there is a strong push from service providers to proliferate their cybersecurity consulting capabilities in an effort to be seen as a holistic security partner that can deliver end-to-end security services.

In this research, we present an assessment and detailed profiles of 28 IT service providers for the IT security capabilities in Europe region featured on the [IT Security Services PEAK Matrix® Assessment 2022 – Europe](#). The assessment is based on Everest Group's annual RFI process for calendar year 2022, interactions with leading IT security service providers, client reference checks, and an ongoing analysis of the IT security services market.

The full report includes the profiles of the following 28 leading IT security service providers featured on the IT Security Services PEAK Matrix – Europe:

- **Leaders:** Accenture, Atos, HCL Technologies, IBM, TCS, and Wipro
- **Major Contenders:** Capgemini, Cognizant, Deloitte, DXC Technology, EY, Infosys, KPMG, Kyndryl, LTI, Microland, NTT DATA, Orange Cyberdefense, PwC, Stefanini, Tata Communications, Tech Mahindra, T-Systems, and Zensar
- **Aspirants:** Happiest Minds, ITC Secure, Mindtree, and Yash Technologies

Scope of this report



Geography
Europe



Providers
28



Services
IT Security Services

IT security services PEAK Matrix® – Europe characteristics

Leaders:

Accenture, Atos, HCL Technologies, IBM, TCS, and Wipro

- Leaders have gained significant mindshare among enterprise clients due to the depth and breadth of their IT security services portfolio and on-ground presence in the European geography. These players have strong focus on next-generation security themes such as data security & privacy, regulatory assessments, verticalized SOCs, IT/OT convergence, OT security, zero trust, security-embedded portfolio, SASE, and IAM
- They have a highly balanced portfolio and continue to keep pace with market dynamics through continued investments in next-generation security solutions and services capability development (internal IP/tools, partnerships, etc.)

Major Contenders:

Capgemini, Cognizant, Deloitte, DXC Technology, EY, Infosys, KPMG, Kyndryl, LTI, Microland, NTT DATA, Orange Cyberdefense, PwC, Stefanini, Tata Communications, Tech Mahindra, T-Systems, and Zensar

- These players have built meaningful capabilities to deliver IT security services. However, their service portfolios are not as balanced and comprehensive as those of Leaders (either in terms of coverage across IT security service segments, delivery mix, service type, or all)
- All these providers are making continued investments in developing internal IP and tools, as well as expanding their service and technology partner ecosystem to plug their capability gaps. This helps position them as strong challengers to Leaders in this space

Aspirants:

