The invisible motions of modern railway transport

How cloud, IT infrastructure, workplace services and security keep critical transport moving.

From the platform, rail travel looks simple. A train arrives, passengers board, the doors close, and the journey continues. What passengers rarely see is the digital ecosystem that makes this possible. Today, reliable railway operations depend on far more than tracks, rolling stock and signalling. Cloud platforms, infrastructure, workplace services, data, cybersecurity and support teams all play a role in keeping services running smoothly. Together, they form an invisible layer that has become just as critical as the physical railway itself.

The moment technology becomes visible through delays, disruptions or security incidents, something has already gone wrong. As rail organisations continue to modernise, the questions become more strategic. How do you renew critical systems without disrupting operations? How do you secure increasingly connected environments? How do you maintain control over data and infrastructure? And how do you turn innovations such as AI into tangible operational value? This ebook explores the choices, challenges and opportunities shaping the next generation of railway operations, and what they mean when the partner you choose is a European one.

In this ebook, you'll discover:

- Why reliable railway operations increasingly depend on a strong digital foundation
- Why modernisation is challenging in railway environments
- Why cyber resilience is about protecting services, not just systems
- What digital sovereignty means in practice and why it has become a strategic consideration for critical infrastructure
- How AI can help reduce incidents, improve operational efficiency and support faster decision-making
- What to look for in a long-term technology partner for critical railway environments

Modernising without disruption

Railway organisations face a challenge that few industries encounter at the same scale: they need to modernise critical systems while maintaining uninterrupted operational continuity.

That modernisation is no longer optional. Legacy platforms become more expensive to maintain, harder to secure and increasingly difficult to integrate with newer technologies. At the same time, expectations continue to rise. Employees expect modern digital tools, passengers expect reliable services and regulators expect stronger governance and security. The challenge is therefore not whether to modernise, but how to do so without disrupting the services that depend on those systems every day.

Transformation is a journey, not a single project

In critical environments, successful modernisation rarely happens through a big-bang migration. Replacing large parts of the technology landscape in one move creates unnecessary risk and leaves little room to recover if something goes wrong. Instead, railway organisations typically adopt a phased approach that prioritises continuity throughout the transformation process.

This means new environments are introduced alongside existing ones, workloads are migrated gradually and every stage includes extensive testing and validation. Just as importantly, knowledge transfer starts long before a project is completed. Modernisation is not only about introducing new technology; it is also about ensuring internal teams can confidently operate, support and further develop those systems once they are in place.

