



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

Focus on Accenture
August 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.

This 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:

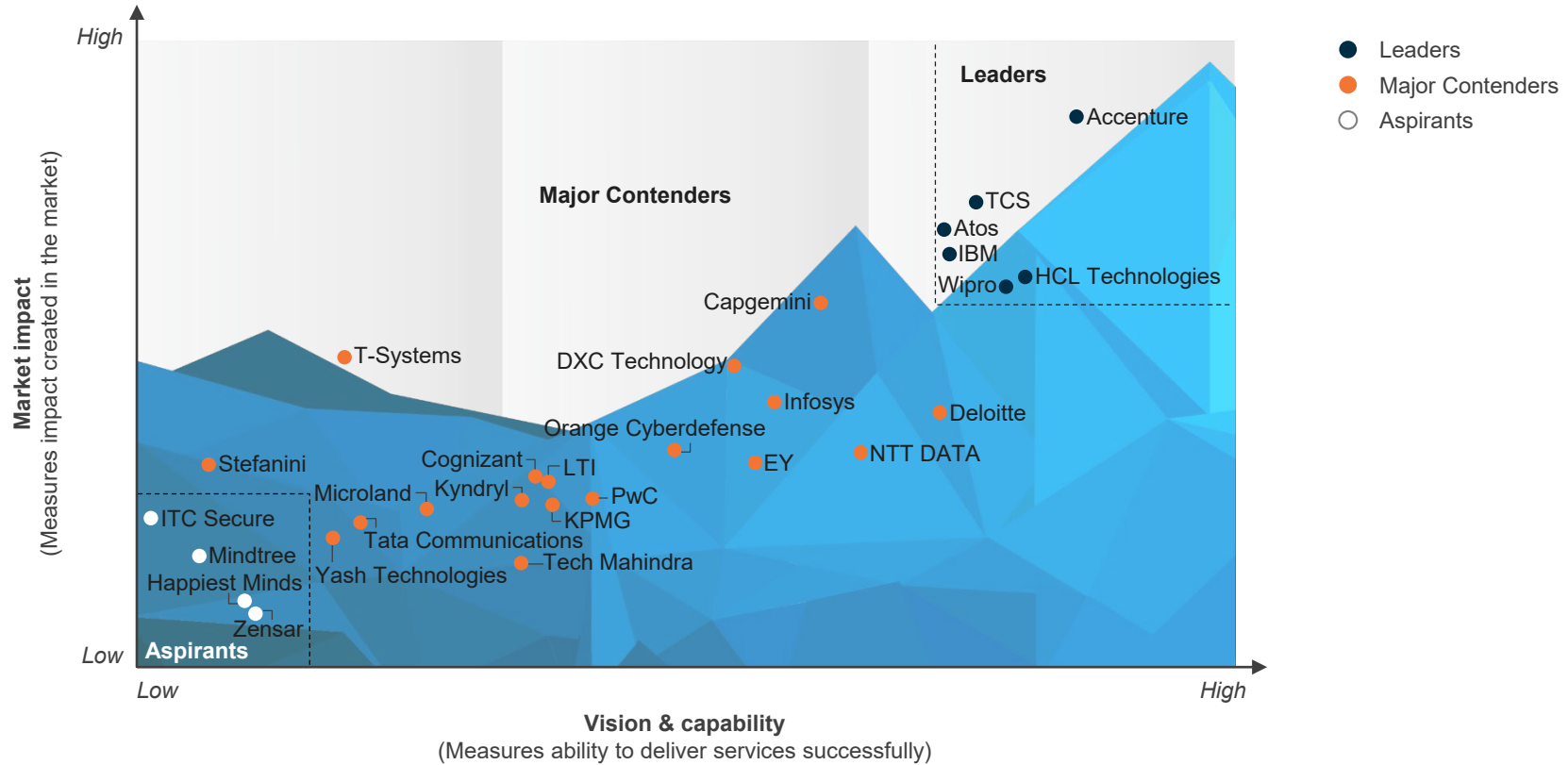
Happiest Minds, ITC Secure, Mindtree, and Yash Technologies

