Omdia
by informa techtarget

CSPs' Transformation Journeys Toward Autonomous Core Networks

Author: Roberto Kompany

January 2026

This Omdia White Paper was commissioned by Ericsson

Contents

This Omdia White Paper was commissioned by Ericsson

Summary

The telecommunications industry is experiencing a significant transformation fueled by the integration of 5G, cloud-native architectures, and artificial intelligence (AI). Communications service providers (CSPs) are leading this evolution, striving to deliver networks that are high-performing, resilient, scalable, and secure, all while addressing growing customer demands for agility and innovation. However, as networks grow more intricate—encompassing multiple technology generations and incorporating virtualized and containerized elements—the shortcomings of manual operations are becoming increasingly apparent. Conventional methods are unable to meet the requirements of network slicing, lifecycle management (LCM), and massive Internet of Things (IoT) device deployments.

Autonomous core networks have become a strategic solution to address these challenges. By leveraging AI-driven closed-loop automation and intent-based orchestration, CSPs can move away from reactive, manual operations toward proactive, self-managing systems. This transformation offers numerous advantages, including enhanced network performance, faster service deployment, lower operational costs, and an improved customer experience. Additionally, it empowers CSPs to capitalize on new revenue streams through advanced capabilities, such as network slicing and differentiated quality of experience (QoE) offerings.

However, the path to autonomy is not merely a technological advancement—it represents a fundamental organizational transformation. To unlock the full potential of Level 4 autonomous core networks, CSPs must prioritize workforce reskilling, cultural shifts, and process reengineering. Emerging roles, such as AI governance specialists and autonomous core network architects—areas where CSPs currently face talent gaps—will become essential. Additionally, technical expertise in AI/machine learning (ML), cloud-native technologies, and orchestration will be critical. Governance frameworks must also be established to ensure trust, security, and compliance in AI-driven decision-making processes.

This report examines the key drivers, challenges, and strategic priorities influencing CSPs' transition to autonomous core networks. Based on Omdia's global survey of 42 CSPs, it offers valuable insights into investment priorities, operational impacts, and the evolving skill requirements. By presenting actionable recommendations and benchmarking industry readiness, the report aims to help CSPs navigate the complexities of achieving autonomy and position themselves for success in an era defined by hyper-connectivity and digital innovation.

This Omdia White Paper was commissioned by Ericsson

The AI and autonomous core transformation journey

Mobile networks are increasingly complex to manage

As CSPs roll out 5G, the complexity of operating large-scale networks has increased dramatically. While upgrades to the radio access network introduce new spectrum layers and device densities, the most transformational changes are occurring at the core.

Deploying 5G means CSPs are simultaneously modernizing their core networks with cloud-native architectures. This shift introduces a multilayer environment in which a mix of physical, virtualized, and containerized assets coexist, increasing operational complexity across multiple generations of core technologies.

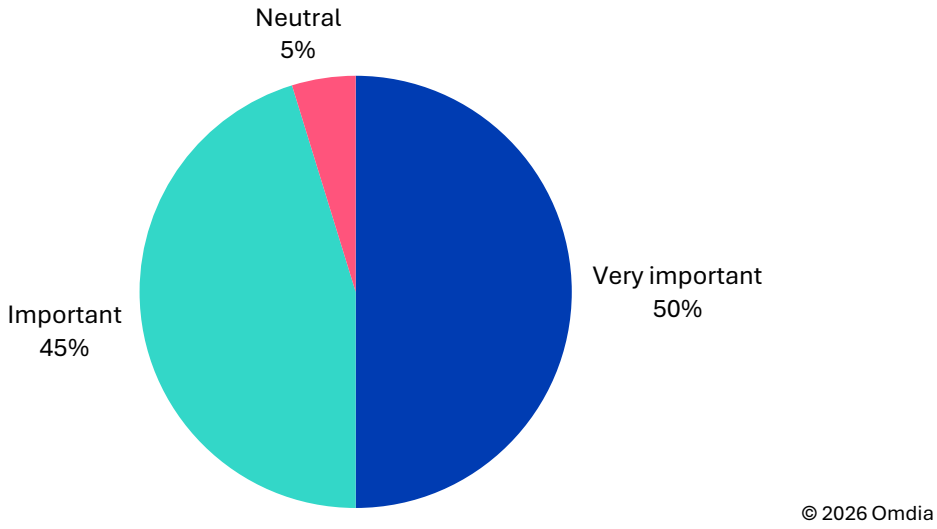
A cloud-native 5G core unlocks new service opportunities—such as network slicing—that depend on real-time orchestration and strict QoE and service-level agreement (SLA) guarantees. These capabilities are central to expanding CSP monetization beyond traditional mobile broadband.

At the same time, as the complexity of services and the number of devices—such as IoT sensors and drones— continue to grow, CSPs face mounting challenges in operational scalability. This includes tasks such as provisioning new devices, optimizing network sites, and ensuring service assurance through root cause analysis (RCA) and quality monitoring. As networks become increasingly complex, manual maintenance and troubleshooting are increasingly unsustainable; it introduces delays, operational risk, and rising workload pressure on operations teams. As CSPs confront this growing operational complexity, it becomes clear that automation must evolve beyond traditional approaches.

Further, according to Omdia's Global Telecoms Opex tracker, CSPs spend around 18% of the total telco opex on network operations. For these reasons, CSPs are working to deploy new automation tools and AI-based solutions to deliver both efficiency and cost reduction.

According to an Omdia survey of 42 global CSPs from North America, Asia & Oceania, Latin America and the Caribbean, Europe, the Middle East, and Africa, carried out in November 2025, only 5% of respondents indicated that they were neutral about how important AI in core networks was to their organization (**Figure 1**). While the question did not ask about where AI would be deployed in the network or the scale of the deployment, the answers show that half of the respondents consider it very important.

Figure 1: CSPs' priority of AI in core



Source: Omdia

The concept of network automation, however, is not new. CSPs have worked with industry partners over the last 10+ years to introduce the concepts of software-defined networking and network function virtualization to introduce virtualized network components and programmability across the networks.

To achieve zero-touch automation, it has become essential to move beyond basic automation and integrate intelligence into the life cycle of network and service management. This intelligence includes capabilities such as self-configuration, self-healing, and self-optimization. TM Forum introduced the concept of autonomous networks to address these needs, and it has since become a critical focus for CSPs in accelerating standardization efforts.

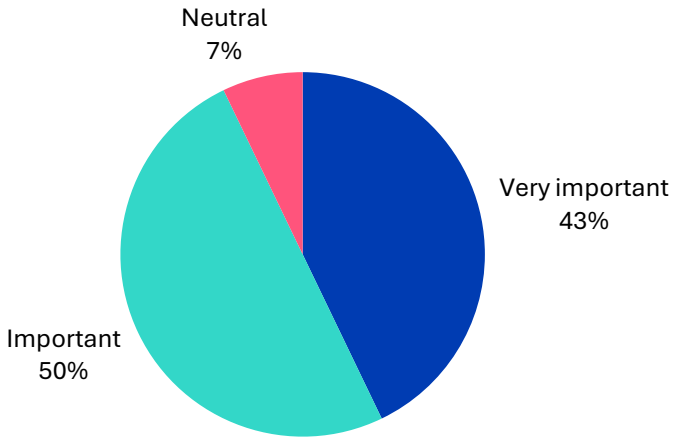
Autonomous networks were developed to help CSPs transition from manual operations to AI-driven, intent-based, closed-loop automation. These networks minimize human intervention by continuously monitoring and analyzing network conditions in real time, enabling automated, actionable decisions to ensure optimal performance. They also provide the foundation needed to manage the scale and complexity of cloud-native 5G core networks.

TM Forum's autonomy model provides a six-level scale (0 to 5) to define an operator's degree of automation and AI-driven capabilities. At Level 0 (no autonomy), all operations are performed manually, while at Level 5 (full autonomy), the network operates

independently, dynamically adapting to business objectives and evolving conditions without human intervention.

When survey respondents were asked about the significance of autonomous core network transformation to their company, 93% indicated that it is either important or very important, with 43% selecting the latter (**Figure 2**).

