Mission-critical networks demand more: Rethink your OSS and BSS

The Playbook for Critical Communications Operators

Authors: Ildefonso de la Cruz and Roz Roseboro

May 2026

In partnership with:

ERICSSON

This Omdia White Paper was commissioned by Ericsson.

Contents

This Omdia White Paper was commissioned by Ericsson.

"The next billion-dollar growth engine for CSPs is the digitalization of mission-critical verticals, and a modern OSS and BSS solution is the key to unlock it."

Executive summary

Source: Omdia

Mission-critical verticals are undergoing rapid digital evolution, driven by the need for more advanced, data-rich applications. The true enabler of this transformation is the adoption of broadband technology. As public safety agencies, railway operators, utilities, and defense units modernize their communications systems, their traditional network architecture and governance are also being reshaped. Where they once operated in isolation, they are now assessing the move towards collaborative ecosystems. That said, the choice of the right partner depends on who can deliver uncompromising reliability, availability, security, and operational efficiency.

In this new environment, modern operations support systems (OSS) and business support systems (BSS) solutions become essential. They are the key to sustaining mission-critical performance through lifecycle management, service assurance, and a wide range of operational functions that ensure these next-generation critical communications networks remain resilient.

Key takeaways

- Critical communications operators are shifting from narrowband to broadband to enhance end-users' situational awareness, automation, and enable new digital use cases such as real-time video and IoT telemetry.
- OSS/BSS modernization is essential to guarantee the stringent requirements of mission-critical operations.
- Communication service providers (CSPs) can unlock a multi-billion-dollar market opportunity by enabling tailored connectivity reliability, managed services, and vertical-specific digital solutions.
- Each vertical has unique drivers, challenges, and adoption paths. All require advanced OSS and BSS to ensure service quality, resilience, and security.
- Critical communication operators and CSPs must adopt a mission-critical-grade OSS and BSS blueprint that includes automation, AI-driven assurance, zero-trust security, and flexible service orchestration.

This Omdia White Paper was commissioned by Ericsson.

Introduction

Mission-critical communication forms the invisible backbone of our society. These systems ensure firefighters can coordinate inside a burning building, that soldiers can communicate securely in contested environments, that electricity grids remain stable during storms, and that trains move safely across national rail networks. They are built on principles of maximum reliability, effectiveness, and security, since the consequences of their disruption or failure would ripple far beyond inconvenience: public protection would be compromised, essential services disrupted, and national security could be put at risk. The focus of this report is on the following mission-critical verticals:

- **Public safety:** Emergency response, law enforcement, fire and rescue, and crisis management systems for public protection and disaster relief
- **Defense:** All military command, intelligence, and security systems that protect national sovereignty and territorial integrity
- **Utilities:** Power generation, transmission, and distribution systems that provide essential energy and supply water to society
- **Rail**: Train transport systems to enable the movement of people and goods

For decades, these organizations in mission-critical verticals have relied on highly specialized narrowband technologies for their communications. These systems were engineered with a singular purpose: to provide reliable, secure voice communication under any circumstance, and they have served society well. However, the world around them has changed; emergencies are more complex and frequent, infrastructure is more interconnected, and operational environments demand richer, faster, and more intelligent information flows. Consequently, these critical sovereign verticals are undergoing a comprehensive digital transformation fueled by innovative advancements in connectivity, their increasing requirements for digitalization, and ambitious automation goals.

This Omdia White Paper was commissioned by Ericsson.

The trends driving the evolution of mission-critical systems

Critical communications operators are specialized organizations—either dedicated government agencies, vertical teams, or specialized service providers—tasked with delivering resilient communication networks essential for public safety, emergency response, national security, and vital vertical operations.

Their technology transformation journey towards the adoption of mission-critical broadband networks is framed in a set of foundational principles that must be consistently upheld to meet the stringent demands of these vertical end-users.

Figure 1: The six foundational pillars supporting mission-critical communications systems

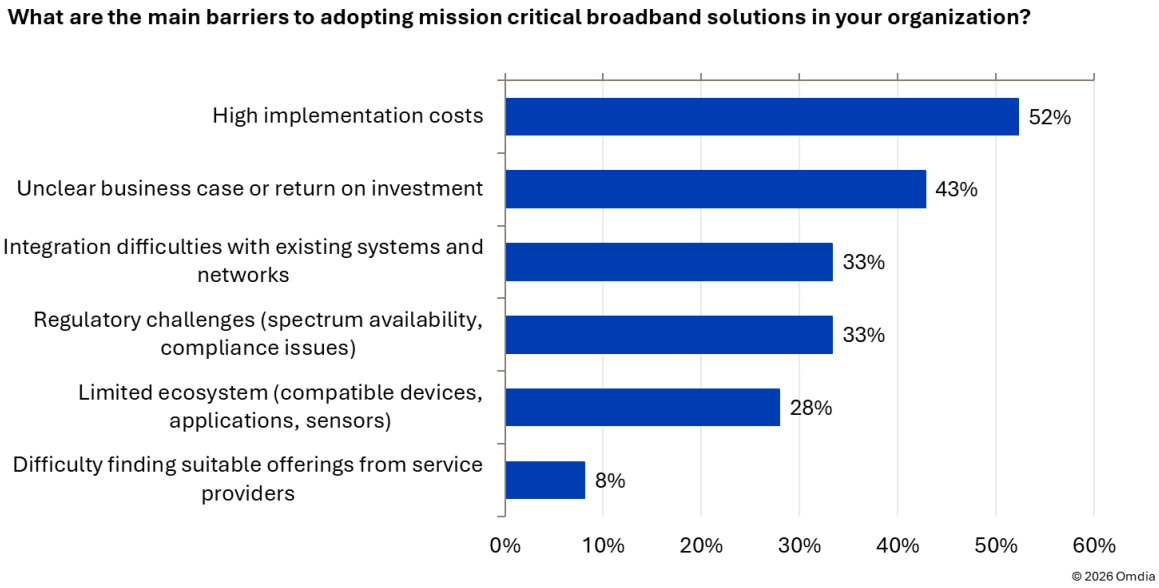
Source: Omdia

This Omdia White Paper was commissioned by Ericsson.

A growing market and strategic opportunity for CSPs

Omdia's survey data (**Figure 2**) shows that, although critical communication operators are eager to ramp up investments in mission-critical broadband, they increasingly recognize that building and operating their own broadband networks can be costly, complex, and—in some cases—unsustainable.