- 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 | Accenture 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)

Accenture | IT security services – Europe (page 1 of 6)

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

- Enterprises will benefit from Accenture’s comprehensive solution set that cuts across security themes such as OT security, application security, cloud security, IAM, and zero-trust; this is further enhanced by Accenture’s continued bolt-on acquisitions
- Enterprises looking to invest in next-generation security will find Accenture attractive due to its extensive investments in innovation and new-age solutions such as blockchain-based identities, connected car security, and digital twin security solution, CyTwin
- Enterprise buyers looking for GDPR and OT compliance services will find Accenture’s maturity assessment tools to be valuable because of the extensive coverage of government regulations and compliances that they provide
- Clients have appreciated Accenture for its ability to deliver complex security engagements and its deep domain and technical expertise, and see it as a strategic partner in security

Limitations

- A few clients have raised concerns about Accenture’s high attrition in security service
- Despite being lauded by clients for its breadth of security offerings and its expertise, clients have raised concerns around its premium pricing and contractual flexibility
- Enterprise buyers searching for a service provider for pure-play managed security services might not find Accenture to be a right fit, as it has more proof points on consulting and design & implementation services
- Some clients from Europe have highlighted that Accenture needs to expand the on-ground presence of its senior management for better stakeholder handling

Accenture | IT security services – Europe (page 2 of 6)

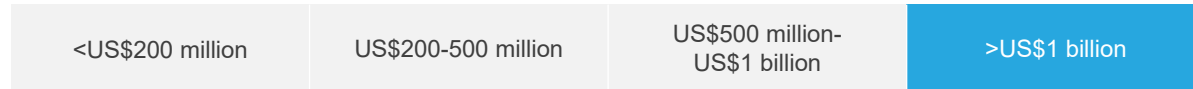
Overview

Vision

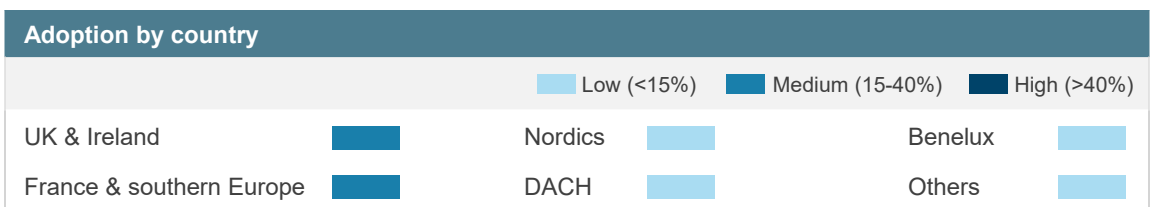
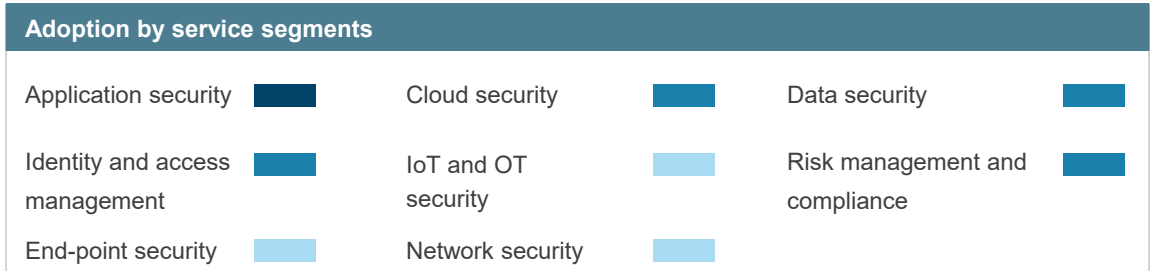
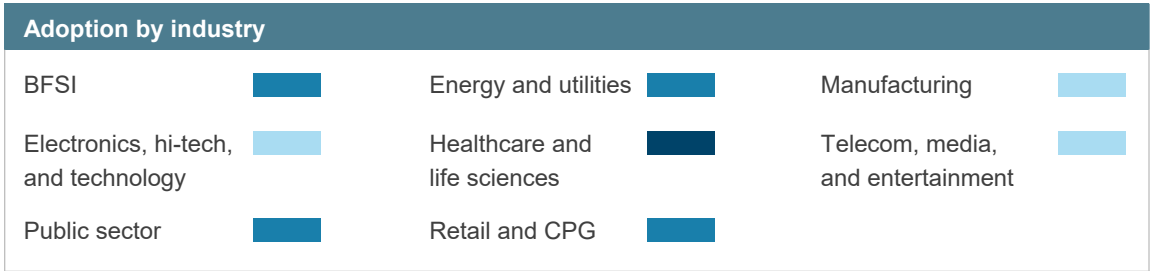
Accenture believes security is central to protecting organizations and bridging the security operations and mainstream business priorities. Its mission is to help its clients and partners securely transition into an omni-connected world.