Figure 2: The importance of autonomous core network transformation to CSPs



Source: Omdia

CSPs' drivers to deploy AI and autonomous core networks

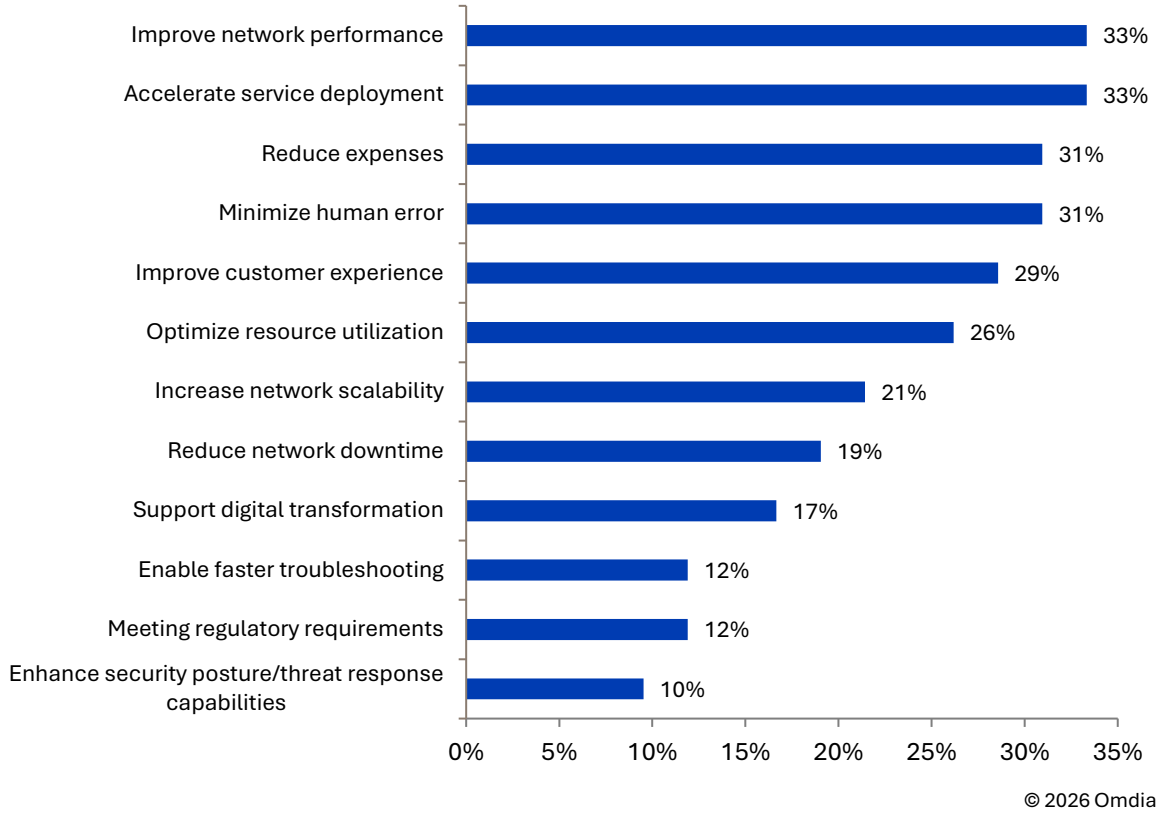
The top three drivers for autonomous core network investment are improved network performance and reliability, accelerated service deployment, and reduced operational costs and complexity.

Improved network performance is considered the top driver by 33% of respondents. This suggests that CSPs have set their sights on deploying and monetizing complex use cases with stringent network requirements to address consumer, enterprise, and mission-critical requirements. Some examples of these use cases are high-quality gaming, autonomous robots, remote inspection with drones, and disaster recovery. AI will help CSPs improve network reliability and deliver the deterministic performance, service assurance, and SLA adherence needed for these use cases.

Given the highly competitive nature of the markets they are playing in, it is no surprise that—according to 33% of respondents—accelerated service deployment is considered important. Autonomous core networks will leverage intent-based automation, zero-touch provisioning, and closed-loop LCM to help CSPs improve customer experience (according

to 29% of respondents) and optimize the resource utilization (according to 26%) needed to launch complex offerings, such as network slicing or private 5G (**Figure 3**).

Figure 3: The business outcomes driving CSPs' autonomous core network investments



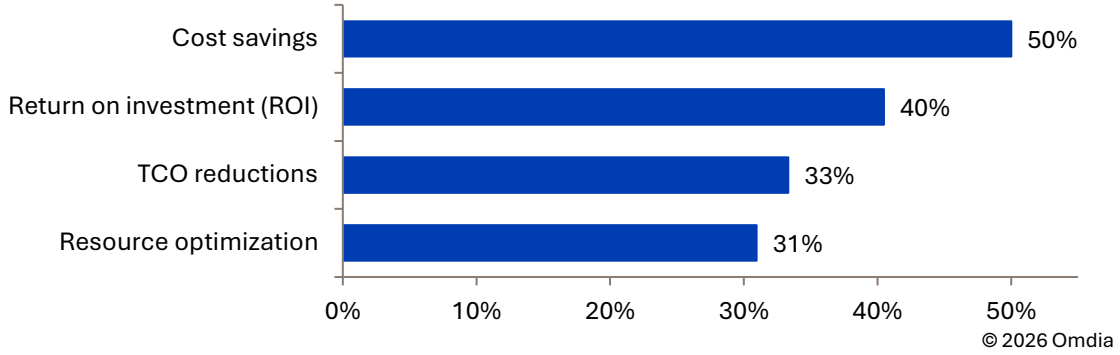
Source: Omdia

CSPs must define how to measure autonomous core networks' initiative benefits

The next question, about how CSPs will measure the success of their autonomous core transformation, was divided into three metric segments: financial, operational, and strategic. The top three quantifiable outcomes that responders selected in the financial metrics were cost savings (50%), ROI (40%), and total cost of ownership (33%) (**Figure 4**).

While cost savings remain a priority for CSPs, ROI is another key financial metric for autonomous core network initiatives, due to its direct connection to business value. It drives benefits as CSPs strive to reduce operational expenses through automation and enhance customer satisfaction and retention through improved service quality.

Figure 4: CSPs' measure of success from autonomous core network's initiatives—financial metrics

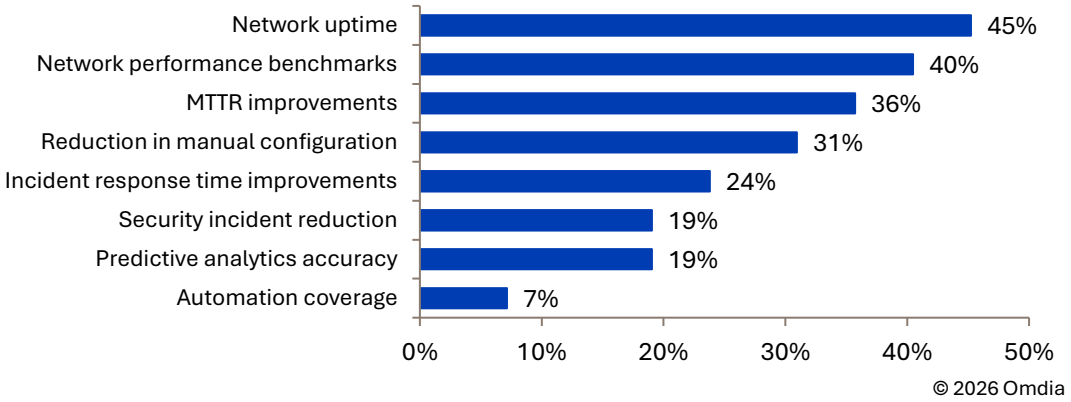


Source: Omdia

While financial metrics remain a priority, there is a direct correlation between some of the financial benefits and operational benefits, such as the reduction in manual configuration having a direct positive impact on cost.

Further, it is noteworthy that 45% of respondents have emphasized network uptime as the top operational outcome, as it directly represents the reliability and resilience of the network. Autonomous core networks are built to reduce human intervention, anticipate and prevent failures, and self-heal when issues arise. High uptime serves as a strong indicator that these capabilities are functioning as intended, ensuring consistent service availability for customers and minimizing the impact of costly outages. Network performance benchmarks and mean time to resolution (MTTR) improvements were selected as the top two and three outcomes by 40% and 36% of respondents, respectively (**Figure 5**).