Figure 2: The main barriers in the adoption of broadband solutions by critical communication operators



Source: Omdia

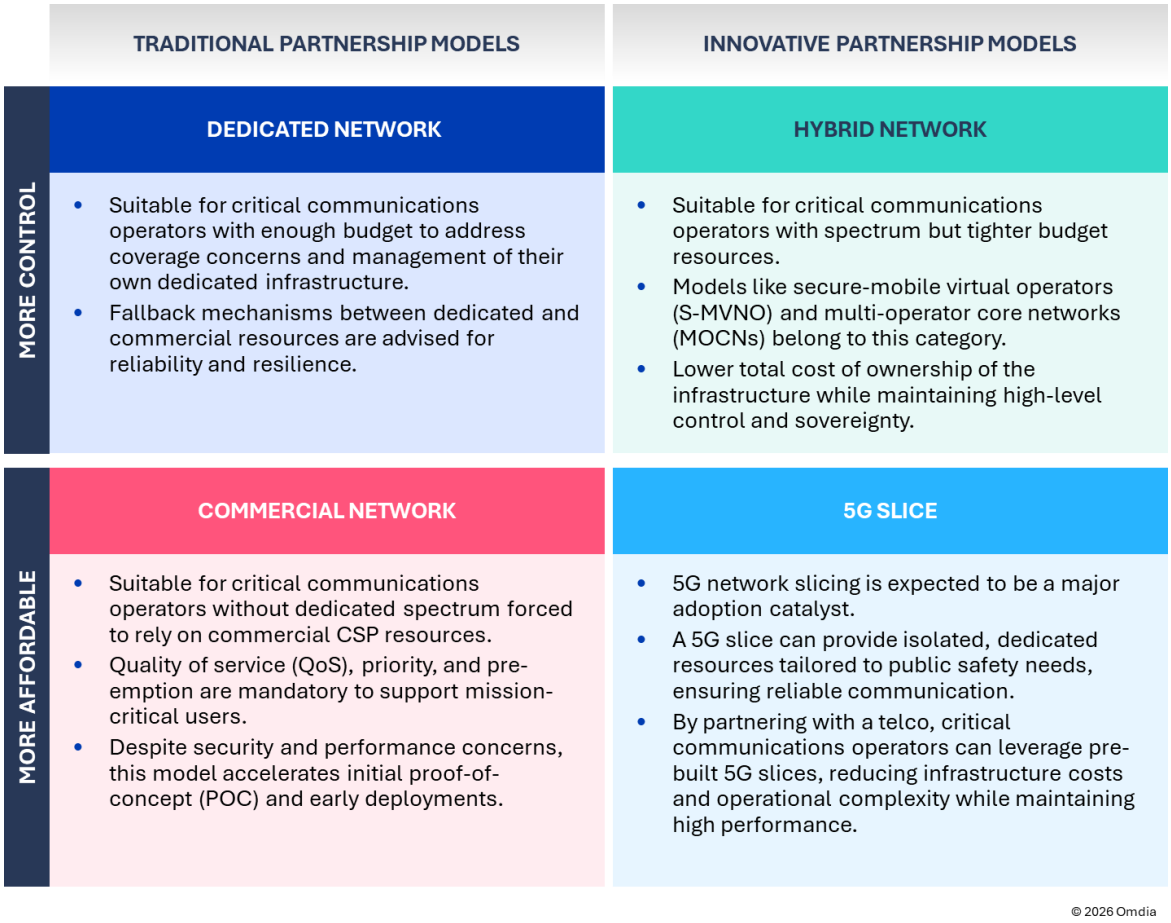
As these concerns intensify, the traditional models of running fully independent, self-contained networks are being evaluated. Critical communications operators are assessing partnership models that help manage the rising complexity and cost of connectivity, and increasingly, extend these partnerships into their services, innovative applications, and advanced digital solutions.

This transformation is opening a significant opportunity for CSPs to step up and become the indispensable partner of these organizations with mission-critical requirements and effectively become enablers of their digitalization journey.

The collaboration between CSPs and critical communications operators does not follow a single formula. Instead, a range of innovative public-private partnership models coexist, with traditional ones for critical broadband adoption, as shown in **Figure 3** (on the next page).

This Omdia White Paper was commissioned by Ericsson.

Figure 3: Public-private partnership models for critical broadband adoption



Source: Omdia

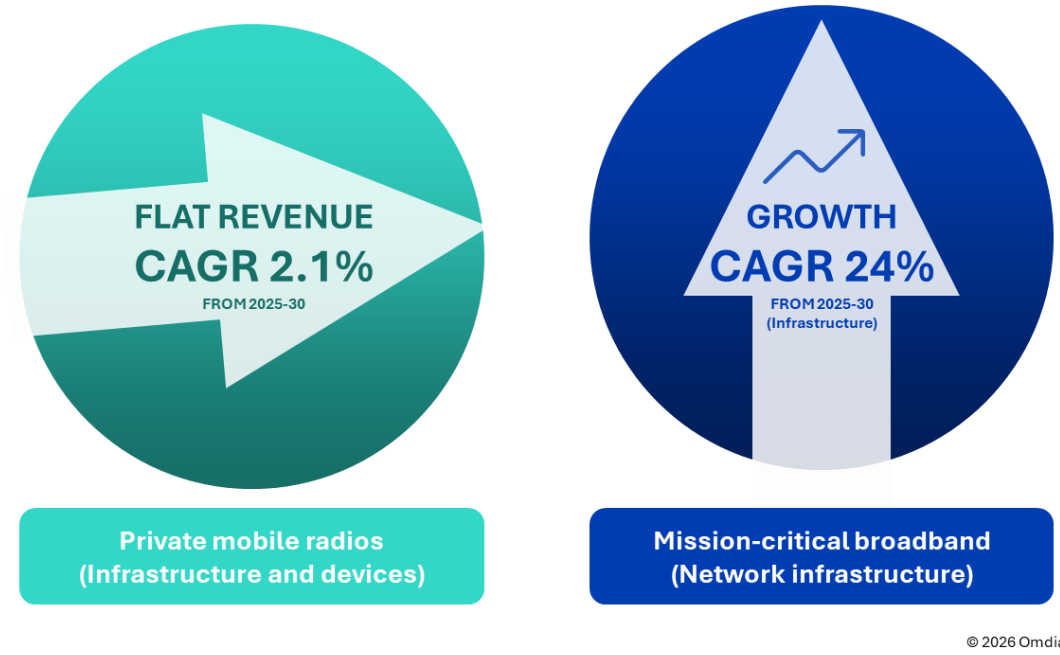
The mission-critical evolution unlocks new market opportunities

The evolution of mission-critical communications represents a layered opportunity rather than an immediate replacement cycle. In the near term, the market opportunity is anchored in the continuation and enhancement of incumbent critical solutions.