Accenture works with clients from deep practitioners to the C-suite to see security as a business accelerator, ensuring the client’s investments in transformative solutions and providing trusted 360-degree value by reimagining business cyber protection that is built for the future. Its comprehensive and industry-tailored security offerings span the entire security lifecycle from cyber strategy to cyber resilience to cyber protection. It serves as a single end-to-end security provider and its holistic perspective allows it to deliver solutions aligned to its client’s needs.

IT security services revenue (2021)



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



Note: The Nordics (Norway, Sweden, Finland, and Denmark); Benelux (Belgium, Netherlands, and Luxembourg); France and Southern Europe (Spain, Italy, and Portugal); DACH (Germany, Austria, and Switzerland) and Poland
 Source: Everest Group (2022)

Accenture | IT security services – Europe (page 3 of 6)

Case studies

Case study 1	Rebuild IT and security services for a global conglomerate post-separation from its parent
Client: a global beauty products company	
Business challenge The client is required to start from the ground up to build a strong IT and security foundation. As a primary separation and transformation partner, Accenture's scope comprised 50+ countries, and 90+ sites, including DSs, offices, studios, factories, and 700+ applications.	
Solution Accenture Security offered comprehensive security consulting, transformation, and operational services for the separation journey covering the below services:	
<ul style="list-style-type: none">• Security governance, risk, and compliance• Identity and access management and security operations & monitoring• Application security testing & DevSecOps• Endpoint detection & response• Infrastructure vulnerability management & penetration testing	
Impact	
<ul style="list-style-type: none">• Delivered 20+ security stage-gate deliverables, 20 security rules, and 6 security standards• 200+ security controls developed, with a security operations center monitoring assets 24*7• 3500+ security threats dealt with, 500+ admin accounts secured using a privileged access management system, and 95+ IT vendor security exams performed• Over 600 applications were evaluated utilizing inherent risk assessment• Over 130 application segments have been added to the remote access solution• A vulnerability management system is utilized to scan all cloud and on-premises assets	

Case study 2	Manage cyber security risk exposure, threats, exposure, and vulnerabilities to deliver business objectives
Client: a global household appliances company	
Business challenge The client engaged with Accenture Security to provide end-to-end security advisory, transformation, and run services to manage their risk exposure	
Solution Accenture conducted a rigorous evaluation of high-risk suppliers for the client, to establish their compliance with cyber security best practices in 17 categories. Accenture's cyber fusion center operating model will then be designed, built, and operationalized to drive the maturity of Cyber Defense capabilities to monitor and safeguard assets internationally. Accenture carries out the following activities:	
<ul style="list-style-type: none">• Using the Cyber SOC program, providing operational help to triage and assess cyber incidents based on security use cases and allowing 24x7 security monitoring capacity.• Providing PCI DSS support to the client information security and compliance team in order to improve customer cardholder data security across multiple payment channels internationally.• Providing a Data Loss Prevention (DLP) plan and roadmap for the client's investments in Microsoft products, as well as deploying the appropriate security solutions to increase the protection of intellectual property and other sensitive data and decrease the risk of insider threats.	
Impact	
<ul style="list-style-type: none">• Improved monitoring, detection, and response to possible cyber threats, with 80 percent coverage throughout their estate and 40+ operationalized use cases• Reduced downtime to zero, vulnerability mitigation, and moving high and very high-security exposures inside tolerance• Reduced the possibility of substantial regulatory fines (e.g., 4% annual turnover)• Structured security training and awareness courses have been put into action• Boosted customer trust in the client's brand and goods while maintaining digital workplace security	