IN PRACTICE

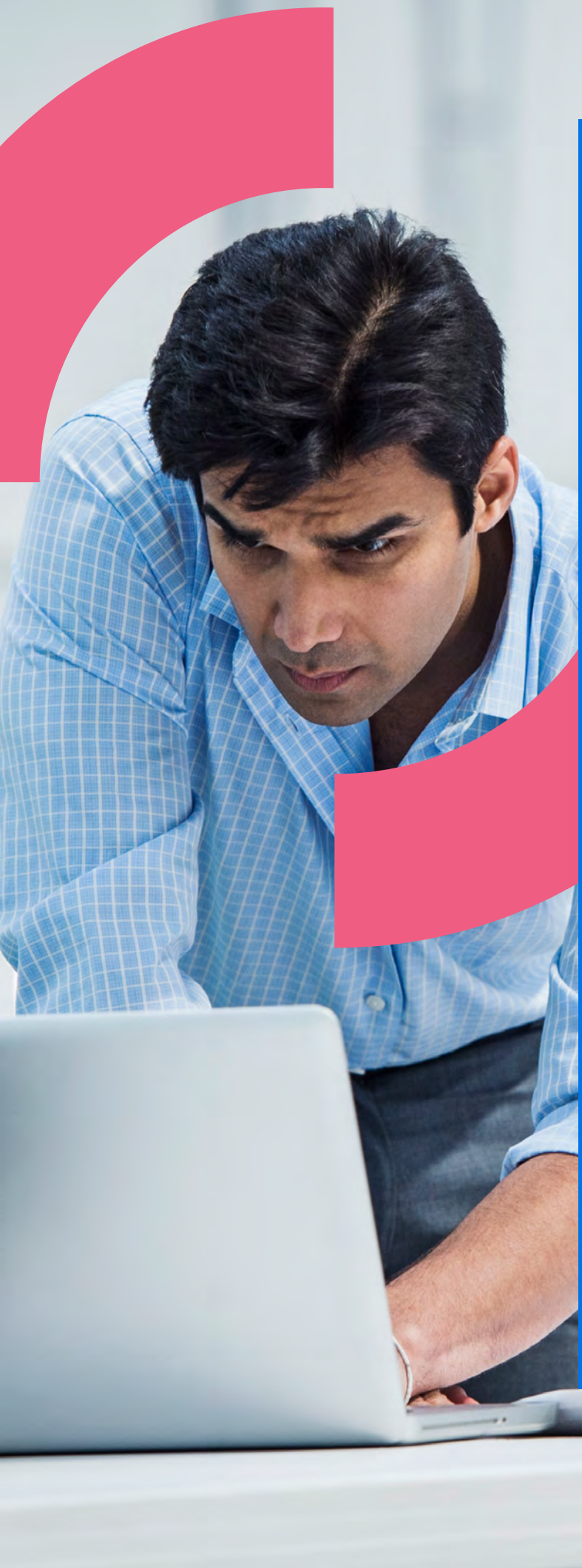
Network Rail

As part of Network Rail's cloud transformation programme, Atos migrated applications from legacy data centres to a modern private cloud environment. Legacy and modern systems operated alongside one another throughout the transition, ensuring continuity while reducing migration risk.

Why hybrid has become the norm

Not every workload belongs in the same environment. Some applications benefit from the scalability and flexibility of public cloud platforms, while others require greater control, lower latency or stricter governance. Operational systems may need to remain close to the railway environment itself, whereas customer-facing applications often benefit from cloud-native services.

As a result, most railway organisations are moving towards hybrid and multi-cloud environments rather than choosing a single deployment model. The objective is not to place everything in one location, but to ensure each workload runs where it delivers the most value. When designed correctly, a hybrid approach combines flexibility, resilience and control, creating an infrastructure that can evolve without compromising operational requirements.



Modernisation doesn't stop after migration

Technology alone does not keep railway operations running. Employees also need reliable workplace services, responsive support and easy access to the systems they rely on every day. When incidents occur, the speed at which people can access information and receive assistance can have a direct impact on operational performance.

The same principle applies once a transformation project has been completed. Migrating to a new environment is only the beginning. Long-term value comes from continuous monitoring, optimisation, maintenance and day-to-day operational management. Managed this way, the environment also becomes easier to keep efficient over time. Continuous optimisation reduces incidents and manual effort and removes the growing cost of maintaining ageing systems rather than letting it build up. Modernisation should therefore not be viewed as a one-off initiative, but as an ongoing effort to improve and protect the digital foundation that supports the railway. The passenger may never notice the difference, but that is precisely what success looks like.

Cyber resilience for critical transport

It is tempting to picture cybersecurity as guarding individual systems. In railway operations, the objective is broader than that. A cyber incident rarely remains confined to a single application or device. When critical systems become unavailable, the impact can quickly extend to passenger services, operational processes and day-to-day railway activities. The goal is therefore not simply to prevent attacks, but to ensure the organisation can continue operating and recover quickly when disruptions occur.

A growing attack surface

Railway operations rely on an increasingly interconnected mix of systems. Signalling and control environments, passenger information systems, workplace applications, cloud platforms and external suppliers all need to exchange information to keep services running efficiently.

That evolution brings clear benefits, but it also changes the cybersecurity challenge. Three trends stand out:

Increasing connectivity: systems that once operated largely in isolation are now connected across the organisation and beyond.

Growing dependencies: railway operations increasingly rely on cloud services, suppliers and external partners.

Persistent legacy technology: many critical systems remain in service for years or even decades and were never designed for today's level of connectivity.

The result

A larger attack surface and a greater number of potential pathways into the environment. Protecting modern railway operations therefore requires a holistic approach that spans IT, OT, cloud environments and third-party ecosystems rather than treating each domain separately.

The impact of NIS2

The growing complexity of railway environments has also changed the way cybersecurity is regulated. Under the European NIS2 Directive, railway operators and infrastructure managers are classified as essential entities. Cybersecurity is therefore no longer viewed solely as a technical responsibility, but as a matter of governance and organisational accountability.

In practice, organisations must:

- Manage cybersecurity risks across their operations and supply chain
- Establish incident response and recovery processes
- Report significant incidents within strict timelines
- Demonstrate management oversight and accountability

NIS2 raises the bar from having security controls in place to demonstrating that the organisation is prepared to respond when incidents occur.

The reporting clock

When a serious incident occurs, an essential service has 24 hours to raise the alarm, 72 hours to file a fuller report, and one month to deliver the full picture. Fines run up to € 10 million or 2% of global turnover.