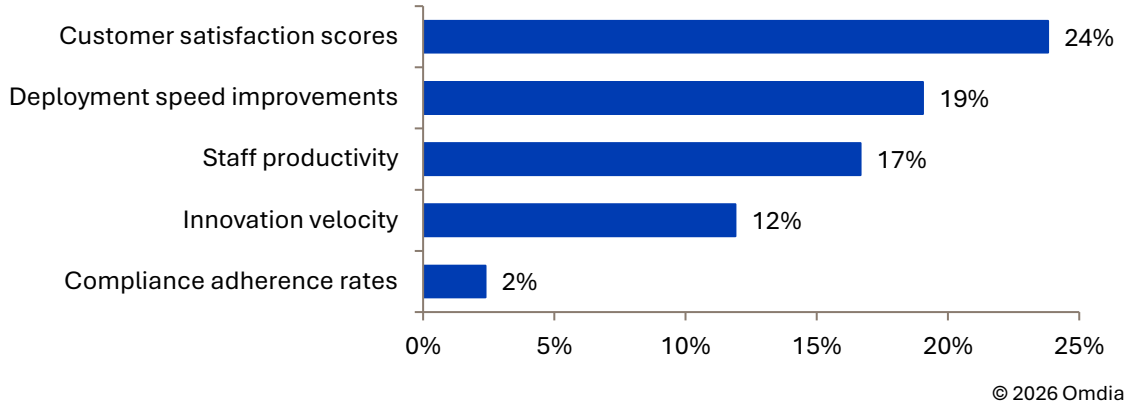
Figure 5: CSPs' measure of success from autonomous core network's initiatives—operational metrics



Source: Omdia

Strategic metrics are a measure of how successful the CSPs' business is beyond just daily operational checks. These metrics are used by the leadership team to gauge the overall success of a business strategy, such as autonomous core network migration. Customer satisfaction scores, deployment speed improvements, and staff productivity were the top three outcomes among the strategic metrics, according to 24%, 19%, and 17% of respondents, respectively (**Figure 6**).

Figure 6: CSPs' measure of success from autonomous core network's initiatives—strategic metrics

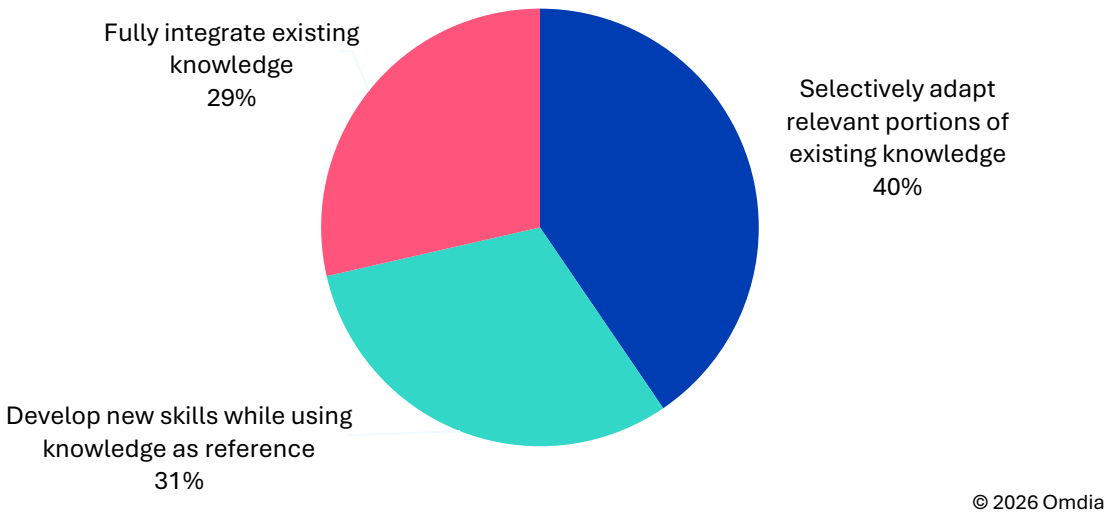


Source: Omdia

As CSPs transition toward autonomous core network operations, incorporating concrete frameworks, such as management, orchestration, analytics, and closed-loop automation, will be essential. CSPs must establish a strategy to integrate engineers with networking and operations know-how, including existing 3GPP and European Telecommunications Standards Institute (ETSI) telecom knowledge, into the new AI/data-driven operations structure. There is also a need to align these with established industry standards and ensure interoperability and consistent operations.

When surveyed, most respondents (40%) indicated that they would selectively adapt portions of existing knowledge (i.e., the engineering know-how) to fit the new organizational structure. Opinions about the other two categories were mixed, with 31% suggesting that new skills would be developed while using existing knowledge as a reference and 29% advocating for fully integrating existing knowledge into the new approach (**Figure 7**).

Figure 7: Integration of 3GPP/ETSI know-how as CSPs transition to autonomous core network operations



Source: Omdia

Key service provider segments

In this section, we summarize the five key service provider segments we have identified and used to structure our research. In the next section of this report, we will benchmark some of the survey questions across these CSPs and discuss how this impacts the choices that need to be made.

Segment 1: Players with a large home market that are also present in multiple geographies (e.g., AT&T, Orange, Telefónica)

Large international players are driving significant advancements in network technology, such as virtualization and migration to cloud native, while investing heavily in business process systems such as AI and analytics, as well as agile and automated operations. Their leadership in these areas is largely attributed to their scale and the extensive resources at their disposal. Additionally, organizations working across multiple operating companies are increasingly focused on standardizing resources across these companies to enhance efficiency and streamline processes.

Segment 2: Large national players with some international investments (e.g., China Unicom, Telecom Italia)

Large national players are prioritizing network technology changes, though their approach is generally less transformative compared to large international players. Segment 2 players share a strong focus on network technology evolution and enhanced customer engagement, similar to Segment 1 players. However, they place greater emphasis on launching new digital services, accelerating time to market, and adopting more agile operating models. This focus is driven in part by their need to catch up with internet cloud providers and leading international operators.

Segment 3: Smaller national players with limited international investments (e.g., Telia, Telstra, TELUS)

Smaller national players are prioritizing network technology upgrades and enhanced operational efficiency. They share some similarities with Segment 2 players, particularly in their focus on adopting more agile operating models. For smaller service providers, customer experience-driven investment and transformation are especially critical. As a result, their investment priorities often include automating business support systems and call center processes. Unlike Segment 1 players, Segment 3 players typically lack the budget and resources to conduct the numerous trials that larger players can afford.

Segment 4: Mobile-first players (e.g., Globe, Airtel, Safaricom)

Mobile-first players place a strong focus on improving customer engagement and enhancing the customer experience as well as on automation, which enables them to optimize operations, reduce costs, and improve service delivery. This includes automating processes in areas such as billing, customer support, and network management. At the same time, like players in other segments, agile operating models have become an increasingly important priority for them.

Segment 5: Smaller national, niche, and virtualized players (e.g., Elisa)

Smaller niche players focus less on network technology and instead concentrate their investments on technologies that deliver the most competitive advantage, such as automation and AI-driven analytics tools. Their primary focus is on carving out a niche by providing specialized services, including tailored solutions designed for specific industries, communities, or demographic groups.

Key actions for CSPs to reach Level 4 in core networks

This section outlines the five key areas where CSPs are driving organizational and operational changes to enhance skills and competencies. It also focuses on understanding the future job roles and investment priorities that are essential for implementing autonomous core networks.