Accenture | IT security services – Europe (page 4 of 6)

Solutions/IP/products

Proprietary solutions/IP/products (representative list)

Solution name	Details
Autonomous identity	Patented analytics and machine learning solution analyzes enterprise access controls and makes recommendations; licensed/sold through partner ForgeRock
Cloud identity governance & administration accelerator	Modular, pre-built reference architectures, data models and integrations to enable cloud-based Identity, Governance, & Administration (IGA) for large, highly-complex organizations
Intelligent App Sec Platform	The Intelligent App Sec Platform is a patented solution that enables secure application development at scale via auto-triage and auto-remediation solutions.
Secure cloud	A secure Cloud is a standardized approach and repeatable IP, automation, and frameworks across AWS, Azure, and Google Cloud that is delivered and deployed directly into the clients' cloud accounts in order to enable true DevSecOps
Secure platforms	IP and tooling for SAP, Oracle, and Salesforce to perform fast, consistent, and accurate security assessments
Accenture delivery methods and estimators for security	Accenture Delivery Methods (ADM) for security provide delivery methods for common security planning and security implementation services. Estimators are available to plan and deliver large-scale, complex consulting/assessment, design/integration, and outsourcing programs
Industry security value chains	Presents the key operational activities, processes, or products for each industry. Critical assets, key threat actors, and sample threats are also identified
Recon darknet detection	An asset-based, automated solution designed to monitor and measure risks to and impact on a client's attack surface. It is used to consistently identify existing threats directly relevant to clients' businesses as well as uncover new and emerging threats that clients use to improve their respective security posture
Connected car security (Memory)	Full-featured identity factory for connected car security, focused on Gallia
IntelGraph Intelligence Portal and API	IntelGraph Intelligence portal combines context-rich reports, powerful visualizations, advanced searching, alerting, and a robust RESTful API to enable faster access to relevant threat data and allow efficient and easy pivoting on threat indicators
Managed Extended Detection and Response (MXDR)	Full suite detection, response, and remediation – including people, platform, licenses, and storage – to proactively mitigate cyber-attacks & malicious activity at a lower price point

Accenture | IT security services – Europe (page 5 of 6)

Partnerships

Partnerships (representative list)		
Partner name	Type of partnership	Details of the partnership
AWS	Technology partnership	Strengthen the ability to detect, prevent, and respond to infrastructure threats (networks, clouds, endpoints, mobile, and IoT)
CrowdStrike	Technology partnership	Detect, respond to, and recover from threat actors and breaches impacting business operations
CyberArk	Technology partnership	Digital identity and privileged access management services
Forescout	Technology partnership	Secure connected devices (IoT/IIoT/ICS) and embedded systems to enable intelligent, connected, and trusted products and services for clients' use internally and to sell to their customers; this includes securely building, implementing, and operating SW & HW
ForgeRock	Technology partnership	Digital identity and autonomous identity services
Fortinet	Technology partnership	Secure connected devices (IoT/IIoT/ICS) that involve securely designing, installing, and running SW and HW
Google	Technology partnership	Strengthen the ability to detect, prevent, and respond to infrastructure threats (networks, clouds, endpoints, mobile, and IoT)
Micro Focus	Technology partnership	Application security scanning, managed security services, SIEM services, and application security services
Microsoft	Technology partnership	Strengthen the ability to detect, prevent, and respond to infrastructure threats (networks, clouds, endpoints, mobile, and IoT)
Nozomi Networks	Technology partnership	Secure connected devices (IoT/IIoT/ICS) and embedded systems to enable intelligent, connected, and trusted products and services for clients' use internally and to sell to its customers; this includes securely building, implementing, and operating SW & HW
Okta	Technology partnership	Design and implement Identity and Access Management (IAM) services capable of securing client environments and experiences
One Identity	Technology partnership	Design and implement IAM services capable of securing client environments and experiences
Palo Alto Networks	Technology partnership	Protect core enterprise applications such as ERPs, CRMs, and other critical business platforms by hardening environments and improving monitoring security testing, governance, and risk and compliance
SailPoint	Technology partnership	Design and implement IAM services capable of securing client environments and experiences
Saviynt	Technology partnership	Design and implement IAM services capable of securing client environments and experiences
ServiceNow	Technology partnership	Transform governance, risk & compliance, and integrated risk management processes, taxonomy, and reporting through technology enablement
Splunk	Technology partnership	Cyber defense security transformation, SIEM services, and managed security services
VMWare	Technology partnership	Detect, respond, and recover from threat actors and breaches impacting business operations
Zscaler	Technology partnership	Strengthen the ability to detect, prevent, and respond to infrastructure threats (networks, clouds, endpoints, mobile and IoT)