Building resilience in practice

Meeting these expectations requires more than policies and procedures. Cyber resilience is ultimately built through a combination of people, processes and technology that work together to detect threats, respond to incidents and minimise disruption.

For many larger organisations, that starts with continuous monitoring. Security Operations Centres (SOCs) provide visibility across the environment, helping teams identify suspicious activity before it escalates into a larger issue. Incident response capabilities ensure that when something does happen, the right people, processes and communication channels are already in place. Other building blocks are equally important:

- **Managed Detection and Response (MDR)**
  to accelerate threat detection and containment.
- **Identity and Access Management (IAM)**
  to ensure only authorised users can access critical systems and data.
- **OT security capabilities**
  tailored to operational environments such as signalling and control systems.
- **Supply-chain security measures**
  to manage risks introduced by suppliers, contractors and external partners.

Bringing these capabilities together is often as important as the capabilities themselves. Atos, for example, operates a network of Security Operations Centres within Europe. It combines threat intelligence, incident response, managed detection and OT security expertise in a single operating model, under European jurisdiction. The objective is not to generate more alerts, but to enable faster, more coordinated responses when incidents occur and maintain control when it matters most.

Sovereignty as a strategic requirement

Where data lives is not the same as who controls it

When organisations evaluate cloud and technology providers, the conversation often starts with where data is stored. But for operators of critical infrastructure, that is only part of the picture. Data residency determines where data is physically located, for example on a server in Brussels or Frankfurt. Data sovereignty determines who ultimately controls that data, which laws apply to it and under what circumstances access can be requested. A provider can host data in Europe while still being subject to legislation outside Europe.

Three questions worth separating:

- **Where does the data reside?** (Physically storing it in Europe answers only the first question.)
- **Who runs the systems?**
- **Which company, under which country's law, ultimately holds the keys?**

Why foreign law can still reach European data

For operators of critical infrastructure, the distinction between residency and sovereignty matters because jurisdiction does not stop at national borders. Legislation such as the US CLOUD Act allows authorities to request access to data held by providers under US jurisdiction, regardless of where that data is physically stored. In other words, storing data in Europe does not automatically guarantee European control over that data.

This reality has made sovereignty an increasingly important consideration for organisations operating critical infrastructure. The conversation is no longer limited to security, performance or cost. It also includes questions around governance, legal exposure and long-term control.

Suddenly, your supplier is a control decision

As a result, technology decisions are increasingly becoming control decisions. Organisations need to understand not only what a platform can do, but also what dependencies come with it.

This shift is becoming visible in procurement processes across Europe. Public-sector and critical-infrastructure organisations increasingly look beyond technical capabilities alone when selecting technology partners. Questions around governance, legal jurisdiction and operational control are becoming just as important as security, availability and performance.

European by design

This is where European providers can offer a distinct advantage. By combining European jurisdiction with local operational expertise and governance frameworks, they can help organisations strengthen sovereignty across their digital estate.