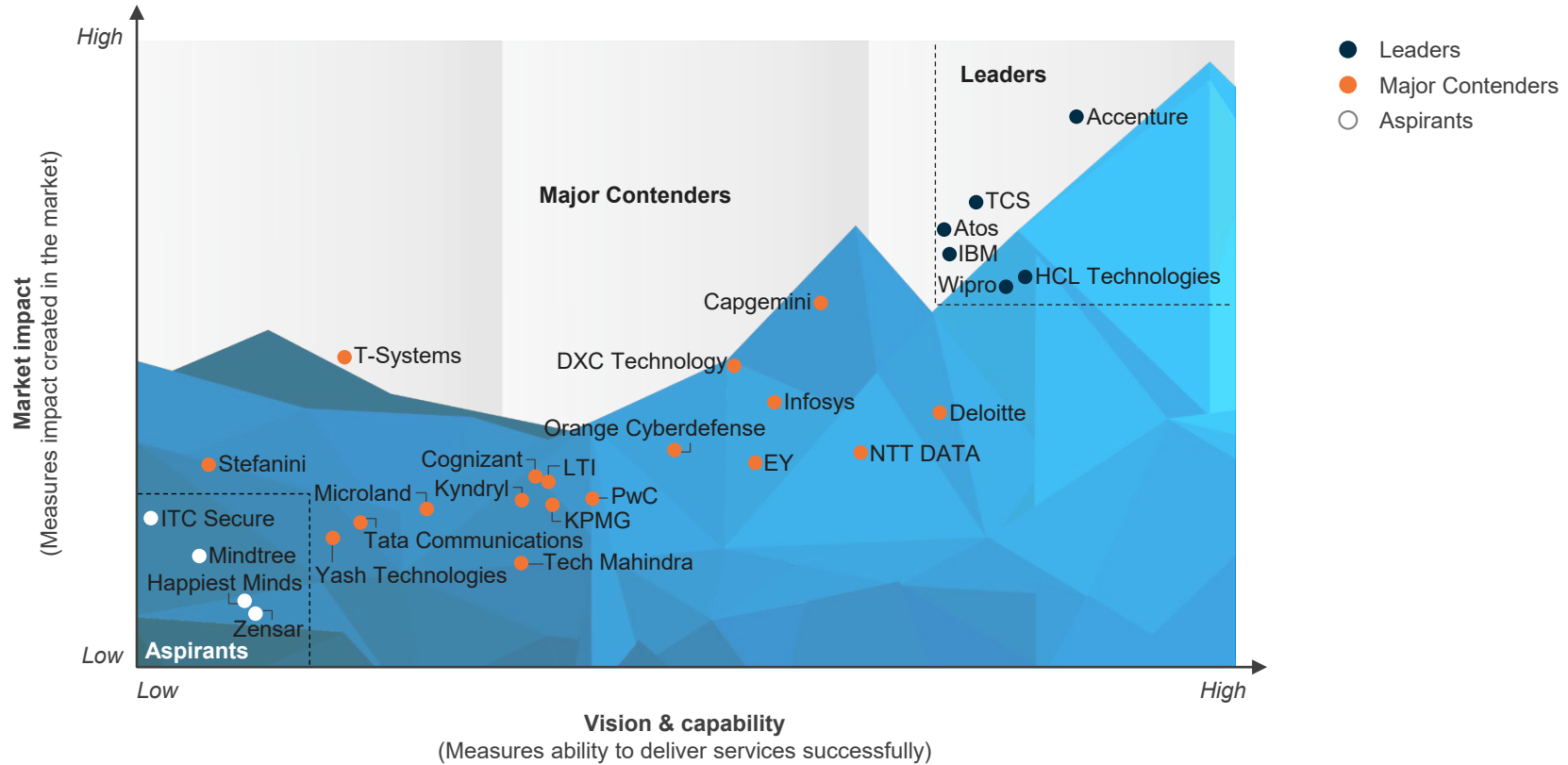
Happiest Minds, ITC Secure, Mindtree, and Yash Technologies

- The IT security services business of Aspirants is at a relatively early stage and is not a leading revenue generator for such players
- Nevertheless, these companies are making investments to build broader capabilities in the IT security services space to cater to buyers through service and technology partnerships as well as internal IP/tools. This is keeping them poised to be major challengers in the space

Everest Group PEAK Matrix®

IT Security Services PEAK Matrix® Assessment 2022 – Europe | Wipro positioned as Leader

Everest Group – IT Security Services PEAK Matrix® Assessment 2022 – Europe^{1,2}



1 Assessments for Capgemini, Deloitte, EY, IBM, KPMG, Orange Cyberdefense, PwC, and T-Systems is based on Everest Group's proprietary Transaction Intelligence (TI) database, service provider public disclosures, and Everest Group's interactions with enterprise buyers










2 Analysis for LTI and Mindtree is based on capabilities before their merger

Source: Everest Group (2022)

Wipro | IT security services – Europe (page 1 of 7)

Everest Group assessment – Leader

Measure of capability:  Low  High

Market impact				Vision & capability				
Market adoption	Portfolio mix	Value delivered	Overall	Vision and strategy	Scope of services offered	Innovation and investments	Delivery footprint	Overall
								