Organizations are not abandoning these systems outright; instead, they are focusing on incremental upgrades and interoperability enhancements with innovative solutions. In parallel, a significant revenue opportunity is emerging through the adoption and rollout of mission-critical broadband networks.

This Omdia White Paper was commissioned by Ericsson.

Figure 4: Omdia's critical communications market growth forecast for 2025–30



Source: Omdia

As broadband networks mature, a third wave of opportunity will emerge through innovative services and a broader solution ecosystem. This includes application-layer services, AI-driven insights, and cross-sector integrations that build on the foundational connectivity layer. It is important to note that these critical communications operators are also looking for further support from CSPs beyond connectivity and into offering a digitalized mission-critical platform enabled by advanced OSS and BSS capabilities, operational intelligence, assurance, automation, ecosystem integration, and service enablement. These value-added services will ultimately drive differentiation and long-term revenue growth beyond connectivity alone.

However, the adoption trajectories vary significantly across verticals. Factors such as spectrum availability, regulatory frameworks, budget allocation cycles, and organizational readiness all influence deployment speed. For example, public safety agencies may face stricter regulatory constraints, while industrial sectors may prioritize investments that yield the greatest top-line (revenue) and bottom-line (cost savings) impact. Understanding these dynamics is essential for stakeholders aiming to capture value across each phase of the mission-critical evolution.

For critical communications operators, like CSPs, this phase represents a dual opportunity: infrastructure deployment and the provision of managed services. Omdia highlights that CSPs' continuous 3GPP standards evolution and enhancement make them strategically well-positioned to monetize this shift. They can leverage existing assets and offer customized options that range from prioritized resources to fully dedicated private networks. Additionally, their end-to-end management services can reduce operational complexity.

Figure 5: Critical communications in sovereign verticals represent an attractive $21bn+ opportunity for the second half of the decade (2026–30)

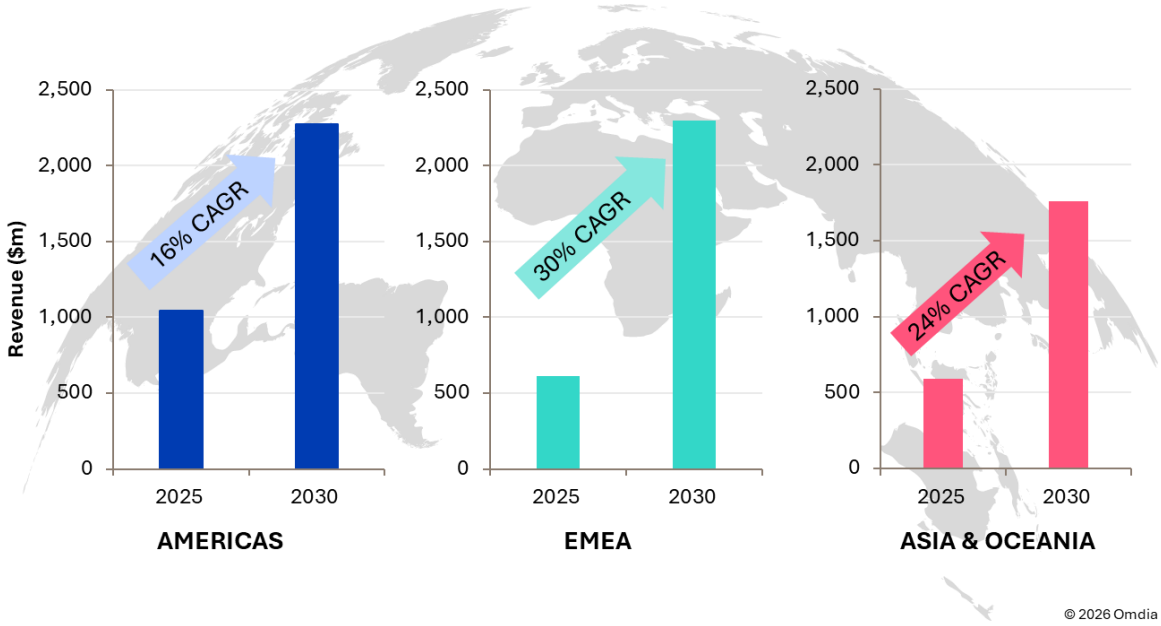
	Public safety	Utilities	Rail	Defense
Transformation driver	Creation of data-centric Collaborative environments	Smart grid adoption	Obsolescence of GSM-R	Military advantage
Urgency	Medium-high	Medium	High	High
Coverage	Nationwide	Regional	Wide area (pre-defined)	Mixed (base, tactical)
Model	Government tenders	Capex –heavy model	Service heavy vertical	Heavily regulated
Key focus	Collaboration	IoT coverage	Converged technologies	Flexible coverage
Opportunity (2026–30)	**$7,900m**	**$3,200m**	**$1,800m**	**$6,900m**
Opportunity for CSPs	Very attractive alignment	PN offering	Starts from 2028	High complexity, high reward
Impact of OSS or BSS	Very high	Medium	Medium-high	High

Source: Omdia

This alignment between CSP capabilities and vertical-specific requirements is, however, uneven, with each vertical experiencing different levels of alignment and near-term opportunity. CSPs are well-positioned to support nationwide and regional deployments, often in partnership with governments, making this a priority segment.

This Omdia White Paper was commissioned by Ericsson.