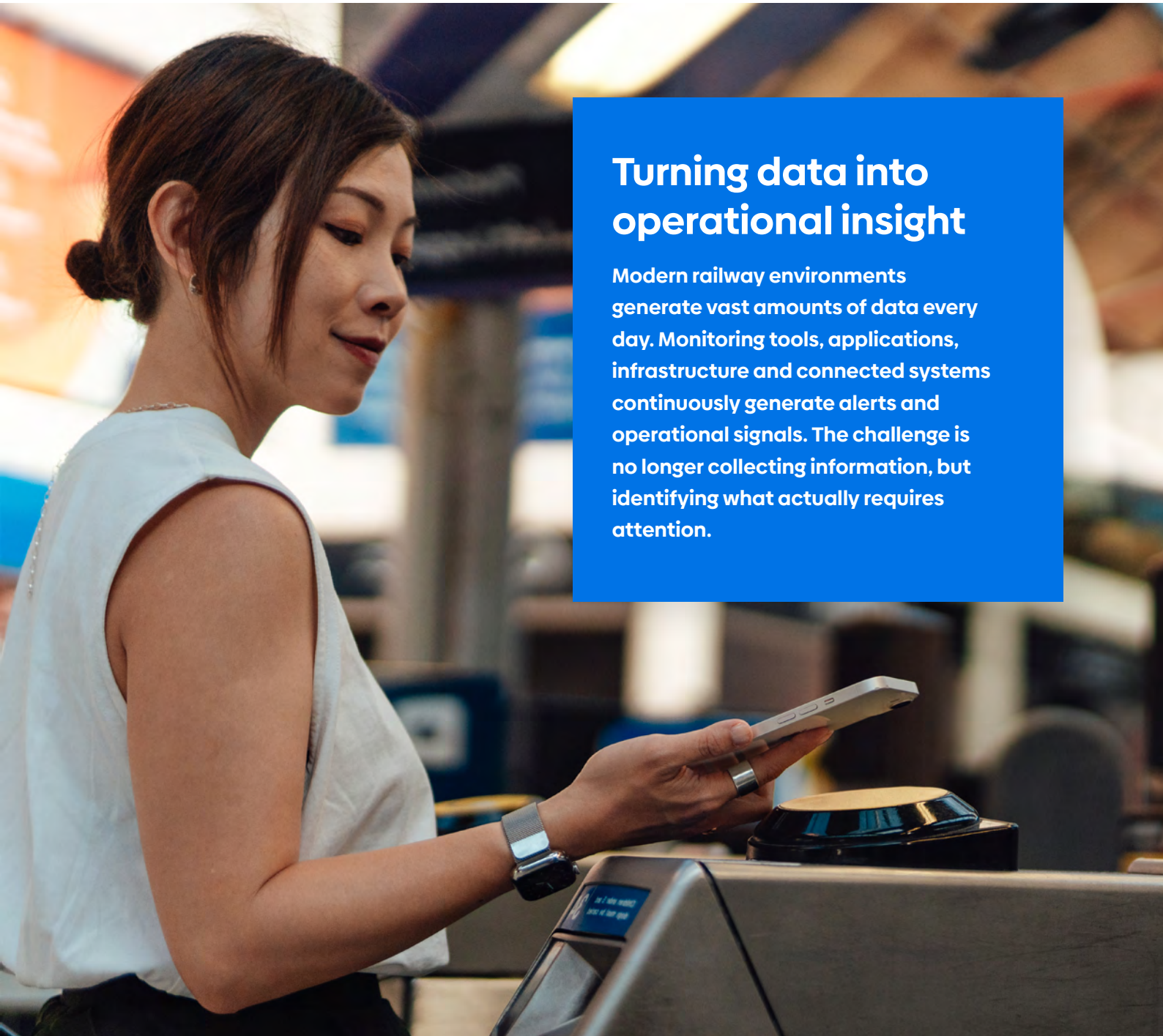
Atos is one example. As a European company and founding member of the GAIA-X initiative, it has developed dedicated frameworks and services to help organisations manage sovereignty requirements across hybrid and multi-cloud environments. This allows sovereignty considerations to be built into cloud, infrastructure and cybersecurity strategies from the outset rather than being addressed afterwards.

Sovereignty does not limit your technology choices. It makes them deliberate: you weigh convenience against control and you keep the systems that matter most out of reach of foreign law.

AI for railway operations

Few technologies have generated as much attention as AI. Yet for railway operators and infrastructure managers, the question is not whether AI is innovative. The question is whether it delivers measurable operational value.

In practice, that means fewer incidents, faster resolution times and less time spent on repetitive tasks. Used well, AI helps organisations manage growing complexity without adding complexity of its own. The most valuable applications are often the least visible: helping teams identify patterns, prioritise actions and make better decisions faster.



Turning data into operational insight

Modern railway environments generate vast amounts of data every day. Monitoring tools, applications, infrastructure and connected systems continuously generate alerts and operational signals. The challenge is no longer collecting information, but identifying what actually requires attention.

AIOps: from alert overload to actionable insights

AIOps, or Artificial Intelligence for IT Operations, is designed to turn large volumes of operational data into meaningful insight. Rather than forcing teams to sift through countless alerts and signals, it helps identify what matters most and when action is required.

In practice, it helps teams by:

- **Connecting related signals that might otherwise appear unrelated**
- **Surfacing the issues that require immediate attention**
- **Automating routine fixes before they become larger problems**

Instead of reacting after something breaks, teams gain visibility while there is still time to act. This type of automation can reduce routine response times by up to 80 percent. The exact impact will depend on the environment, but the principle is clear: less time spent sorting through alerts means more time focused on preventing disruption.

Predictive maintenance

The same principle can be applied to physical assets in railway operations. By analysing operational and maintenance data, AI can help identify potential failures before they disrupt services. This allows maintenance teams to move from reactive interventions to planned, proactive maintenance. Atos, for example, works with train manufacturer Talgo on real-time data and predictive maintenance initiatives aimed at improving reliability and operational efficiency.