Strengths

- Wipro has expanded its cybersecurity delivery capabilities through acquisitions such as Edgile and Capco for consulting and Ampion for analytics and DevOps, providing clients with robust solutions and expert talent
- Clients have appreciated Wipro’s ability to move fast on new-age security themes through its investments in multiple start-ups via the Wipro venture capital fund
- Enterprises looking for a service provider with robust GRC and data security capabilities will find Wipro to be a good fit because of its credible proof points around ServiceNow GRC and its investments in data security services
- Clients have acknowledged Wipro’s ability to contain attrition through various talent retention initiatives such as the CyberSecurist program, leadership skill-building initiatives, and its partnership with academia
- Wipro offers automation-enabled solutions such as EdgileArC for GRC and HOLMES for Cyber that covers TPRM, which results in reduced human effort and accurate outcomes

Limitations

- Enterprise buyers from public sector vertical must be wary that Wipro has limited proof points in delivering security services to this specific vertical
- Enterprises looking for a robust onshore-nearshore presence will find Wipro lagging its peers in providing a strong localized presence
- A few clients have highlighted that Wipro takes a siloed approach in delivering security services and is not proactive in pitching innovative solutions
- Some clients have indicated that Wipro needs to be more innovative in its pricing constructs
- Enterprises buyers from automotive industry might not find Wipro to be a good fit because it lags peers in delivering dedicated security services for this vertical
- Enterprises buyers looking for OT security services should be aware that Wipro has limited partnerships in this domain and lags peers in building dedicated solutions for OT

Wipro | IT security services – Europe (page 2 of 7)

Overview

Vision

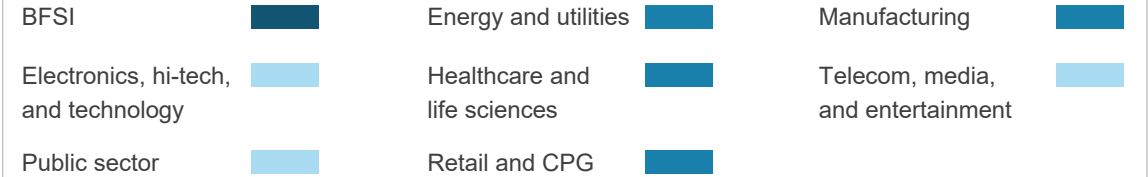
Wipro's vision is to assist various enterprises in achieving a resilient cyber future. It also wants to be on the leading edge of technology innovation, get recognition from its peers in the cyber services industry, and purposefully give back to the cyber security community.

IT security services revenue (2021)

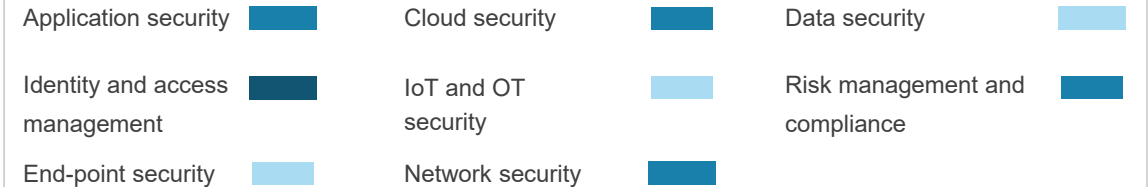


Low (<10%) Medium (10-20%) High (>20%)

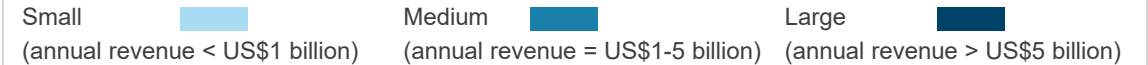
Adoption by industry



Adoption by service segments

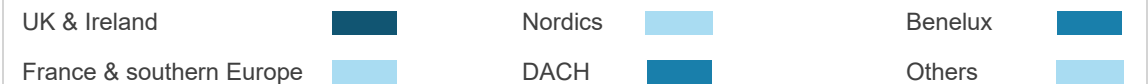


Adoption by buyer group



Adoption by country

Low (<15%) Medium (15-40%) High (>40%)



Source: Everest Group (2022)

Wipro | IT security services – Europe (page 3 of 7)

Case studies

Case study 1

Redesigned a service delivery model to ensure better compliance

Client : the world's second-largest tobacco company

Business challenge

The client's environment is decentralized and distributed, and numerous infrastructure components do not meet the desired thresholds. Without a comprehension of the organization's security posture, various suppliers were jointly managing all the client's DCS and DRS.