Figure 6: Omdia's forecast of CSPs' total addressable market (TAM) in mission-critical broadband infrastructure by region (2025–30)



Source: Omdia

The enabling role of OSS and BSS in mission-critical networks

Each of these innovations depends on broadband networks that can deliver mission-critical performance. Behind those networks lie crucial, often overlooked layers: operations support systems (OSS) and business support systems (BSS). OSS and BSS enable critical communications operators to effectively offer full control over the management of their network, services, and end-user interactions. While distinct in their functions, they work together to ensure seamless operations and customer satisfaction. As mentioned, mission-critical networks support verticals like public safety, defense, utilities, and rail that all demand performance characteristics far beyond those of traditional commercial networks. Consequently, the OSS and BSS systems supporting these networks must play complementary roles to ensure their strict requirements are met consistently, predictably, and transparently.

Modern OSS and BSS solutions enable critical communications operators the ability to guarantee performance, anticipate issues, and adapt services instantly as conditions

change. CSPs position themselves as trusted partners capable of supporting advanced use cases and transforming the operational workflows of mission-critical sectors, creating confidence that their communications will remain stable, secure, and predictable.

Table 1: Mapping critical communications requirements to the OSS (operational) and BSS (commercial and experience) capabilities that enable it

Requirement	Network context	How OSS capabilities address it	How BSS capabilities address it
High availability	Near-zero downtime; "always-on" expectations (e.g., 99.99% uptime) with rapid recovery from attacks and failures (natural disasters, cyberattacks, infrastructure damage).	Continuous network monitoring, fault management, redundancy modeling, automated failover orchestration, and health checks.	Business continuity processes, billing continuity, and proactive customer communication during DR events.
Low latency	Deterministic, ultra-low delay required for real-time video, autonomous systems, or tactical operations.	Real-time performance monitoring, traffic engineering, edge orchestration, and latency-aware routing.	Product differentiation (low-latency tiers), usage-based pricing, and latency-guaranteed service bundles.
Reliability and resilience (Disaster recovery)	Ability to withstand failures, cyberattacks, or physical disruptions and recover quickly.	Fault management, root cause analysis (RCA), self-healing networks, topology awareness, predictive maintenance analytics.	Customer communication workflows, outage notifications, churn mitigation, resilience-based service tiers.
Scalability	Ability to scale horizontally/vertically as device counts surge (e.g., IoT sensors).	Capacity planning, network inventory, automated provisioning, and elastic resource orchestration.	Scalable billing engines, subscription management, and dynamic offer creation for large device fleets.
Security	Protection against cyber threats, unauthorized access, and data breaches.	Security event monitoring, intrusion detection integration, policy enforcement, and compliance automation.	Identity management, fraud detection, secure billing/payment systems, and role-based access for agencies.
Real-time monitoring	Continuous visibility into network health, performance, and mission-critical KPIs.	Telemetry ingestion, KPI dashboards, alarm management, AI/ML anomaly detection, and real-time analytics.	Customer experience dashboards, SLA compliance reporting, and real-time service visibility for agencies.
Service assurance	Guaranteeing service quality and performance under all conditions.	End-to-end service monitoring, SLA assurance engines, predictive analytics, and closed-loop remediation.	SLA definition, penalty enforcement, customer reporting, and mission-critical service catalogs.
Interoperability	Multi-vendor, multi-technology, and cross-agency integration (e.g., legacy + 5G + satellite).	Standards-based interfaces (TMF Open APIs), mediation layers, inventory normalization, and topology federation.	Product catalog abstraction, partner settlement, and cross-provider billing for multi-agency operations.
Automation and orchestration	Fast, error-free service delivery with minimal manual intervention.	Zero-touch provisioning, workflow orchestration, closed-loop automation, and slice orchestration.	Automated order management, customer onboarding workflows, and dynamic service activation.
Network slicing (5G)	Logical partitioning of networks for different mission-critical use cases (e.g., public safety slice).	Slice lifecycle management, orchestration, performance isolation, and slice-specific assurance.	Slice-based monetization, SLA-tiered pricing, slice-specific reporting, and billing.
Regulatory compliance	Adherence to telecom, safety, and data regulations (e.g., lawful intercept, GDPR).	Audit trails, compliance reporting, lawful intercept support, and configuration governance.	Taxation, billing compliance, data privacy enforcement, and financial reporting.
Customer experience (QoE)	End-user perception of service quality critical for agencies relying on broadband for operations.	QoE analytics, service impact analysis, proactive issue detection, and device-level performance insights.	CRM integration, customer support systems, personalized offers, agency-specific dashboards.

Source: Omdia

OSS and BSS must be ready for the mission ahead

For critical communications operators, the main trigger when choosing a partner to execute their digitalization journey is the ability to deliver assured, predictable, and highly customized services for their operations, which cannot tolerate failure.

Legacy CSP systems were never designed to support the dynamic, real-time, and mission-critical requirements that now define these verticals. Mission-critical customers require tailored configurations, like priority access for first responders, secure slices for defense operations, deterministic latency for rail signaling, or massive IoT onboarding for utilities.

CSPs that modernize their OSS and BSS to meet mission-critical expectations can position themselves as indispensable partners in this transformation. OSS and BSS solutions enable CSPs to deliver the responsiveness or reliability that mission-critical users require for services like closed-loop automation, assurance, and dynamic resource allocation across complex service chains.

The strategic conclusion is clear: CSPs cannot credibly compete in mission-critical vertical markets on network investments alone. The ability to deliver guaranteed performance, real-time assurance, and tailored vertical service models is the key to becoming a critical player in the digitalization journey that mission-critical verticals are undergoing. What's more, CSPs can accelerate the journey towards network autonomy and meet these stringent requirements in simpler, more automated ways. Hence, the modernization of their OSS and BSS stack is a foundational strategy towards growing from connectivity providers into trusted partners who can navigate complex sovereignty requirements of reliability, control, and independence.