Faster, cooler-headed cyber-security

The value of AI is not limited to operational efficiency. It is also helping organisations strengthen their cyber resilience by improving how threats are detected, analysed and prioritised. In modern railway environments, security teams are required to monitor a growing number of systems, users and external connections. AI can help by identifying suspicious activity, correlating events across different environments and providing additional context for investigation.

Rather than replacing human expertise, AI helps security teams focus their attention where it is needed most. By accelerating detection and investigation, it enables organisations to respond more quickly when potential threats emerge and reduce the risk of incidents escalating into operational disruption.

AI assists, people decide

As AI becomes more embedded in operations and cybersecurity, one principle remains unchanged: accountability stays with people. AI can improve detection, prioritisation and routine decision-making, but it does not replace operational expertise. For railway organisations, its real value lies in helping experienced teams make better decisions, respond faster and maintain control in increasingly complex environments. Used that way, AI is not a leap of faith. It is a practical tool for keeping critical operations one step ahead.

The importance of choosing the right technology partner

Throughout this ebook, we explored four challenges that increasingly define the future of railway operations.

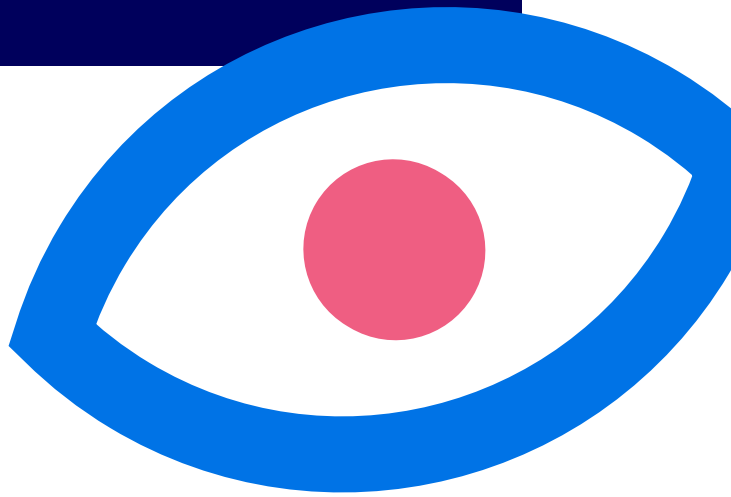
- How do you modernise critical systems without disrupting operations?
- How do you strengthen cyber resilience as environments become more connected?
- How do you maintain control over data and digital infrastructure in a rapidly evolving regulatory landscape?
- How do you use AI to turn growing complexity into actionable insights?

Separately, these may seem like different conversations. In practice, they all point to the same challenge: how do you continuously evolve the technology beneath the railway while maintaining the reliability, safety and continuity that passengers, operators and regulators expect? For organisations operating critical infrastructure, that is ultimately the question a technology partner must help answer.

What to look for

Railway organisations need more than a technology supplier. They need a partner that understands continuity, can connect multiple technology domains and has proven experience in critical environments. When evaluating potential partners, four questions are worth asking:

- Do they understand the operational realities of a railway environment?
- Can they bring together cloud, infrastructure, workplace services, cybersecurity and AI as part of a single strategy?
- Can they provide the level of control, governance and sovereignty required for critical systems and sensitive data?
- Do they have proven experience operating and transforming environments where downtime is not an option?



Addressing the full digital foundation of the railway

Atos brings a distinctive combination of expertise and experience. For over thirty years, the company has been working with railway operators, infrastructure managers and transport organisations across Europe. That experience extends beyond delivering technology projects. Atos does not just help railways digitise; it takes responsibility for operating, securing and evolving the critical platforms that keep daily railway operations running, as a European partner committed for the long term.

By combining capabilities across cloud, infrastructure, digital workplaces, cybersecurity, sovereign digital environments and AI, Atos helps organisations address the full digital foundation of the railway rather than isolated parts of it. This allows transformation initiatives, security requirements, governance objectives and operational priorities to be managed as part of a broader strategy instead of separate programmes. Managed as one whole, that foundation is also easier to keep efficient over time, reducing incidents and making your IT costs predictable.

If your organisation is evaluating how to modernise critical infrastructure, strengthen cyber resilience, address sovereignty requirements or unlock the value of AI, the conversation starts with understanding how these challenges connect. Atos helps railway organisations translate those priorities into a practical and sustainable roadmap for transformation.

Get in touch →

Atos