Solution

Wipro redesigned the service delivery model and onboarded services into an integrated service framework. It also enhanced the client service framework in the following ways:

- Transitioned services incrementally starting with two services initially, and within 12 months it integrated 10 services across the security services portfolio
- Standardized & optimized network security infrastructure, firewall assurance, and governance, audit, and reporting

Impact

- Increased endpoint compliance posture from 90 to 99% for servers and overall endpoints by 60 to 95%
- Improved firewall compliance posture from 65% to 99%
- Reduced incident ticket volumes by 20%

Case study 2

Adoption of identity and life cycle management solution for a Swiss multinational

Client: a Swiss multinational food and drink processing conglomerate

Business challenge

Due to the client's extensive customization, introducing frozen jobs to the One IDM solution and carrying out health checks posed significant challenges. Additionally, business stakeholders demanded access to information on the progress of everyday tasks that involved the ops team's manual labor and time.

Solution

Wipro adopted one IDM as an identity life cycle management solution to manage users in the active directory, web applications, the Safeguard PAM system, and other systems. It implemented specific rules that would be required due to extensive customization in the identity life cycle area. Additionally, an IMC dashboard solution was put into place, which helped in extracting the health status from One IDM and displaying it on a dashboard for the operations team. To facilitate decision-making and improve corporate visibility, all frozen jobs were identified, presented on the dashboard with problem codes, and produced automatic reports.

Impact

- Reduced 50% of administrative overheads
- Saved 120 minutes per day in health checks
- Increased 30% efficiency to issue resolution as triaging is done and presented on a dashboard

Wipro | IT security services – Europe (page 4 of 7)

Solutions/IP/products

Proprietary solutions/IP/products (representative list)	
Solution name	Details
Cyber Defense Portal (CDP)	CDP is a platform that gives a single pane view of cyber security risks, threats, attacks, and response measures undertaken in the enterprise. It provides a view of the security posture of the enterprise by monitoring application and infrastructure vulnerabilities, threat intelligence, and security monitoring by integrating a variety of security tools. The goal of the CDP is to help customers and thwart coordinated cyber attacks across the enterprise’s digital landscape.
Security Management Center (SMC)	It aids in the transformation journey of customers by increasing efficiencies in managing operations on the security infrastructure covering both on-premise and the cloud.
SlaaS	SlaaS is an advanced security monitoring service that is powered by an ecosystem of partner tools, home-grown platforms, and custom use cases. The solution consists of a multi-tenant-based SIEM platform that is integrated with the TlaaS, CDP Portal, and the customer environments through collectors.
Threat Intelligence-as-a-Service (TlaaS)	TlaaS provides the capability to identify, contextualize, and deliver intelligence. Wipro’s TlaaS continuously discovers the critical threats targeting businesses by mapping external threat intelligence to the client’s unique digital assets. It delivers tailored intelligence from across the clear, deep, and dark web in the form of categorized alerts to customers' organizations.
Playbook-as-a-Service	Playbook-as-a-Service powered by a SOAR platform helps to automate security incident detection and response in an organization with the help of playbooks, API integrations, and automation scripts. This also provides analysts with a reliable platform to perform incident response and handle security incidents seamlessly.
Cloud Application Risk Governance (CARG)	CARG offers a risk and compliance posture view of the application hosted on the cloud to the business and application owners. CARG gives complete visibility from the compliance perspective of the application with customizable use case implementation as per customer requirements. CARG platform and back-end framework of security control definition are suitable for any cloud service provider.
Identity Management Center (IMC)	The IMC is a platform that strings together multiple types of IAM solutions by bringing in valuable functionality including a centralized and unified dashboard.
Third-party Risk Management Platform (TPRM-HOLMES)	This solution helps organizations accelerate the pace and frequency of risk assessment of dependent third parties. It is aligned to the business owners of the organization by providing risk and compliance posture across business applications, processes, and organizational hierarchy.
Monitoring Automation Framework (MAF)	MAF helps to provide centralized monitoring for the various IAM tools present in the customer’s identity landscape through API-based integrations with these tools.