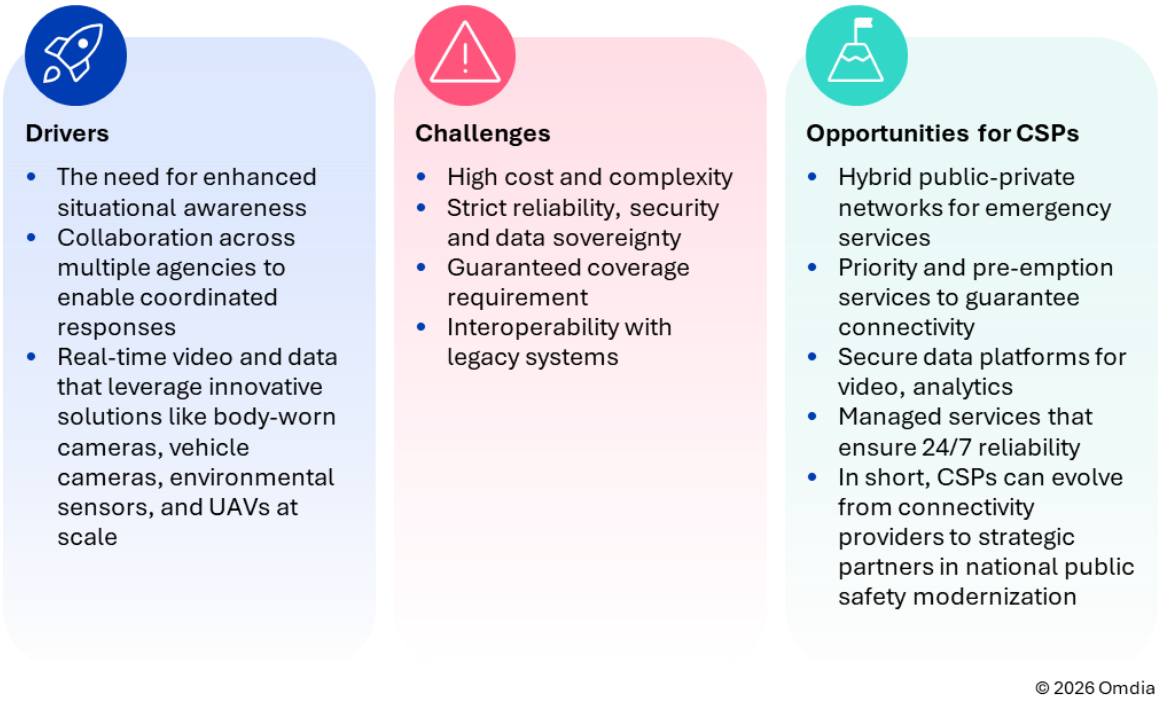
This Omdia White Paper was commissioned by Ericsson.

A vertical snapshot of mission-critical systems

Public safety

Ensuring life-critical, always-available communications that enable real-time situational awareness and coordinated response across police, fire, and emergency medical services. **Figure 7** provides an overview of the public safety vertical's journey toward mission-critical broadband, while **Tables 2** and **3** (on the next page) detail how OSS and BSS address the vertical requirements.

Figure 7: Journey toward mission-critical broadband – Public safety



Source: Omdia

Table 2: Vertical requirements addressed by OSS – Public Safety

Enabled use cases	User requirements	OSS element	How it works
Real-time situational awareness dashboards for command centers; early detection of degraded responder connectivity	Ultra-reliability, real-time visibility	**Service assurance and QoE analytics**	Monitors mission-critical KPIs (latency, packet loss, jitter) for emergency traffic and devices.
Immediate rerouting of emergency traffic; rapid mitigation during network failures in disaster areas	Rapid fault isolation and recovery	**Fault management (AI-assisted)**	Rapidly identifies outages affecting specific emergency zones.
Priority voice/video (MCPTT, MCVideo), body-worn camera streaming, drone feeds for incident response	Guaranteed QoS and isolation	**Network slicing management**	Designs, activates, and monitors dedicated public safety slices with strict SLA enforcement.
Automatic prioritization during mass-casualty events; surge handling during large public gatherings	Zero-touch response under stress	**Automation and closed-loop control**	Dynamically adjusts resources and QoS policies when congestion or incidents are detected.
Integration of legacy narrowband systems with LTE/5G mission-critical networks; phased technology migration	Multi-technology interoperability and service continuity	**Interoperability and mediation**	Translates and normalizes signaling, voice, video, alarms, and operational data across TETRA/P25 and LTE/5G systems to ensure seamless interoperability and migration continuity.

Source: Omdia

Table 3: Vertical requirements addressed by BSS – Public Safety

Enabled use cases	User requirements	BSS element	How it works
Contractual assurance for national emergency networks; SLA-backed public safety slices	Guaranteed service levels	**SLA management**	Defines and tracks strict uptime/latency/coverage SLAs for public safety agencies.
Role-based access to services and applications; differentiated profiles for police, fire, EMS	Multi-agency coordination, role control	**Customer and agency management (CRM)**	Manages agencies, users, roles, and entitlements (dispatcher vs field officer).
Rapid onboarding of new agencies; tailored offers for different forces	Mission-specific service packaging	**Product and offer catalog**	Makes public safety bundles (priority access, secure MCX, dedicated slices, devices).
Nationwide emergency network funding; transparent cost split between ministries and agencies	Government funding, shared infrastructure	**Billing and funding models**	Supports subsidies, cost-sharing, and multi-agency cost allocation.