Accenture | IT security services – Europe (page 6 of 6)

Investments and recent activities

Investments (representative list)

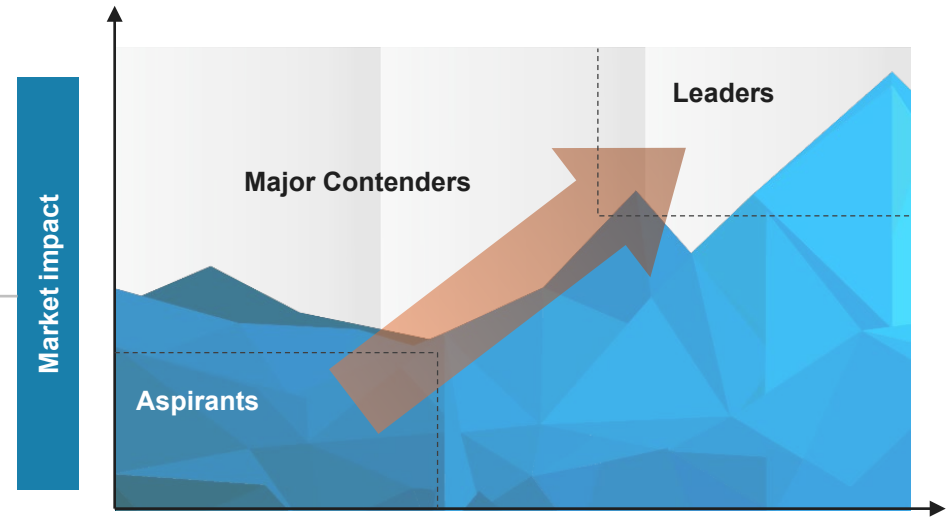
Investment name	Details
Acquisitions	Invested in six acquisitions to increase the cyber defense in the Israeli market with a focus on threat intelligence and to provide cyber security and cloud and infrastructure in France and Europe including IAM capabilities in France/Gallia. Some of the recent acquisitions in cyber security and cloud space include Maglan, Arismore, Context Information Security, Symantec Cyber Security Services, Openminded, and Sentor.
Talent	<p>Accenture invested in talent in FY21 to rapidly upskill its employees, which includes cloud certifications from cloud service provider partners such as Microsoft Azure, AWS, GCP, Alibaba, VMware, Workday, Salesforce, and others</p> <ul style="list-style-type: none"> • Security training and certification: programs to nurture employees in cyber security and soft skills such as ecosystem of social learning, analytics, and certifications include CISSP, CIPP, SBASA, CompTIA Security+, CompTIA CyberSec CSA, AWS, and many more • Non-STEM females training: Accenture, in cooperation with Pink Academy, offers 8-week training programs for female students with a humanistic/economic background who are eager to master security core skills in cloud security, cyber defense, and data protection, strategy, and risk
Others	Accenture features laboratories and a forum that focus on data recovery using Machine Learning, application attack prediction using graph analytics, and monthly virtual roundtables on relevant themes and periodic in-person events, respectively.