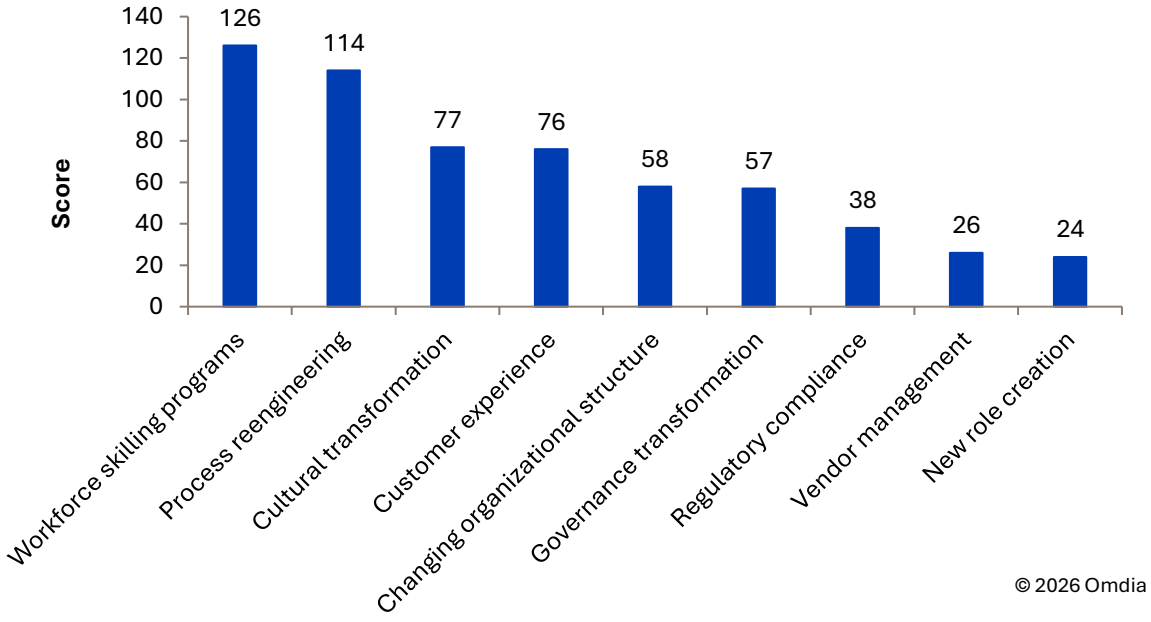
Organizational impact: CSPs' workforce skilling programs, process reengineering, and cultural transformations are the top three priorities

The autonomous core networks transformation is a significant undertaking, as it demands substantial changes to the operating model by breaking down silos and fostering closer collaboration between departments. This shift will also have a profound impact on the workforce and organizational culture, requiring CSP employees to transition from performing repetitive, manual tasks to taking on roles focused on oversight and governance so they can ensure the effective performance of automated systems.

When survey respondents were asked to rank the most essential organizational transformations on a scale of 1 to 5 (with 1 as the most essential), workforce skilling programs emerged as the top priority. Respondents recognized that the success of the transformation hinges on prioritizing the development of new competencies in AI/ML, data analytics, and automated network management. Following closely, process reengineering and cultural transformation were ranked as the second and third most critical areas for organizational change.

Process reengineering is essential for implementing autonomous core networks due to the introduction of advanced AI and automation. Operating in this environment will differ significantly from traditional silo-based processes designed for manual intervention. In this new paradigm, intent-based operations—where business intent is translated into network actions—along with real-time and closed-loop control, will enable autonomous core networks to function with continuous monitoring and self-healing capabilities (**Figure 8**).

Figure 8: The most essential organizational transformations for CSPs when implementing Level 4 autonomous core networks



Source: Omdia

Adoption of Level 4 autonomous core networks will have a considerable impact on CSPs' various departments, such as planning and engineering, operations and assurance, and optimization teams.

For the planning and engineering department, the tasks will be less about specifying the technical "how" steps, such as configuring the router protocols or setting up the quality of service rules for specific interfaces, but rather about defining the "what," that is, the business intent that the customer or a service requires.

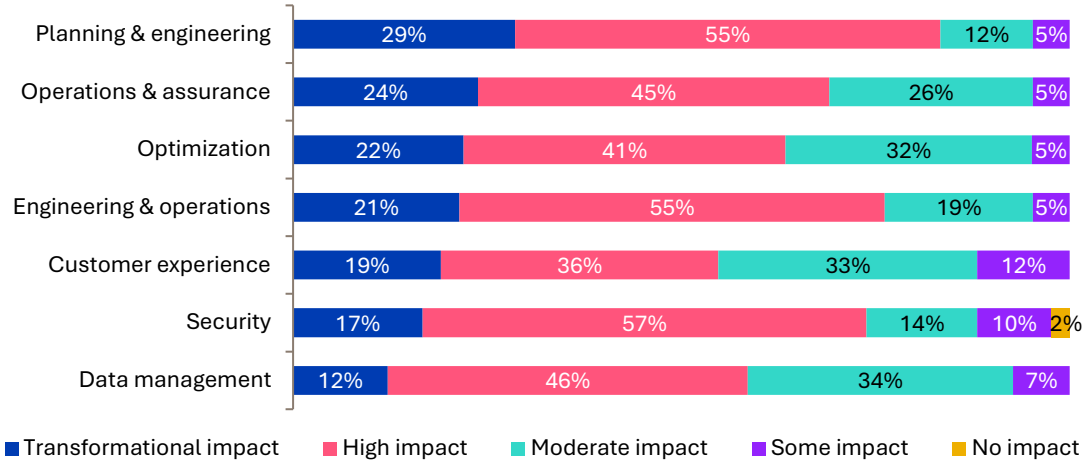
Planning and engineering teams must work more closely with operations and assurance because autonomy erases the traditional boundaries between design and execution. Autonomous core networks rely on closed-loop automation—a core principle that sets them apart from traditional automation. For these loops to function effectively, they need real-time performance insights from assurance systems. As a result, planning can no longer be a one-time activity; it must become a continuous, adaptive process.

When asked, 29% of survey respondents said that Level 4 autonomous core network adoption will have a transformational impact on the planning and engineering department, while 55% of respondents said it will have a high impact. This pattern is also closely followed by the second category: operations and assurance.

The impact that CSPs' security department will experience with its ability to collaborate across the organization due to Level 4 autonomous core network adoption will be high, according to 57% of respondents. This shift will require security teams to transition from reactive collaboration to proactive integration within the automation framework. They will need to work more effectively with development and testing teams while ensuring that security policies are seamlessly embedded into the network's automated processes.

It is interesting to note that 55% of respondents said the impact of Level 4/5 autonomous core network adoption on both planning and engineering—the future design and build-out of the network and engineering/operations—regarding current ongoing deployments and maintenance will be high (**Figure 9**).

Figure 9: The impact that each CSP department will experience with their ability to collaborate across the organization due to Level 4 autonomous core network adoption



Source: Omdia

When comparing CSP segments in terms of which departments will experience the most transformational impact, it is unsurprising that respondents from mobile-first CSPs anticipate significant changes across four key areas: planning and engineering, optimization, engineering and operations, and customer experience. This is because achieving Level 4 autonomous core networks will necessitate a complete reinvention of how mobile infrastructure is designed and managed. For the optimization department, the adoption of autonomous core networks will replace frequent manual and periodic tasks with real-time, AI-driven, closed-loop control.

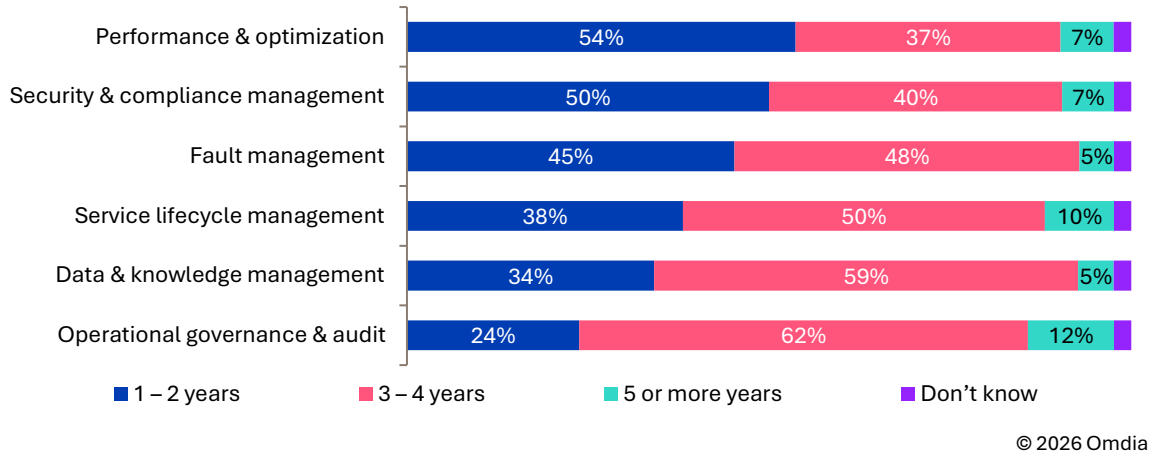
Operational changes: Building on low-hanging fruit use cases while planning for more complex ones

When asked about the expected timeframes for different use cases to reach Level 4 autonomous core networks, respondents identified the top three most likely to achieve this within one to two years as: performance and optimization (54%), security and compliance management (50%), and fault management (45%).