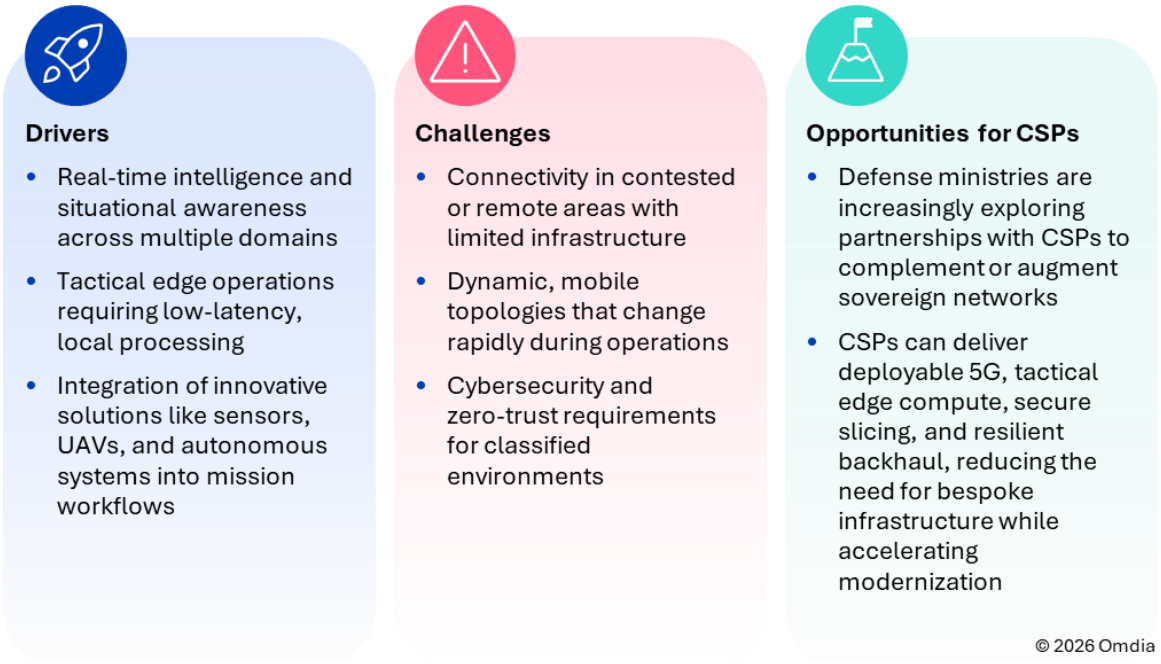
Source: Omdia

This Omdia White Paper was commissioned by Ericsson.

Defense

Maintaining secure, resilient, multi-domain communications that function in contested, mobile, and rapidly changing tactical environments. **Figure 8** provides an overview of the defense vertical's journey toward mission-critical broadband, while **Tables 4** and **5** (on the next page) detail how OSS and BSS address the vertical requirements.

Figure 8: Journey toward mission-critical broadband – Defense



Source: Omdia

This Omdia White Paper was commissioned by Ericsson.

Table 4: Vertical requirements addressed by OSS – Defense

Enabled use cases	User requirements	OSS element	How it works
Secure battlefield communications; protected command-and-control links; hardened tactical networks	Cyber resilience, confidentiality	**Security management (zero trust, encryption)**	Continuously monitors security posture, enforces policies, integrates with IDS/IPS, and key management.
Real-time drone video analytics; AR for soldiers; local decision-making when backhaul is degraded	Low latency at tactical edge	**Edge and MEC orchestration**	Deploys and manages compute at forward locations; orchestrates apps close to users.
Rapid reconfiguration of battlefield networks; dynamic routing based on unit movement	Dynamic, mobile environments	**Network topology inventory**	Tracks mobile nodes, satellites, vehicles, field units, and their connectivity.
Maintaining comms under cyber or kinetic attack; graceful degradation instead of total loss	Survivability under attack	**Fault and resilience management**	Self-healing, rerouting, and redundancy strategies in contested or jammed environments.
Electronic warfare-resilient communications; agile spectrum use in joint operations	Spectrum efficiency, EW adaptation	**Spectrum and resource management**	Dynamically allocates frequencies and power; adapts to interference and jamming.

Source: Omdia

Table 5: Vertical requirements addressed by BSS – Defense

Enabled use cases	User requirements	BSS element	How it works
Long-term managed service agreements for defense networks; measurable mission-readiness metrics	Mission assurance, accountability	**Contract and SLA management**	Encodes performance guarantees and penalties in defense contracts.
Interoperable coalition networks; controlled access for NATO or coalition exercises	Multi-nation operations	**Partner and coalition management**	Manages access, policies, and entitlements across allied forces and coalition partners.
Budget transparency for defense ministries; mission-based cost reporting	Resource accountability	**Usage and cost allocation**	Tracks usage by unit, theater, or mission; allocates costs accordingly.
Controlled access to classified networks; differentiated access for contractors vs active forces	Secure access control	Identity and access management (IAM)	Role- and clearance-based access to services, data, and network segments.

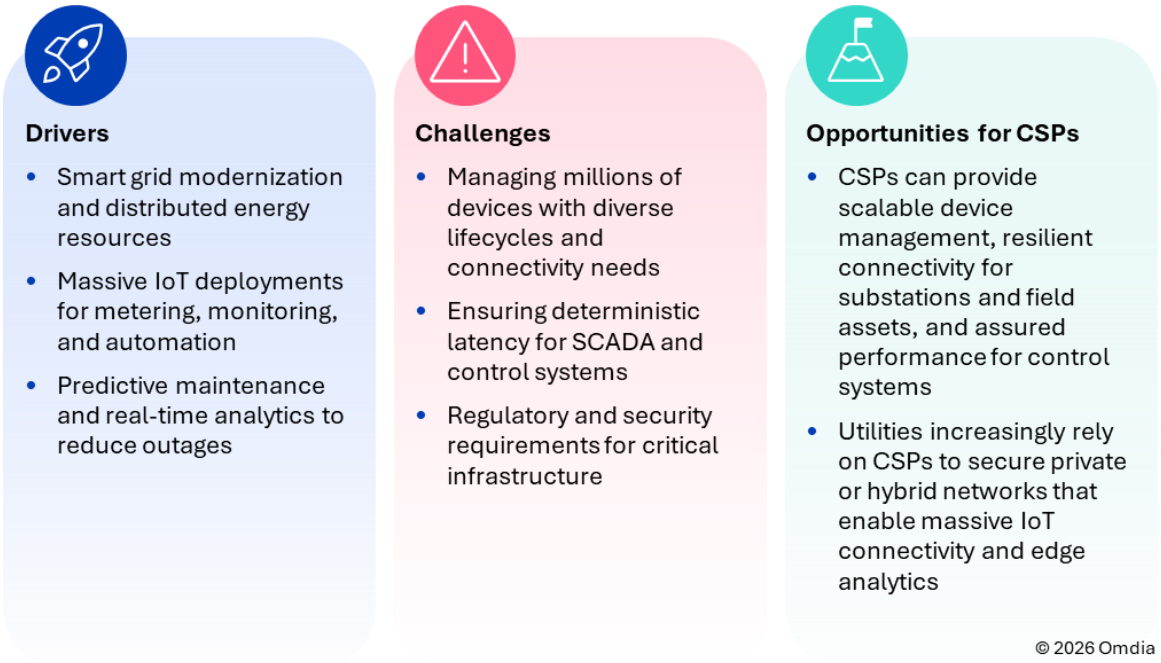
Source: Omdia

This Omdia White Paper was commissioned by Ericsson.

Utilities

Supporting the stability and safety of national critical energy infrastructure through reliable, scalable, and deterministic communications for millions of IoT devices and control systems. **Figure 9** provides an overview of the utilities vertical's journey toward mission-critical broadband, while **Tables 6** and **7** (on the next page) detail how OSS and BSS address the vertical requirements.