Wipro | IT security services – Europe (page 5 of 7)

Partnerships

Partnerships (representative list)		
Partner name	Type of partnership	Details of the partnership
Microsoft	Cloud security	Wipro has a multi-channel relationship. As a key global advisory, SI, and Managed Security Services Provider (MSSP) partner its co-sell offerings go across Azure and M365 security and privacy. It is an elite global partner, and it provides MXDR and broader cyber security services via its industry solutions delivery arm.
AWS	Cloud security	Wipro is an AWS MSSP competency partner and provides joint AWS security solutions to global customers. Wipro offers different AWS security services and extensively leverages AWS native security services for large-scale cloud deployment projects.
Google	Cloud security	Google and Wipro offer leading security solutions and services within cyber security risk advisory, transformation, and managed security services. Wipro is also a Google security specialization partner. Wipro and Google are working on providing advanced managed security and cloud security operations capabilities.
Palo Alto	Cloud security	Wipro collaborates strategically with Palo Alto Networks as a CPSP partner to leverage its Coretex SOAR, Prisma cloud, and Strata capabilities across Wipro's CDC MSSP stack and cloud security services.
Zscaler	Network security	This is Wipro's strategic partner for zero trust network solutions & secure cloud migrations. The Wipro and Zscaler partner program provides new training certifications for the Zscaler Digital Experience (ZDX) platform.
Sailpoint	Identity and access management	Wipro developed joint solutions with Sailpoint, primarily for on-premise-based identity governance and administration and delivers SI and managed services to clients.
CyberArk	Identity and access management	It developed joint solutions with CyberArk, primarily in the area of Privileged Access Management (PAM), and delivers SI, and managed services to clients.
Saviynt	Identity and access management	The company developed joint solutions with Saviynt, primarily for cloud-based identity governance and administration, and delivers SI and managed services to clients.
ServiceNow	Risk management and compliance	The GRC practice has successfully delivered hundreds of client projects across ServiceNow GRC and security operations modules. Wipro has built over 25 solution accelerators on ServiceNow.
SAP Security & GRC	Risk management and compliance	The company GRC practice has successfully delivered over 25 engagements across different SAP security & GRC modules.
OneTrust	Risk management and compliance	The GRC practice has successfully delivered over 50 engagements across OneTrust GRC and data privacy modules.

Wipro | IT security services – Europe (page 6 of 7)

Partnerships

Partnerships (representative list)		
Partner name	Type of partnership	Details of the partnership
Cisco	Endpoint security	Wipro developed joint solutions with Cisco Security for multiple solutions including MDR, perimeter security defense, CASB, messaging, and web security solutions.
CrowdStrike	Endpoint security	Wipro developed joint solutions with CrowdStrike for multiple solutions including MDR, next-generation antivirus, and delivery as a service to clients.
RSA	Risk management and compliance	Wipro developed joint solutions with RSA primarily in the area of GRC and delivering SI and managed services to clients.
MetricStream	Risk management and compliance	Wipro developed joint solutions with MetricStream primarily in the area of GRC.
Forcepoint	Data security	Wipro established 360-degree relationships, both in delivering joint solutions to Wipro’s clients and as a global Professional Services (PS) partner to Forcepoint clients across the globe.
Microfocus	Data security	Wipro developed joint solutions with Microfocus for multiple solutions including application security assurance (Security code review and DevSecOps), data security, and in delivering SI and managed services to clients.
Symantec	Data security	It entered into partnerships across multiple domains such as compliance, data center security, advanced threat protection, and data leakage prevention.
Splunk	Data security	This helps in security analytics for big data.
IBM	Network security	Wipro developed joint solutions with IBM primarily in the area of SIEM and security operations and in delivering SI and managed services to clients.
Checkpoint	Network security	Wipro developed joint solutions with Checkpoint primarily in the area of network perimeter defense and in delivering SI and managed services to clients.
McAfee	Data security	Wipro leverages McAfee solutions to deliver managed networks, endpoint, and data security services.
F5	Network security	Wipro leverages F5 products to deliver network security, load balancer, and web application services.
Radware	Application security	It leverages Radware products to deliver network security, load balancer, and web application services.