The accelerated progress of these use cases is largely driven by their high priority and the need to process massive volumes of data—particularly in performance and optimization, where extensive analysis is required. Similarly, security and compliance management remain a top priority for many CSPs due to the growing scale and sophistication of modern cyber threats. Addressing these challenges increasingly demands AI-driven tools, as manual approaches are no longer sufficient (**Figure 10**).

Conversely, the survey results indicate that operational governance and audit is the use case that most respondents (62%) believe will take three to four years to reach Level 4. Data and knowledge management was another example, cited by 59% of respondents. The primary reasons for this slower progress include the need for extensive cross-organizational collaboration and significant accountability transformations, both of which require more time to implement.

Figure 10: CSP plans to reach Level 4 autonomous core networks for use cases



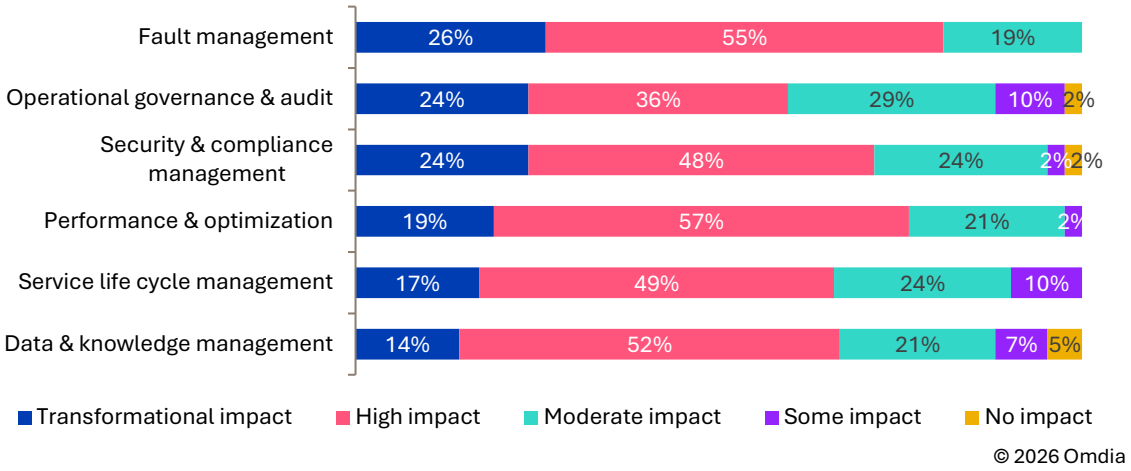
Source: Omdia

CSP respondents anticipate varying levels of impact from Level 4 autonomous core in transforming processes from manual operations to self-managed systems, with high impact being identified as the most significant. The top three processes expected to have

high impacts are performance and optimization (57%), fault management (55%), and data and knowledge management (52%).

This indicates that these processes will function entirely without manual intervention, with human roles shifting to intent validation and overseeing the management of automated exceptions that may occur (**Figure 11**).

Figure 11: The Level 4 autonomous core impact in transforming manual processes into self-managed systems



Source: Omdia

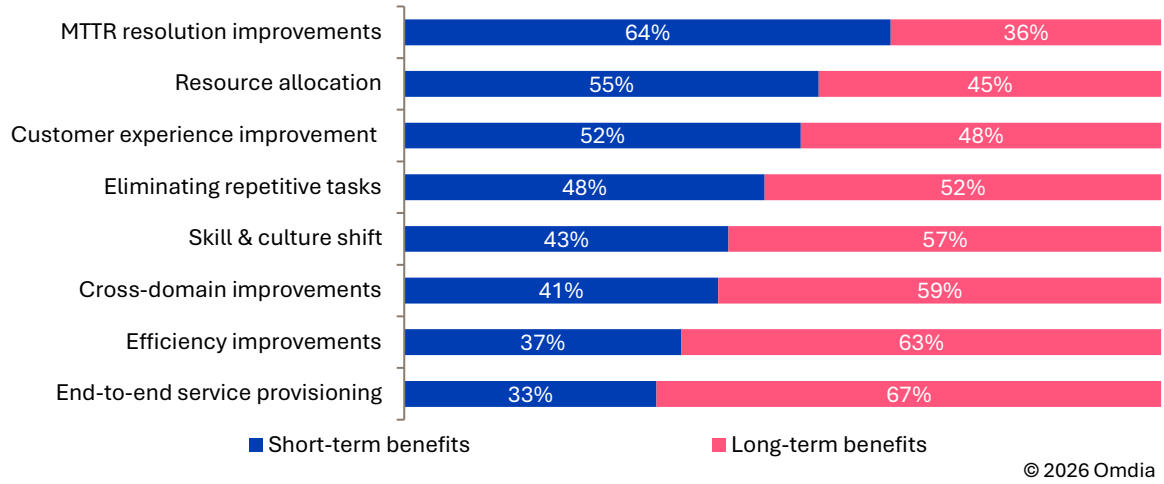
As CSPs plan their migration to Level 4 autonomous core networks, the top three operational areas considered by the respondents where they expect short-term benefits are MTTR (64%), resource allocation (55%), and customer experience improvement (52%).

In a competitive market, CSPs must prioritize minimizing network downtime, as measured by MTTR, not only as an operational objective but also as a key customer retention strategy. A Level 4 autonomous network offers significant advantages, including automated fault detection, RCA, and self-healing capabilities.

With the increasing architectural and service complexity of modern networks, manual provisioning and orchestration are no longer scalable. Real-time monitoring will be essential to ensure customers and devices consistently receive the required network key performance indicators. Additionally, resource allocation will greatly benefit from the automation introduced by Level 4 autonomous networks. CSPs will aim to automate this process as quickly as possible to stay competitive.

Conversely, end-to-end service provisioning will necessitate automation across domains beyond the core network, requiring these domains to also achieve Level 4. Due to the inherent complexity, this will be a longer-term process (**Figure 12**).

Figure 12: Timeframe CSPs expect to realize benefits once they migrate to Level 4 autonomous core networks



Source: Omdia

Regional differences are evident in CSP priorities. While North America closely aligns with the global perspective, Europe's top three short-term goals are reducing MTTR, improving customer experience, and eliminating repetitive tasks, all at 80%. In contrast, Asia & Oceania prioritize resource allocation (100%), MTTR reduction (67%), and cross-domain improvements (67%).