Figure 9: Journey towards mission-critical broadband – Utilities



Source: Omdia

This Omdia White Paper was commissioned by Ericsson.

Table 6: Vertical requirements addressed by OSS – Utilities

Enabled use cases	User requirements	OSS element	How it works
Real-time grid balancing; early detection of instability or overload conditions	Grid stability, control reliability	**Performance monitoring and analytics**	Monitors latency, jitter, and packet loss for SCADA/control traffic.
Smart metering infrastructure; remote monitoring of substations and pipelines	Massive scale, lifecycle control	**IoT device and network management**	Onboards, configures, and monitors millions of meters, sensors, and RTUs.
Self-healing smart grids; automated isolation of faulty segments to prevent cascading failures	Fast, coordinated response	**Automation and orchestration**	Automates load shedding, rerouting, and fault isolation based on analytics.
Large-scale smart meter rollouts; rapid deployment of sensors in new substations	Rapid provisioning at scale	**Service fulfillment**	Automates activation of connectivity and services for new devices and sites.
Predictive maintenance; optimized field operations, and upgrade planning	Infrastructure visibility and planning	**Asset/inventory management**	Maintains a unified view of network assets, field devices, and connectivity.

Source: Omdia

Table 7: Vertical requirements addressed by BSS – Utilities

Enabled use cases	User requirements	BSS element	How it works
Smart meter billing; time-of-use pricing; industrial demand-based billing	Usage-based pricing, regulatory compliance	**Billing and charging**	Integrates meter data into rating and billing; supports complex tariffs.
Energy usage insights; tailored offers for large industrial customers; outage communication	Consumer and industrial engagement	**Customer management**	Manages residential, commercial, and industrial customer profiles and contracts.
Incentive programs for load shifting; bundled connectivity + energy services	New service models and flexibility	**Product catalog**	Defines energy-as-a-service, demand response, and flexibility services.
Fraud/theft detection; identification of non-technical losses in the grid	Loss prevention, integrity	**Revenue assurance**	Detects anomalies between usage and billing; flags potential theft or leakage.

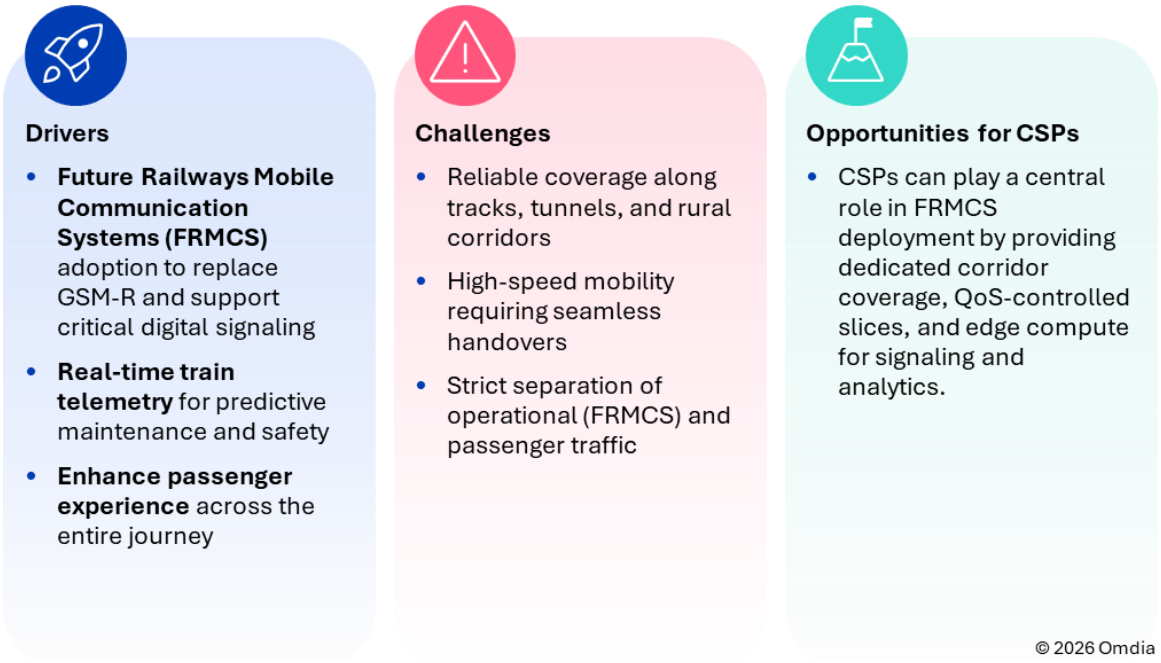
Source: Omdia

This Omdia White Paper was commissioned by Ericsson.

Rail

Enabling safe, efficient rail operations through ultra-reliable, low-latency communications for signaling and train control and communications as networks transition from GSM-R to FRMCS. **Figure 9** provides an overview of the rail vertical's journey toward mission-critical broadband, while **Tables 8** and **9** (on the next page) detail how OSS and BSS address the vertical requirements.

Figure 10: Journey towards mission-critical broadband – Rail



Source: Omdia

This Omdia White Paper was commissioned by Ericsson.

Table 8: Vertical requirements addressed by OSS – Rail

Enabled use cases	User requirements	OSS element	How it works
Safe train control (ETCS/CBTC); early detection of signaling degradation	Safety and uptime for signaling	**Service assurance**	Monitors the reliability and latency of signaling and control communications.
Guaranteed performance for signaling; controlled QoS for passenger services	Traffic prioritization and isolation	**Network slicing/QoS control**	Separates operational traffic (signaling, control) from passenger Wi-Fi and infotainment.
Minimizing train delays; targeted maintenance dispatch	Rapid recovery along linear assets	**Fault management**	Detects, localizes, and isolates failures along tracks, tunnels, and stations.
Continuous train-to-ground communication; real-time telemetry and CCTV streaming	Seamless handover at high speed	**Mobility management**	Ensures stable connectivity for trains moving at high speed across cells.
Real-time signaling decisions; local analytics for trackside sensors and CCTV	Low latency for control decisions	**Edge computing (MEC)**	Processes data near tracks and stations; hosts critical applications locally.