Wipro | IT security services – Europe (page 7 of 7)

Investments and recent activities

Investments (representative list)

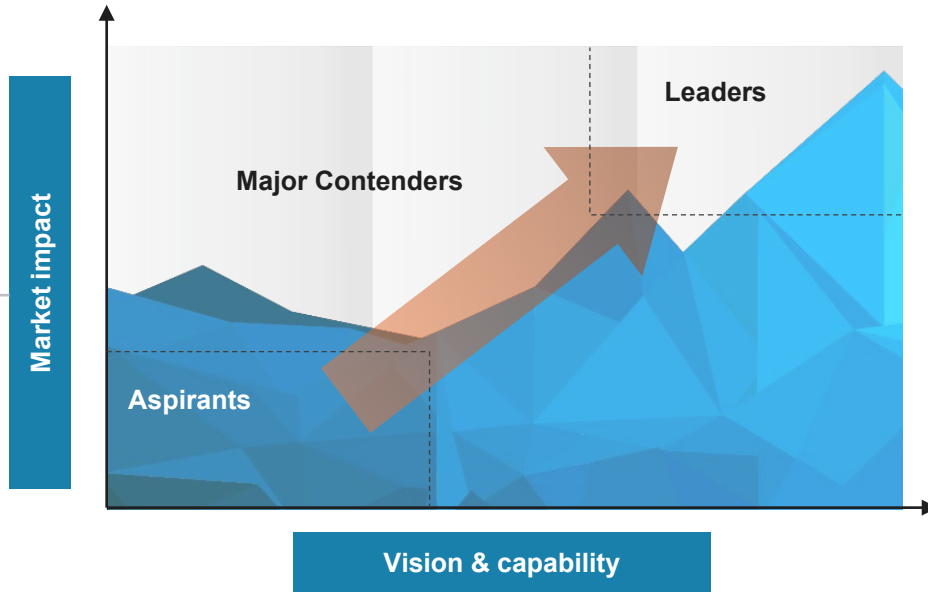
Investment name	Details
Acquisition	Wipro acquired three companies, Edgile, Capco (risk & security practice), and Ampion, to strengthen its leadership in strategic cyber security services across North America, Europe, and APAC
Talent	Rolled out the CyberSecurist functional model to drive holistic development across cyber technology, risk, sector, consulting, and program management with a renewed career architecture framework
Others	<ul style="list-style-type: none"> • ShiftLeft: a modern AppSec platform that helps minimize the attack ability of client’s applications, improve developer productivity, and accelerate software delivery • Securonix: Securonix is a next-generation analytics platform with SOAR capabilities that can be deployed across the cloud and on-premises. It is being leveraged for shared services engagements for analyzing millions of security events in real-time • Vulcan: Vulcan Cyber provides the industry’s first vulnerability remediation orchestration platform, built to help businesses reduce cyber risk through measurable cloud and application security • Vectra: Vectra enables the clients to conduct real-time continuous threat monitoring across the network and the data center to instantly identify any phase of a cyber attack • Cycognito: Cycognito enables security teams to eliminate critical attack vectors. Cycognito offers a SaaS platform that can map the attack surface of organizations and help eliminate blind spots that can be exploited by attackers • Immuta: it helps in automating data access and privacy controls to accelerate self-service data delivery, simplify administration, reduce risk, and safely unlock more data use in the cloud

Appendix

Services PEAK Matrix® evaluation dimensions

Measures impact created in the market – captured through three subdimensions

- Market adoption**
Number of clients, revenue base, YoY growth, and deal value/volume
- Portfolio mix**
Diversity of client/revenue base across geographies and type of engagements
- Value delivered**
Value delivered to the client based on customer feedback and transformational impact