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



Vision & capability

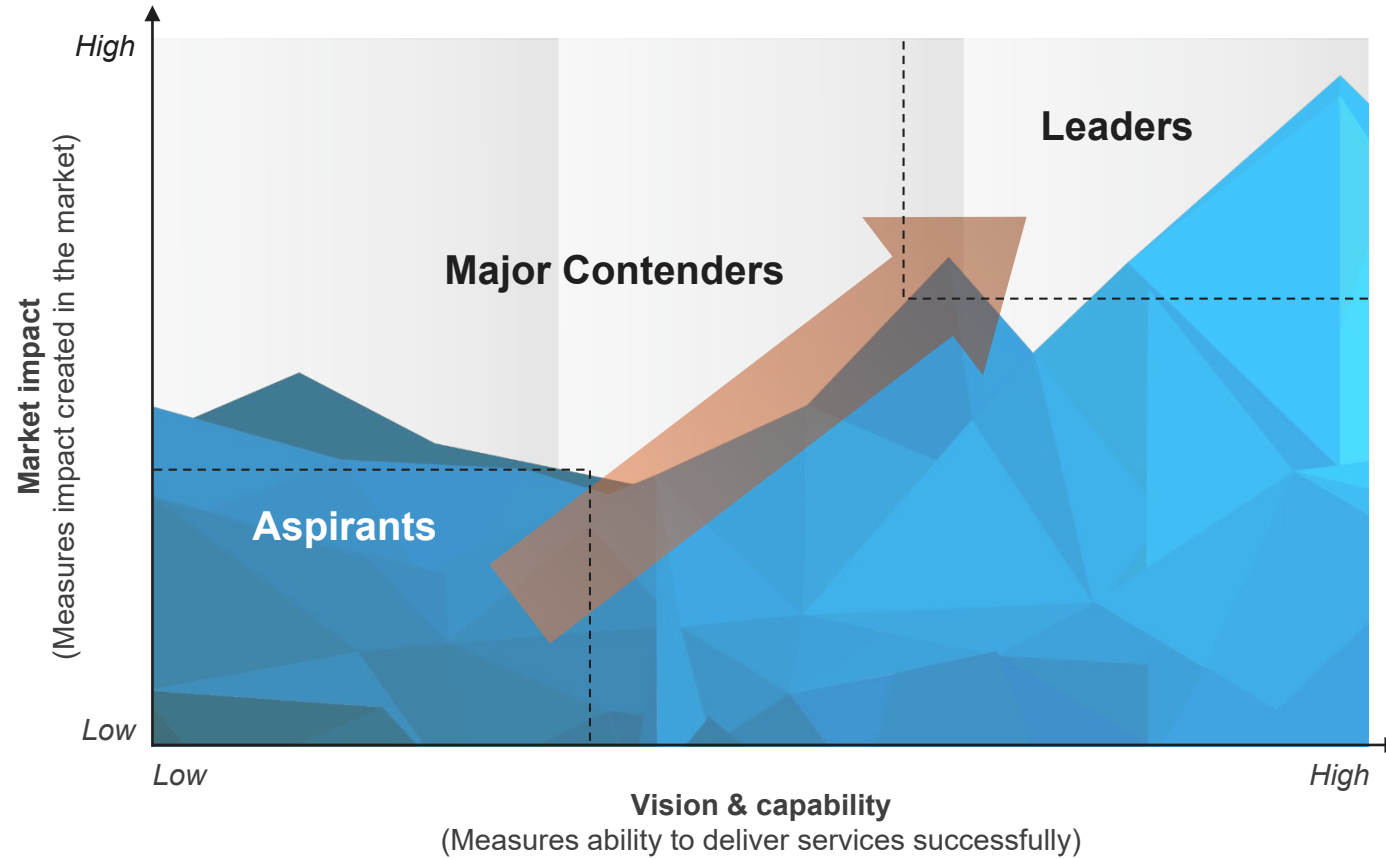
Measures ability to deliver services successfully. This is captured through four subdimensions

- 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.