Skills and competencies: CSPs need less than 24 months to develop the key skills

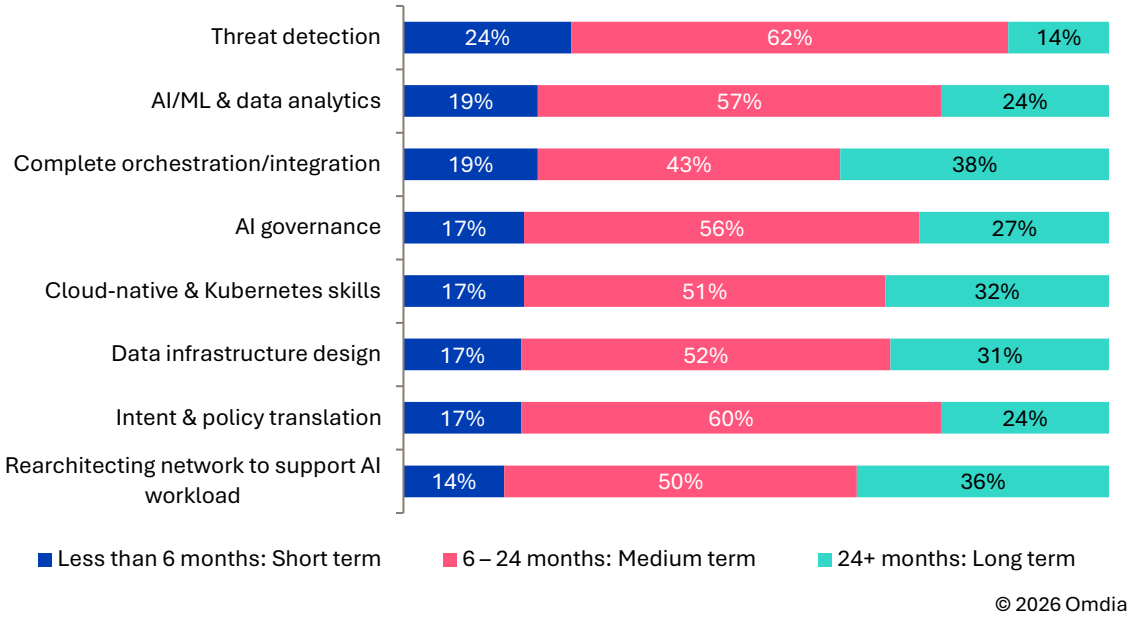
To fully leverage the capabilities of Level 4 autonomous core networks, CSPs must focus on developing both technical and soft skills. While some of these skills are more challenging to cultivate, respondents indicated that most technical skills could likely be developed within 6 to 24 months.

It should also be noted that there are no clear starting and ending points for these skill sets, and it is also not about moving from 0% skills to 100% skills in 6 to 24 months. Further, CSPs may already possess some of these skill sets, while skills acquisition will also probably be a long-term continuous process.

When asked about the time frame for staff to acquire key technical skills, 24% of survey respondents identified threat detection as the highest-priority skill to be developed in the shortest time. Both AI/ML data analytics and complete orchestration/integration skills were selected as second and third technical skills that could be developed in less than six months, according to 19% of respondents.

Threat detection was the skill set most frequently identified by respondents as falling within the 6- to 24-month development timeframe. Additionally, intent and policy translation (60%) and AI/ML data analytics (57%) ranked among the top three skills prioritized for development (**Figure 13**).

Figure 13: Time frame CSPs' staff are expected to develop technical skills for Level 4 autonomous core networks

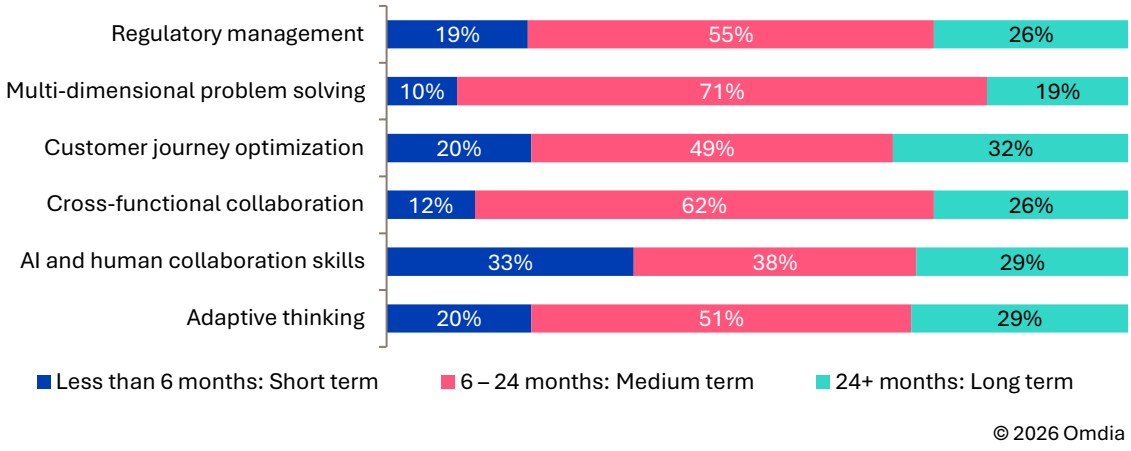


Source: Omdia

Similarly, most CSP respondents believe that developing key soft skills will be essential within the next 6 to 24 months. According to the survey, 71% of respondents highlighted multidimensional problem solving—the ability to diagnose faults that AI and automation tools cannot resolve—as the top skill CSPs will need to develop in the next 6 to 24 months.

Cross-functional collaboration (62%), which involves working seamlessly with software developers, business owners, and data scientists to translate high-level business intent into autonomous core network policies, and regulatory management (55%) were also in the top three soft skills CSPs will need to prioritize during this period (**Figure 14**).

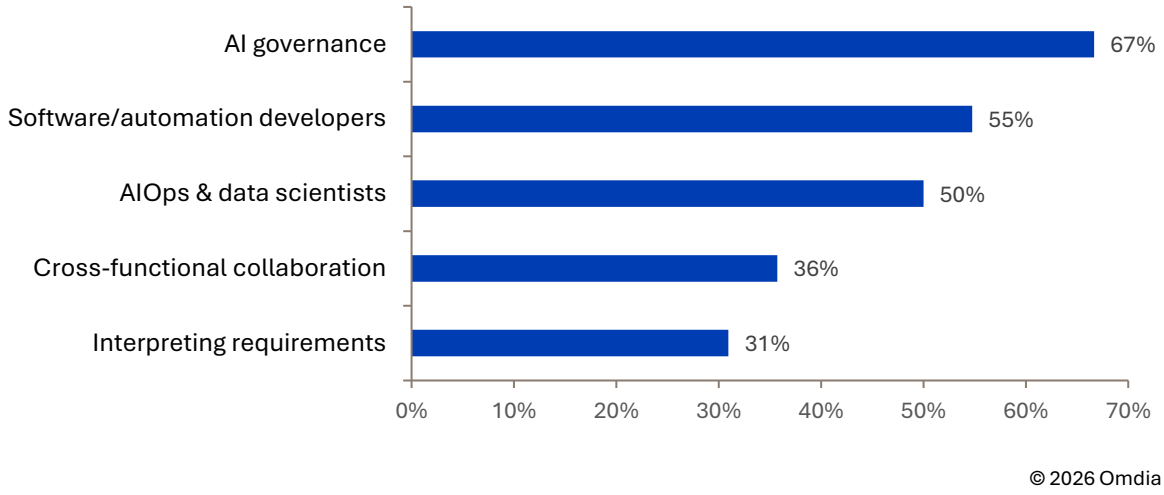
Figure 14: Time frame CSPs' staff are expected to develop soft skills for Level 4 autonomous core networks



Source: Omdia

AI governance—a role focused on validating, debugging, and ensuring the trust, ethics, and explainability of AI operations (AIOps) models making closed-loop decisions—was identified as the top skill by 67% of respondents. The other key roles CSPs must fill within the next two years, often through external hires, include software and automation developers (55%) and AIOps and data scientists (50%) (**Figure 15**).