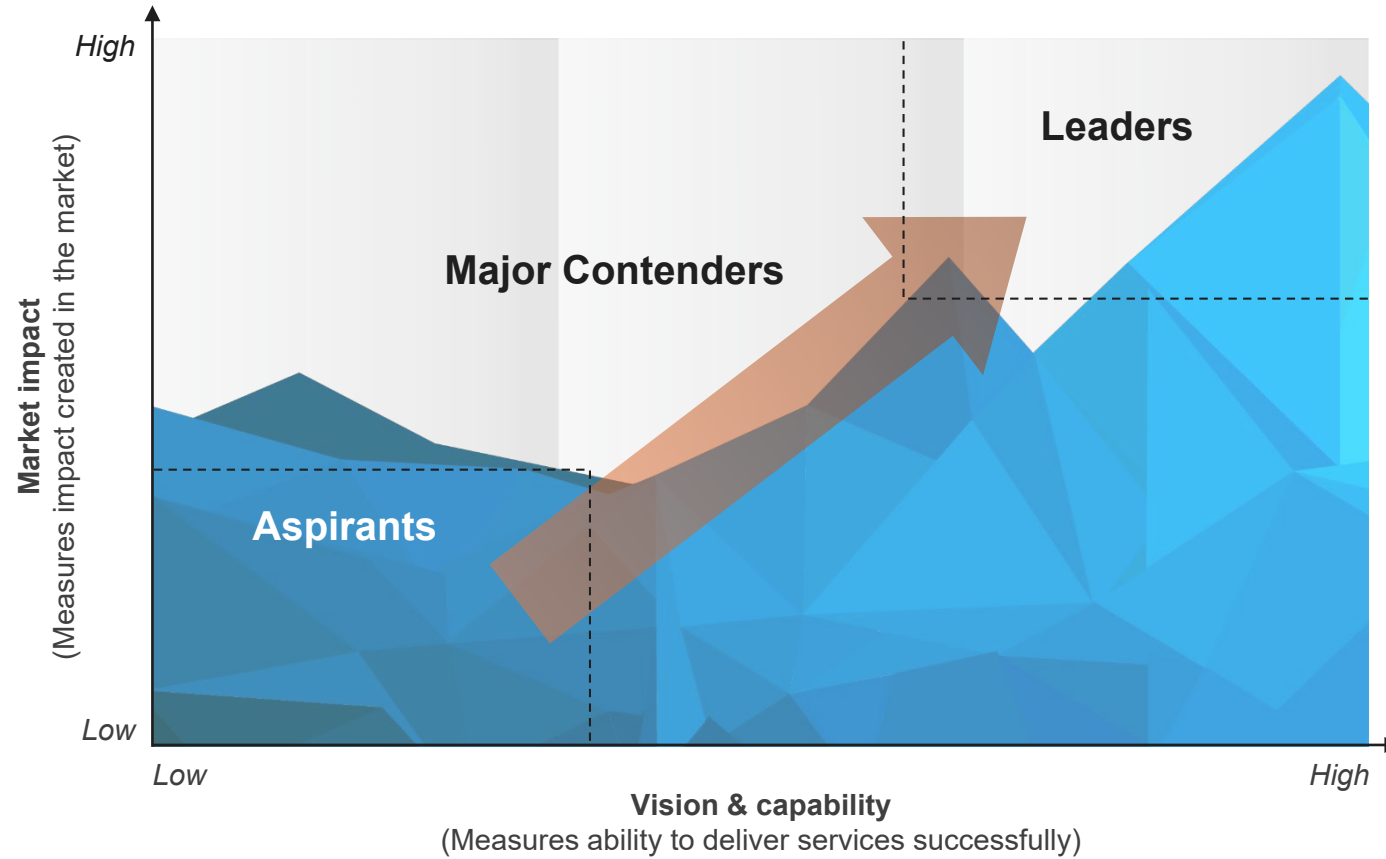
Measures ability to deliver services successfully. This is captured through four subdimensions

- Vision and strategy**
Vision for the client and itself; future roadmap and strategy
- Scope of services offered**
Depth and breadth of services portfolio across service subsegments/processes
- Innovation and investments**
Innovation and investment in the enabling areas, e.g., technology IP, industry/domain knowledge, innovative commercial constructs, alliances, M&A, etc.
- Delivery footprint**
Delivery footprint and global sourcing mix

Everest Group PEAK Matrix® is a proprietary framework for assessment of market impact and vision & capability



Everest Group PEAK Matrix®



FAQs

Does the PEAK Matrix® assessment incorporate any subjective criteria?