Source: Omdia

Table 9: Vertical requirements addressed by BSS – Rail

Enabled use cases	User requirements	BSS element	How it works
Real-time passenger information; delay notifications; onboard digital services	Passenger satisfaction and information	**Customer experience systems**	Integrates ticketing, Wi-Fi, notifications, and apps into a unified experience.
Digital fares; bundled connectivity + ticket products; roaming between operators	Revenue management	**Billing ad and ticketing integration**	Links transport services, connectivity, and ticketing into unified billing flows.
Contracts between rail operators and CSPs for corridor coverage and signaling connectivity	Operational guarantees for operators	**SLA management**	Defines and tracks uptime and performance SLAs for rail operators.
Multi-operator rail systems; integrated services across national and regional operators	Ecosystem and multi-operator integration	**Partner management**	Manages relationships with rail operators, authorities, and service partners.

Source: Omdia

This Omdia White Paper was commissioned by Ericsson.

Enabling the digitalization of critical verticals with OSS and BSS

As mentioned earlier, to compete for mission-critical vertical markets, CSPs need to ensure their OSS and BSS are up to the task. The first step in doing so is to ensure the underlying platform is modernized so it delivers the governance and visibility needed to manage risk, maintain service quality, and support multiple stakeholders across complex environments. This way, OSS and BSS can provide mission-critical operators with the backbone for the full-service lifecycle, spanning design, activation, assurance, and monetization.

Ericsson's OSS and BSS portfolio offers solutions that deliver on the stringent requirements of public safety, defense, utilities, and rail verticals, providing end-to-end lifecycle control purpose-built for mission-critical networks and services. Its capabilities cover service definition, catalog-driven orchestration, provisioning, activation, assurance, and billing, all delivered in a coordinated and consistent manner. This eliminates operational fragmentation, accelerates time-to-service, and establishes a repeatable, scalable model for launching and managing mission-critical services with confidence.

- Ericsson's Core Commerce solutions, including Digital Experience Platform, Catalog Manager, and Order Care, enable operators to rapidly design, commercialize, and lifecycle-manage mission-critical services through a unified and catalog-driven approach. These capabilities support dynamic service configuration, multi-agency service management, order handling, and customer engagement while simplifying operational processes and accelerating time-to-market. The modular and API-driven architecture also enables easier integration with ecosystem partners, external systems, and evolving mission-critical business models.
- Ericsson's Service Orchestration and Assurance integrates service order management with orchestration. Service intent orchestration enables automated, agile, and scalable delivery, while assurance monitors performance and real-time inventory tracks network state. The Adaptive Inventory delivers end-to-end network and service visibility across physical, virtual, and logical domains, addressing multi-vendor, multi-technology complexity through federation and automation. These products make end-to-end operations visible, controllable, and automatable.
- Ericsson's Charging and Billing Evolved solution enables real-time usage collection, charging, billing, and reconciliation across multiple departments and agencies within mission-critical networks. It provides transparent and auditable usage visibility, ensuring accurate cost allocation, financial accountability, and inter-agency

settlement. The solution also supports flexible charging models and policy-driven monetization, helping organizations manage shared network resources efficiently while maintaining operational resilience and trust.

- Ericsson Digital Monetization Platform brings together Ericsson's Core Commerce and Monetization platforms, along with TM Forum-aligned open APIs, to deliver a comprehensive BSS solution.

- Many CSPs are embracing cloud-native and AI-driven, modernized OSS and BSS. They are transitioning from monolithic systems to highly modular cloud-native systems that can be scaled more efficiently and upgraded more simply and with lower risk. Hosting cloud-native applications in the public cloud brings the added advantages of scalability and flexibility with robust security and reliability, and access to hyperscaler innovation. Ericsson's Cloud and IT managed services enable outcome-focused operations by providing E2E operational visibility, operational continuity, service reliability, and efficient business processes across distributed network, IT, and cloud domains, unlocking the necessary operational efficiency requested by critical communications operators.

- Finally, while AI has been used in OSS and BSS for some years, generative AI (GenAI) and agentic AI are opening up a whole new world of possibilities to improve customer experience and increase automation. Ericsson's Data and AI solutions—like its Telco DataOps Platform—provide unified data collection, refinement, management, and governance that integrates data from network, IT, and business layers. Its Telco IT AI Apps leverage AI and GenAI to deliver intelligent insights to improve service availability, reduce total cost of ownership, and deliver smooth operations. Expert Analytics measures perceived subscriber experience using correlated metrics and events from network nodes, probes, devices, OSS and BSS, and other sources, enabling users to predict, prioritize, and resolve subscriber-impacting events. Together, they enable more intelligent, AI-driven operations.

Case Study: Emergency Services Network, UK

Ericsson partnered with IBM to deliver the Emergency Services Network (ESN) in Great Britain. The ESN will coordinate efforts and responses from frontline staff, making the streets safer and delivering on the UK government's Plan for Change. Ericsson will leverage its core network and OSS/BSS portfolios, alongside its mission-critical expertise and other professional services, to deliver the new network. The ESN will support more than 300,000 emergency responders in Great Britain, providing them with better technology and faster access to data in emergency situations and frontline operations. Police forces, fire services, and ambulance trusts will be able to share live data and imagery, location reports, and essential public safety information as they work on time-critical rescue and response efforts.

To read more about this, visit this page.

This Omdia White Paper was commissioned by Ericsson.

Conclusion

Omdia sees mission-critical digitalization as a defining opportunity for CSPs, as broadband becomes the operational foundation for communication in all mission-critical verticals. As the shift from narrowband systems to critical broadband accelerates, CSPs' success in capturing this multi-billion-dollar market will depend on vertical expertise, trusted partnerships, and a commitment to operational excellence. It is with this last one that their OSS and BSS solutions can give them the advantage. Their OSS and BSS platforms must evolve into real-time engines that support the reliability, security, effectiveness, and simplicity of the network to meet the stringent expectations of mission-critical users.

To capture this opportunity, Omdia recommends that CSPs modernize their OSS and BSS with mission-critical requirements in mind, develop vertically aligned strategies, strengthen their ecosystem relationships, and follow the guidelines of standards bodies. CSPs that act now will shape the future of national critical infrastructure. Those that delay risk losing ground to more agile competitors.

This Omdia White Paper was commissioned by [Client Name].

Appendix

Authors

Ildefonso de la Cruz, Senior Principal Analyst, Critical Communications
Roz Roseboro, Senior Principal Analyst, Telecoms
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 Materials 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

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.