Figure 15: CSPs' skill gaps that need to be filled in the next two years



Source: Omdia

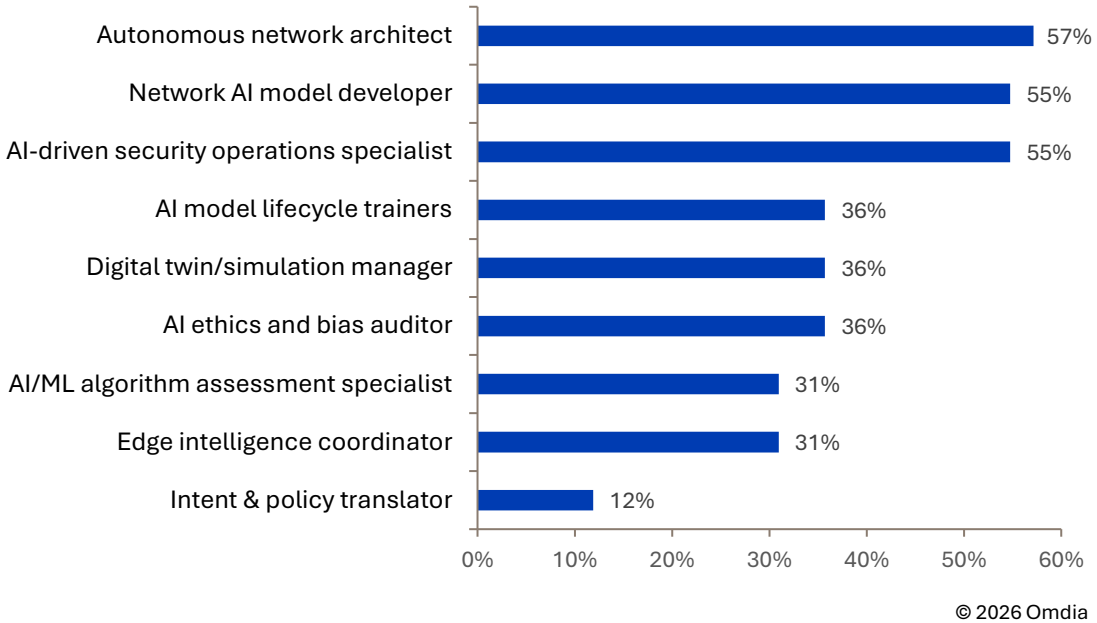
Future job roles and career paths: Autonomous network architects, AI model developers, and security operations specialists are the top three positions CSPs will invest in over the next three to five years

Designing, building, and operating autonomous core networks is a highly complex process, requiring CSPs' staff to possess the necessary expertise to manage this transformation effectively. Key responsibilities for this role include defining blueprints, ensuring compliance with standards such as ETSI's Zero Touch Service Management, implementing closed-loop automation, and establishing policies for intent-based networking. The survey revealed that 57% of respondents identified autonomous core network architects as the top role CSPs plan to establish or invest in.

The other positions within the top three are network AI model developers and AI-driven security operations specialists, according to 55% of respondents.

Although the intent and policy translator role ranked last among the categories identified by respondents, it remains critically important in enabling the shift from manual, network element-based management to intent-based networking. This role plays a key part in abstracting and decomposing the "what" of network requests and leveraging policy generation to translate them into the "how," supported by a comprehensive set of technical rules (**Figure 16**).

Figure 16: The positions CSPs expect to establish in the next three to five years



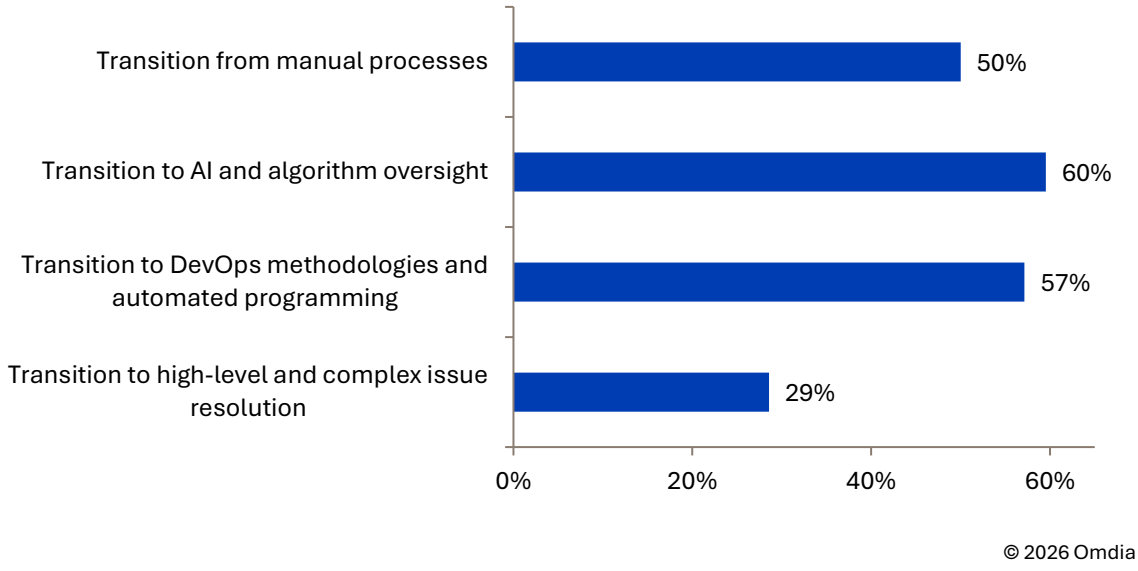
Source: Omdia

According to 60% of survey respondents, one of the most significant changes in network operations staff responsibilities is the shift toward overseeing AI and algorithms. This transition is ranked as the top change in responsibility, as CSPs must ensure that AI systems provide accurate hallucination-free recommendations while progressing toward autonomous core networks at Level 4. Safeguarding against potential issues is critical, as it prevents network outages caused by incorrect optimization, mitigates security risks such as the misinterpretation of fake data injected by malicious actors, and avoids regulatory fines due to privacy violations, such as non-compliance with General Data Protection Regulation (GDPR) standards.

The transition to DevOps methodologies and automated build, test, and deploy is identified as the second most significant change, according to 57% of respondents. Nonetheless, DevOps is not a new concept in the telecom industry. It originated in the broader IT/software world and was adopted by telecom during the shift from virtualization to cloud-native environments, driven by the need for automation tools such as continuous integration and continuous delivery.

DevOps methodologies also closely align with closed-loop automation and continuous updates, which autonomous networks require. The journey, however, has been challenging, and CSPs must continue to integrate software development with IT operations to fully realize its benefits (**Figure 17**).

Figure 17: Changes in network operations people's responsibilities in the next one to two years



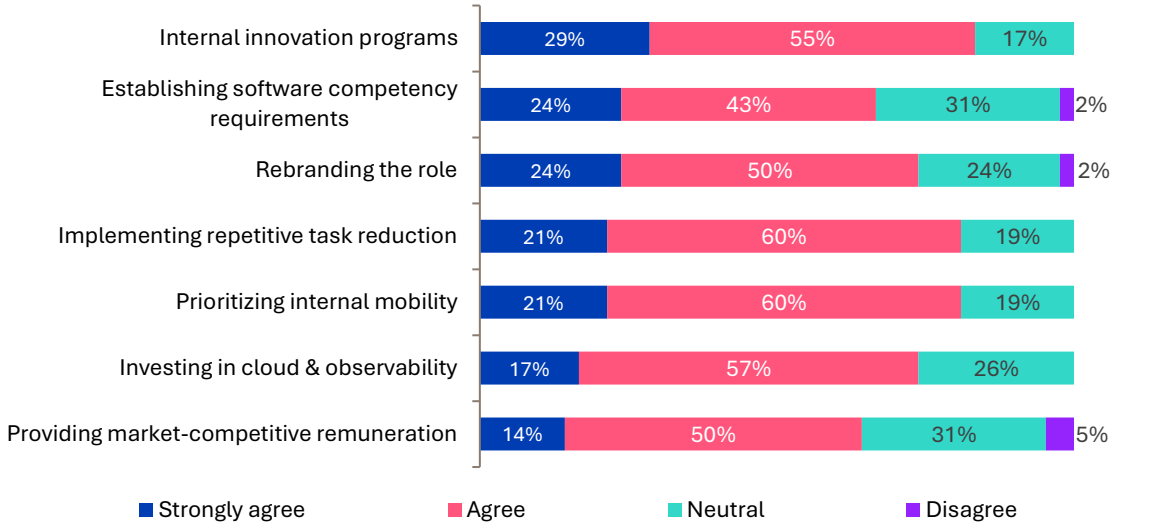
Source: Omdia

As stated before, the journey to Level 4 autonomous core networks will involve significant staff reskilling in software and AI tools, and yet, given the market competition for these skills, CSPs must ensure that as the new network operations' career tracks are developed, they remain attractive to the staff.

When asked about strategies for transforming network operations into an attractive career path, 60% of respondents—the largest share—agreed that reducing repetitive tasks and prioritizing internal mobility would be the most effective approaches. Eliminating repetitive tasks allows staff to focus on more innovative and engaging work, while emphasizing internal mobility creates formal career pathways, enabling operations staff to advance into specialized roles such as data science, network architecture design, and automation development.