Everest Group's PEAK Matrix assessment adopts an unbiased and fact-based approach (leveraging provider / technology vendor RFIs and Everest Group's proprietary databases containing providers' deals and operational capability information). In addition, these results are validated / fine-tuned based on our market experience, buyer interaction, and provider/vendor briefings

Is being a “Major Contender” or “Aspirant” on the PEAK Matrix, an unfavorable outcome?

No. The PEAK Matrix highlights and positions only the best-in-class providers / technology vendors in a particular space. There are a number of providers from the broader universe that are assessed and do not make it to the PEAK Matrix at all. Therefore, being represented on the PEAK Matrix is itself a favorable recognition

What other aspects of PEAK Matrix assessment are relevant to buyers and providers besides the “PEAK Matrix position”?

A PEAK Matrix position is only one aspect of Everest Group's overall assessment. In addition to assigning a “Leader”, “Major Contender,” or “Aspirant” title, Everest Group highlights the distinctive capabilities and unique attributes of all the PEAK Matrix providers assessed in its report. The detailed metric-level assessment and associated commentary is helpful for buyers in selecting particular providers/vendors for their specific requirements. It also helps providers/vendors showcase their strengths in specific areas

What are the incentives for buyers and providers to participate/provide input to PEAK Matrix research?

- Participation incentives for buyers include a summary of key findings from the PEAK Matrix assessment
- Participation incentives for providers/vendors include adequate representation and recognition of their capabilities/success in the market place, and a copy of their own “profile” that is published by Everest Group as part of the “compendium of PEAK Matrix providers” profiles

What is the process for a provider / technology vendor to leverage their PEAK Matrix positioning and/or “Star Performer” status ?

- Providers/vendors can use their PEAK Matrix positioning or “Star Performer” rating in multiple ways including:
 - Issue a press release declaring their positioning. See [citation policies](#)
 - Customized PEAK Matrix profile for circulation (with clients, prospects, etc.)
 - Quotes from Everest Group analysts could be disseminated to the media
 - Leverage PEAK Matrix branding across communications (e-mail signatures, marketing brochures, credential packs, client presentations, etc.)
- The provider must obtain the requisite licensing and distribution rights for the above activities through an agreement with the designated POC at Everest Group.

Does the PEAK Matrix evaluation criteria change over a period of time?

PEAK Matrix assessments are designed to serve present and future needs of the enterprises. Given the dynamic nature of the global services market and rampant disruption, the assessment criteria are realigned as and when needed to reflect the current market reality as well as serve the future expectations of enterprises



Everest Group is a research firm focused on strategic IT, business services, engineering services, and sourcing. Our research also covers the technologies that power those processes and functions and the related talent trends and strategies. Our clients include leading global companies, service and technology providers, and investors. Clients use our services to guide their journeys to maximize operational and financial performance, transform experiences, and realize high-impact business outcomes. Details and in-depth content are available at www.everestgrp.com.

Stay connected

Website

everestgrp.com

Social Media

-  @EverestGroup
-  @Everest Group
-  @Everest Group
-  @Everest Group

Blog

everestgrp.com/blog

Dallas (Headquarters)

info@everestgrp.com
+1-214-451-3000

Bangalore

india@everestgrp.com
+91-80-61463500

Delhi

india@everestgrp.com
+91-124-496-1000

London

unitedkingdom@everestgrp.com
+44-207-129-1318

Toronto

canada@everestgrp.com
+1-647-557-3475

This document is for informational purposes only, and it is being provided "as is" and "as available" without any warranty of any kind, including any warranties of completeness, adequacy, or fitness for a particular purpose. Everest Group is not a legal or investment adviser; the contents of this document should not be construed as legal, tax, or investment advice. This document should not be used as a substitute for consultation with professional advisors, and Everest Group disclaims liability for any actions or decisions not to act that are taken as a result of any material in this publication.