Additional strategies include investing in the cloud and observability, offering market-competitive remuneration, and rebranding the role, which were supported by 57%, 50%, and 50% of respondents, respectively. These approaches aim to ensure that operations staff feel engaged, valued, and motivated in their roles (**Figure 18**).

Figure 18: Success in transforming network operations roles into desirable career tracks



Source: Omdia

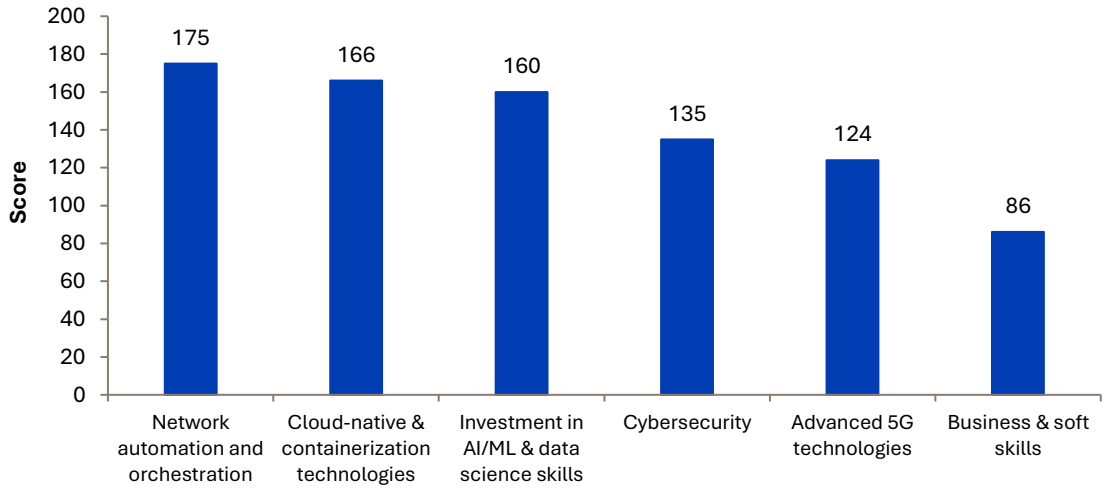
Investment priorities: Network automation and orchestration skill-building is the highest priority

CSPs must invest in reskilling the staff to get the most out of their autonomous core network implementation. When survey respondents were asked to rank from one to five, with one as the highest priority, which skill-building activities are the most important for achieving autonomous core network implementation, network automation and orchestration received the highest ranking, followed by cloud-native and containerization technologies and investment in AI/ML and data science skills.

Network automation involves replacing error-prone, repetitive tasks with automated processes to ensure proper configuration, efficient management, and optimal network performance. Additionally, orchestration focuses on reducing human intervention by coordinating multi-domain network components through an end-to-end service orchestrator. The closed-loop automation process combines automation and orchestration to dynamically adjust configurations and implement changes based on real-time network data. The combination of automation and orchestration is one of the pillars of autonomous core networks.

Interestingly, the investment in AI/ML and data science skills is ranked third. However, this does not diminish the importance of these activities, given that developing the right data set for AI/ML tools is another pillar of autonomous core networks (**Figure 19**).

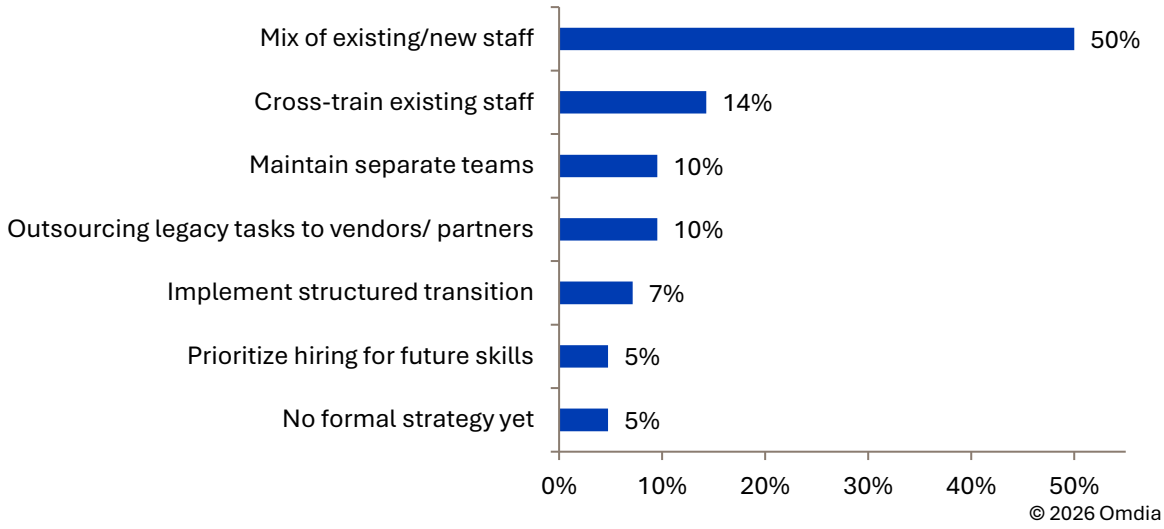
Figure 19: The skill-building activities with the highest priority to achieve Level 4 autonomous core network implementation



Source: Omdia

On the transformation journey to Level 4 autonomous core networks, CSPs must ensure the right skills mix is developed or hired as previously described. However, CSPs must also have a strategy for the existing staff with network experience. According to the survey, 50% of respondents believe that CSPs must ensure a mix of existing and new staff hires (**Figure 20**).

Figure 20: CSPs' strategies for balancing legacy expertise with future-oriented skill developments



Source: Omdia

Conclusions

The journey toward autonomous core networks is not merely an evolution of technology—it is a fundamental transformation of how CSPs design, operate, and monetize their networks. As highlighted throughout this report, the complexity of modern mobile networks, driven by 5G adoption, IoT proliferation, and multilayered architectures, has made manual operations unsustainable. CSPs must embrace AI-driven automation and intent-based networking to achieve operational efficiency, resilience, and scalability.

Omdia's CSP survey findings underscore the urgency of this transformation: 93% of CSPs consider autonomous core networks to be important or very important, with the top drivers including improved network performance, accelerated service deployment, and cost reduction. These priorities reflect the competitive pressures CSPs face and the need to deliver differentiated capabilities, such as network slicing, and develop use cases to address consumer, enterprise, and mission-critical use cases with stringent requirements.

However, technology alone will not deliver autonomy. Organizational readiness—through workforce reskilling, cultural change, and process reengineering—is equally critical. CSPs need less than 24 months to develop key technical skills in intent and policy translation, AI/ML, and cloud-native technologies, alongside soft skills such as cross-functional collaboration and multidimensional problem solving. New roles, including autonomous core network architects and AI governance specialists, will become central to operations, ensuring trust, compliance, and ethical AI decision-making.

The benefits of Level 4 autonomy are clear: reduced MTTR, improved resource allocation, and enhanced customer experience. Yet, CSPs must balance short-term wins with long-term goals, such as cross-domain orchestration and end-to-end service automation. Success will depend on strategic investment in automation, orchestration, and AI capabilities, coupled with governance frameworks that safeguard reliability and security.

In conclusion, autonomous core networks represent a strategic imperative for CSPs seeking to thrive in an era of hyper-connectivity and digital innovation. Those that act decisively—aligning technology, talent, and organizational transformation—will unlock new monetization opportunities, deliver superior customer experiences, and position themselves as leaders in the next generation of telecom networks.

This Omdia White Paper was commissioned by Ericsson

Appendix

Further reading

Core Market Tracker – 3Q25 Analysis December 2025)

Core Market Tracker – 3Q25 Data December 2025)

2026 Trends to Watch: Core Networks (October 2025)

Blockchain Technology and Adoption Trends (December 2019)

"Blockchain is good for more than just Bitcoin," (September 2019)

Roberto Kompany, Principal Analyst, Mobile Infrastructure
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Get in touch

www.omdia.com
askananalyst@omdia.com

Copyright notice and disclaimer